

# Теория кодирования

В.М. Сидельников

25 августа 2006 г.



# Оглавление

0.1	Введение . . . . .	9
<b>1</b>	<b>Базовые понятия</b>	<b>11</b>
1.1	Пространство Хемминга . . . . .	11
1.1.1	Метрика Хемминга . . . . .	11
1.1.2	Линейный код . . . . .	12
1.1.3	Двойственный код . . . . .	13
1.1.4	Пространство, образованное равновесными двоичными векторами . .	14
1.2	Сфера $S^{n-1}$ . . . . .	15
1.2.1	Метрика на сфере . . . . .	15
1.2.2	Ортогональные и унитарные преобразования . . . . .	16
1.2.3	Орбитный код . . . . .	17
1.3	Метрическое вложение кода в пространстве Хемминга на единичную сферу евклидова пространства . . . . .	18
1.3.1	Вложение двоичного пространства Джонсона на евклидову сферу . .	26
<b>2</b>	<b>Оценки</b>	<b>29</b>
2.0.2	Оценка Хемминга (Граница сферической упаковки) . . . . .	29
2.0.3	Оценки сверху для числа элементов равновесных кодов . . . . .	31
2.0.4	Оценка Элайса-Бассалыго . . . . .	32
2.0.5	Оценка Плоткина и матрицы Адамара . . . . .	32
2.0.6	Оценки Синглтона и Грайсмера . . . . .	36
2.0.7	Оценка для числа элементов антиподального кода . . . . .	38
2.0.8	Оценка Варшамова-Гилберта . . . . .	40
2.0.9	Асимптотические границы . . . . .	41
2.0.10	Основные задачи теории кодирования . . . . .	43
<b>3</b>	<b>Центральные функции на линейном пространстве Хемминга</b>	<b>45</b>
3.1	Специальные функции . . . . .	45
3.1.1	Характеры . . . . .	45
3.1.2	Автоморфизмы группы $\mathfrak{G}$ . . . . .	46
3.1.3	Скалярное произведение . . . . .	47
3.1.4	Классы сопряженных элементов . . . . .	48
3.1.5	Центральные функции относительно подгруппы $H$ группы $\text{Aut}(\mathfrak{G})$ .	48
3.2	Ортогональные многочлены . . . . .	51
3.2.1	Элементарная абелева группа . . . . .	51
3.2.2	Примарная группа порядка $p^l$ . . . . .	54

3.2.3	Многочлены Кравчука и мономиальная группа . . . . .	55
3.2.4	Симметрическая группа в качестве группы $H$ и полная весовая функция кода . . . . .	57
3.2.5	Ортогональные многочлены для примарного кольца вычетов . . . . .	58
3.2.6	Многочлены Кравчука, как зональные сферические функции . . . . .	59
<b>4</b>	<b>Оценка линейного программирования</b>	<b>63</b>
4.1	Положительно определенные функции . . . . .	63
4.2	Оценка линейного программирования . . . . .	65
4.2.1	Оценка Дельсарта . . . . .	65
4.2.2	Выбор многочлена в оценке (4.2.6) . . . . .	67
<b>5</b>	<b>Коды Рида-Соломона и БЧХ-коды</b>	<b>73</b>
5.0.3	Определение кода Рида-Соломона . . . . .	73
5.0.4	Коды Рида-Соломона. . . . .	74
5.1	Циклические коды . . . . .	76
5.1.1	Циклические коды $RS_q(n, d)$ типа 1 . . . . .	79
5.1.2	Представление вектора циклического кода в виде рекуррентной последовательности . . . . .	79
5.1.3	Представление векторов циклического кода в виде значений функции "след" . . . . .	81
5.1.4	Представление элементов циклического кода в виде элементов группового кольца циклической группы над конечным полем . . . . .	82
5.2	Коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) . . . . .	89
5.2.1	Группа автоморфизмов БЧХ-кода . . . . .	89
5.2.2	Представление БЧХ-кода в виде идеала кольца $R_r^{(n)}$ . . . . .	90
5.2.3	Параметры БЧХ-кода . . . . .	91
5.2.4	Циклические коды Боуза-Чоудхури-Хоквингема . . . . .	93
5.2.5	Точное значение размерности БЧХ-кода при не слишком больших значениях $d$ . . . . .	93
5.3	Обобщенные коды Рида-Соломона $RS_q(n, d)$ . . . . .	95
5.3.1	Обобщенные БЧХ-коды . . . . .	96
5.3.2	Циклический обобщенный БЧХ-код длины $n = q + 1$ . . . . .	96
5.3.3	Коды Гошпы . . . . .	97
5.4	Автоморфизмы кода . . . . .	100
5.4.1	Группа автоморфизмов кода . . . . .	101
5.4.2	Подгруппы группы автоморфизмов кодов Рида-Соломона $RS_q(n, d)$ . . . . .	103
5.5	Группа обобщенных автоморфизмов кода . . . . .	104
5.5.1	Группа дробно-линейных преобразований. . . . .	105
5.6	Число обобщенных кодов Рида-Соломона . . . . .	106
5.6.1	Число проверочных матриц кода $RS_q(n, d)$ . . . . .	106
5.6.2	Число обобщенных кодов Рида-Соломона . . . . .	106

<b>6</b>	<b>Декодирование кодов Рида-Соломона</b>	<b>109</b>
6.1	Что такое алгоритм декодирования?	109
6.1.1	Вводные понятия	111
6.2	Синдромный метод декодирования RM-кодов	113
6.2.1	Предварительные замечания	113
6.2.2	Вспомогательные утверждения	114
6.2.3	Многочлен локаторов ошибок	115
6.2.4	Алгоритм Берлекэмпа	117
6.2.5	Как вычислить многочлен $O_u(x)$ , если $ \Delta_r  = 0$ для некоторого $r \leq u - 1$ ?	121
6.2.6	Формула Кристофеля-Дарбу	122
6.2.7	Как вычислить число $u$ ошибок, поразивших кодовый вектор?	124
6.2.8	Один несиндромный алгоритм декодирования кода Рида-Соломона	125
6.2.9	Краткий обзор некоторых результатов по декодированию кодов Рида-Соломона	126
<b>7</b>	<b>Коды Рида-Маллера</b>	<b>131</b>
7.0.10	Булевы функции и многочлены Жегалкина	131
7.0.11	Элементарные свойства кода Рида-Маллера	133
7.1	Декодирование кода Рида-Маллера	137
7.1.1	Алгоритм декодирования RM-кода первого порядка по максимуму правдоподобия и "быстрое" умножение вектора на матрицу Адамара	138
7.1.2	Полиномиальный алгоритм декодирования RM-кода порядка $r > 1$	140
7.1.3	Основная идея полиномиального декодирования RM-кода $r$ -го порядка	142
7.1.4	Декодирование кода $RM_{1,m}$ первого порядка	143
7.1.5	Декодирование кода $RM_{2,m}$	144
7.1.6	Эффективность алгоритма декодирования в случае $r = 2$	146
7.1.7	Оценка вероятности ошибки декодирования кода по критерию максимального правдоподобия	148
7.2	Другие способы представления векторов RM-кода	151
<b>8</b>	<b>Некоторые частные классы кодов</b>	<b>155</b>
8.1	Вспомогательные результаты. Вычисление некоторых тригонометрических сумм.	155
8.2	Код Кердока	159
8.3	Код Препарата	162
8.4	Циклический линейный код, порождаемый булевыми функциями ранга 2	165
8.5	Авто и взаимная корреляция последовательностей	166
8.6	Коды с кодовым расстоянием 5 или 6	173
8.6.1	БЧХ-коды	174
8.6.2	Троичный БЧХ-код, исправляющий две ошибки	174
8.6.3	Троичный код работы [26], исправляющий две ошибки	175
8.6.4	Коды Геворкяна	177

<b>9</b>	<b>Весовой спектр линейного кода</b>	<b>181</b>
9.1	Спектр линейного кода и многочлены Кравчука . . . . .	183
9.1.1	Соотношение МакВильямс для весовой функции линейного кода . . .	183
9.1.2	Соотношение МакВильямс для полной весовой функции линейного кода . . . . .	185
9.1.3	Использование соотношения МакВильямс для вычисления спектра кода. . . . .	186
9.1.4	Функция типа $\chi^2$ для элементов спектра кода $\mathcal{K}$ . . . . .	189
9.1.5	Выражение функции $\Xi(\mathcal{K})$ через спектр двойственного кода. . . . .	190
9.1.6	Среднее функции $\Xi(\mathcal{K})$ . . . . .	192
9.1.7	Пример вычисления спектра кода $\mathcal{K}$ с помощью функции $\Xi(\mathcal{K})$ . . .	192
9.2	Спектр БЧХ-кодов . . . . .	193
<b>10</b>	<b>Схемы отношений</b>	<b>199</b>
10.0.1	Введение . . . . .	199
10.1	Построение схем отношений . . . . .	201
10.1.1	Схемы отношений $\mathcal{S}_H(\mathfrak{G})$ . . . . .	201
10.1.2	Примеры . . . . .	203
10.2	Схемы отношений на $\mathfrak{G}^n$ . . . . .	204
10.3	Алгебра Боуза-Меснера ассоциативной схемы . . . . .	206
10.3.1	Некоторые сведения из теории представления конечных групп . . . .	206
10.3.2	Базисы алгебры Боуза-Меснера . . . . .	208
10.3.3	Вычисление коэффициентов $P_k(j)$ для ассоциативной схемы $\mathcal{S}_H(\mathfrak{G})$ , у которой $H = Inn(\mathfrak{G})$ . Продолжение примера 10.1.2 . . . . .	211
10.3.4	$\mathfrak{G}$ — группа $(\mathbb{F}_p, +)$ . Продолжение примера 10.1.1 . . . . .	213
10.3.5	Схемы отношений Хемминга . . . . .	214
10.4	Метрики на схеме отношений $\mathcal{C}_H(\mathfrak{G})$ . . . . .	215
10.4.1	Скалярное произведение на группе . . . . .	216
10.4.2	Продолжение примера 10.1.1 . . . . .	216
10.4.3	Продолжение примера 10.1.2 . . . . .	217
10.4.4	Метрики на группе $\mathfrak{G}$ . . . . .	218
10.4.5	Метрика на группе $\mathfrak{G}^n$ . . . . .	220
10.4.6	Краткий обзор результатов по схемам отношений . . . . .	221
<b>11</b>	<b>Квантовые коды</b>	<b>223</b>
11.0.7	Определения . . . . .	224
11.0.8	О некоторых конечных группах порядка 8 . . . . .	226
11.0.9	Операторы . . . . .	227
11.0.10	Квантовые коды, образованные собственными векторами коммутативной подгруппы $\mathcal{H}_L$ группы $\mathcal{E}^{\otimes n}$ . . . . .	229
11.0.11	Квантовый "код Хемминга" длины $n = 2^m$ . . . . .	231
11.0.12	Квантовый код с кодовым расстоянием 5 . . . . .	233

<b>12 Открытые системы шифрования на основе кодов, корректирующих ошибок, и как некоторые из них можно расколоть</b>	<b>235</b>
12.0.13 Введение . . . . .	235
12.0.14 Группа автоморфизмов кода $RS_q(n, d)$ , $n = q$ . . . . .	236
12.0.15 Число проверочных матриц кода $RS_q(n, d)$ . . . . .	237
12.0.16 Группа обобщенных автоморфизмов кода $RS_q(n, d)$ , $n = q + 1$ , Рида-Соломона . . . . .	237
12.0.17 Группа дробно-линейных преобразований. . . . .	239
12.1 Декодирование . . . . .	240
12.2 Системы открытого шифрования на основе кода, корректирующего ошибки	242
12.2.1 Система открытого шифрования Маклиса. . . . .	242
12.2.2 Система открытого шифрования Нидеррайтера. . . . .	244
12.2.3 Сравнение систем открытого шифрования Маклиса и Нидеррайтера.	245
12.2.4 Некоторые свойства систем открытого шифрования Маклиса и Нидеррайтера. . . . .	246
12.3 Как раскалывается система открытого шифрования Нидеррайтера, построенная с помощью обобщенного кода Рида-Соломона ? Общие подходы. . . .	247
12.4 Алгоритм определения секретного ключа системы открытого шифрования, использующего обобщенный код Рида-Соломона . . . . .	248
12.4.1 Как определить первые три элемента $\omega_j$ ? . . . . .	248
12.4.2 Определение элементов $\omega_j$ , $j > 3$ . . . . .	249
12.4.3 Определение элементов $z_j$ и матрицы $h$ . . . . .	251
12.4.4 Заключительные замечания . . . . .	252
<b>13 Совершенная секретность в полилинейных системах распределения ключей</b>	<b>255</b>
13.1 Модель системы распределения ключей . . . . .	255
13.1.1 Введение . . . . .	255
13.1.2 Вводные замечания . . . . .	256
13.1.3 Математическая модель системы распределения ключей . . . . .	257
13.2 Определение полилинейной системы распределения ключей $\mathcal{S}$ . . . . .	258
13.2.1 Свойства ключевой системы . . . . .	259
13.3 Конструкция полилинейной $(t, w)$ -системы распределения ключей . . . . .	260
13.4 Основной результат . . . . .	262
13.4.1 Возможные конструкции множеств $Q$ . . . . .	264
13.5 Системы распределения ключей Блундо и др. . . . .	265
13.6 Нижние оценки числа ключей у пользователей $(w, t)$ —системы распределения ключей . . . . .	266
<b>14 Дизъюнктные и разделяющие коды</b>	<b>269</b>
14.1 Дизъюнктные коды (superimposed code) . . . . .	269
14.1.1 Разделяющие коды . . . . .	271
14.1.2 Построение разделяющих $(w, 1)$ —кодов, [30] . . . . .	273
14.2 Каскадная конструкция дизъюнктных кодов . . . . .	275
14.3 Максимальные дизъюнктные $l$ —коды . . . . .	277
14.3.1 Максимальный дизъюнктный $l$ —код $\mathcal{Q}_{q,l}$ с $q$ элементами . . . . .	278

14.4 Криптографические приложения дизъюнктивных кодов . . . . .	282
---	-----



## 0.1 Введение

В настоящей книге изучаются методы построения и свойства кодов, корректирующих ошибки. Она предназначена для математиков и специалистов по информационным технологиям, имеющих некоторую математическую подготовку, которые хотят достаточно глубоко изучить отдельные разделы теории кодирования и некоторые ее приложения. Вместе с тем начальные главы книги дают в достаточно элементарной форме полное представление об основных понятиях и главных результатах в теории кодов, корректирующих ошибки. Эти главы могут быть положены в основу университетского курса лекций по теории кодирования.

В первой части книги дано подробное изложение нескольких традиционных и давно сложившихся направлений классической теории кодирования. К ним относятся линейные и циклические коды, оценки объема кода, декодирование некоторых кодов, описание интересных в том или ином смысле классов кодов и многое другое. Хотя этим направлениям уже посвящено несколько очень хороших учебников и монографий, в настоящей книге найдется достаточно много новых и интересных результатов, не вошедшие в эти издания. Во многих случаях изложение даже хорошо известных результатов дается с новой точки зрения, которая, как полагает автор, расширит кругозор читателя.

Вторая, большая часть книги включает в себя изложение результатов, которые слабо или вообще не затрагивались в учебной и монографической литературе по теории кодирования. К таким направлениям автор относит: декодирование кодов Рида-Маллера и отчасти кодов Рида-Соломона, весовой спектр линейного кода, квантовые и дизъюнктивные коды, приложения теории кодирования к криптографии такие, как совершенная секретность в полилинейных системах распределения ключей и стойкость некоторых известных кодовых систем открытого шифрования.

Как первая так и особенно вторая части включает в себе достаточно большое число оригинальных результатов автора.

Изложение является достаточно доступным, на это автор обращал особое внимание. В то же время читателю для понимания текста необходимо некоторые элементарные и общеизвестные знания из алгебры (линейная алгебра, конечные поля, группы, кольца, многочлены и т.п.), геометрии (метрика, евклидова сфера и ), а также и начальные знания по некоторым другим разделам математики в объеме примерно двух первых курсов математического факультета. Понятия более специального плана всегда имеют подробное определение и объяснение. Вместе с тем текст не всегда является очень легким для понимания. Это прежде всего относится к разделам, в которых изучаются достаточно сложные объекты.

Автор в течении нескольких лет читал лекции по отдельным разделам теории кодирования студентам и аспирантам Московского государственного университета им. М.В. Ломоносова.

Традиционно к теории кодирования относят весьма широкий круг исследований, тяготеющих к дискретной математике. Из этого широкого круга только весьма малая часть отражена в данной книге. В частности, не рассматриваются неравномерные, алгебро-геометрические, сверточные и некоторые другие коды. По всем упомянутым кодам изданы прекрасные монографии (см., например, [78], [83]). Естественно, автор во второй половине книги писал только о тех направлениях теории кодирования, к которым он имеет наиболь-

ший научный интерес.

Книга имеет не очень большое пересечение с известными автору книгами по теории кодирования. Даже прекрасная книга МакВильямс и Слоан "Теория кодов, исправляющих ошибки", [7] с очень большим охватом материала перекрывается с содержанием данной книге только в достаточно небольшой степени.

Следует особо сказать, что теория кодирования имеет множество приложений к практике, причем не только к технике передачи информации по каналам связи с шумами. Имеются самые неожиданные приложения, например, с помощью теории кодов можно построить, так называемую, полилинейную систему распределения ключей, свойства которой с одной стороны похожи на свойства системы Диффи-Хеллмана, а с другой обеспечивают совершенную секретность ключа, что не присуще системе Диффи-Хеллмана. Об этом подробно написано в главе 13.

По представлениям автора, теория кодирования является одним немногих инкубаторов, в котором возникают новые содержательные математические задачи в нескольких достаточно абстрактных направлениях математики: алгебры, теории чисел и геометрии. К примеру алгебро-геометрические коды, которые были открыты в конце 70-х годов прошлого столетия отечественным ученым В.Д. Гоппой (см. например, [25]), к настоящему времени превратилось в крупное направление математики, развивающееся на стыке алгебраической геометрии и теории кодирования [5].

# Глава 1

## Базовые понятия

Теория кодирования в узком смысле изучает расположения точек в различных метрических пространствах. Поэтому изложение собственно теории кодирования естественно начать с достаточно подробного описания метрических пространств, которые наиболее часто в ней изучаются.

### 1.1 Пространство Хемминга

#### 1.1.1 Метрика Хемминга

Мы рассматриваем конечное  $q$ -элементное множество  $X = \{a_0, \dots, a_{q-1}\}$ . Множество  $X^n$  состоит из всех  $n$ -ок ( $n$ -мерных векторов) с координатами из множества  $X$ . Очевидно,  $|X^n| = q^n$ . Элементы  $X^n$  будем обозначать полужирными начальными буквами латинского алфавита:  $\mathbf{a} = (a_0, \dots, a_n)$ ,  $\mathbf{b} = (b_0, \dots, b_n)$  и т.д.

На множестве  $X^n$  мы определим метрику Хемминга  $d(\cdot, \cdot)$  следующим образом:

$$d(\mathbf{a}, \mathbf{b}) = \text{числу чисел } j, \text{ для которых } a_j \neq b_j. \quad (1.1.1)$$

Как легко убедиться, функция  $d(\cdot, \cdot)$  действительно является метрикой в обычном понимании этого термина. В частности, для неё выполнено "неравенство треугольника":  $d(\mathbf{a}, \mathbf{b}) \leq d(\mathbf{a}, \mathbf{c}) + d(\mathbf{c}, \mathbf{b})$  для всех  $\mathbf{c} \in X^n$ . (Упражнение)

Пространство  $X^n$  вместе с метрикой  $d$  будем называть метрическим пространством Хемминга. Оно является одним из стандартных пространств, на котором рассматривается теория кодов, корректирующих ошибки.

#### Кодовое расстояние

Кодом  $\mathcal{K}$  называется произвольное подмножество элементов метрического пространства  $X^n$ .

**Определение 1.1.1** Кодовым расстоянием  $d = d(\mathcal{K})$  кода  $\mathcal{K}$  называется минимальное расстояние между двумя различными элементами (векторами) кода  $\mathcal{K}$ :

$$d(\mathcal{K}) = \min_{\substack{\mathbf{a}, \mathbf{b} \in \mathcal{K} \\ \mathbf{a} \neq \mathbf{b}}} d(\mathbf{a}, \mathbf{b}) \quad (1.1.2)$$

### 1.1.2 Линейный код

Обычно в качестве  $X$  рассматривается множество с какой-либо алгебраической структурой. В частности, в качестве  $X$  берётся конечное поле или конечное кольцо. Эта структура необходима для построения содержательной теории кодирования на пространстве  $X^n$ .

Мы начнем изучение, предположив, что  $X$  — конечное поле  $\mathbb{F}_q$ ,  $q = p^l$ , где  $p$  — простое число. В этом случае  $X^n$  можно рассматривать как  $n$ -мерное пространство над полем  $\mathbb{F}_q$ . Его мы будем обозначать через  $\mathbb{F}_q^n$ .

Интересным является случай  $q = 2$ . В этом случае пространство  $X^n$  называется двоичным линейным пространством Хемминга.

В то же время естественно рассматривать и более общий случай:  $X$  — это конечная группа или конечное кольцо. В частности, наиболее широко рассматривался случай, в котором  $X$  — кольцо вычетов по модулю 4 или в несколько более общем случае  $X$  — кольцо Гауа. Заметим, что почти все рассматриваемые далее определения (линейный и двойственный коды, вес и многие другие), очевидным образом могут быть введены и в подобных пространствах  $X$  или  $X^n$ .

**Определение 1.1.2** Произвольное подпространство пространства  $\mathbb{F}_q^n$  называем линейным кодом. Для него мы оставляем прежнее обозначение  $\mathfrak{K}$ .

Через  $k = \dim \mathfrak{K}$  мы обозначаем размерность линейного кода  $\mathfrak{K}$ . Пусть  $\omega = \{\omega_1, \dots, \omega_k\}$  — базис пространства  $\mathfrak{K}$ . В теории кодирования принято называть матрицу  $A = A(\mathfrak{K})$ , строками которой являются векторы  $\{\omega_1, \dots, \omega_k\}$ , порождающей матрицей кода  $\mathfrak{K}$ .

Любой вектор  $\mathbf{x}$  кода  $\mathfrak{K}$  может быть представлен в виде

$$\mathbf{x} = \mathbf{z}A, \quad (1.1.3)$$

где  $\mathbf{z}$  —  $k$ -мерный вектор пространства  $\mathbb{F}_q^k$ .

Если матрица  $A$  выписана в явном виде, то мы говорим, что код  $\mathfrak{K}$  задан порождающей матрицей  $A$ .

**Определение 1.1.3** Функция

$$wt(\mathbf{a}) = \text{число координат у вектора } \mathbf{a}, \text{ отличных от нуля}, \quad (1.1.4)$$

называется весом Хемминга или просто весом вектора  $\mathbf{a}$ .

Функция  $wt(\mathbf{a})$  является часто используемой в теории кодирования функцией. Например, с ее помощью упрощается вычисление кодового расстояния для линейных кодов  $\mathfrak{K} \subset \mathbb{F}_q^n$ .

**Лемма 1.1.1** Кодовое расстояние линейного кода  $\mathfrak{K} \subset \mathbb{F}_q^n$  равно минимальному весу вектора в линейном подпространстве  $\mathfrak{K}$ . Другими словами,

$$d(\mathfrak{K}) = \min_{\mathbf{a} \in \mathfrak{K}, \mathbf{a} \neq 0} wt(\mathbf{a}). \quad (1.1.5)$$

**Доказательство** непосредственно вытекает из очевидного равенства  $d(\mathbf{a}, \mathbf{b}) = wt(\mathbf{c})$ , где  $\mathbf{c} = \mathbf{a} - \mathbf{b} \in \mathfrak{K}$ .  $\square$

Таким образом, вместо изучения совокупности взаимных расстояний между парами векторов  $\mathbf{a}, \mathbf{b}$  (функции от двух аргументов) линейного кода достаточно рассмотреть совокупность весов ненулевых элементов линейного подпространства  $\mathfrak{K}$  (функции одного аргумента).

### 1.1.3 Двойственный код

В этом разделе мы изучаем линейные коды  $\mathcal{K} \subseteq \mathbb{F}_q^n$  над конечным полем  $\mathbb{F}_q$ ,  $q = p^l$ . Скалярное  $\langle \mathbf{x}, \mathbf{y} \rangle$  произведение в поле  $\mathbb{F}_q$  векторов  $\mathbf{x} = (x_1, \dots, x_n)$  и  $\mathbf{y} = (y_1, \dots, y_n)$  линейного пространства  $\mathbb{F}_q^n$  мы определим следующим образом

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \dots + x_n y_n. \quad (\text{все операции в поле } \mathbb{F}_q) \quad (1.1.6)$$

Два вектора  $\mathbf{x}, \mathbf{y}$  называются ортогональными, если  $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ .

**Определение 1.1.4 (Двойственный код)** Код  $\mathcal{K}^\perp$  образованный всеми векторами, которые являются ортогональными ко всем векторам кода  $\mathcal{K}$ , называется двойственным к коду  $\mathcal{K}$ .

Очевидно, что  $\mathcal{K}^{\perp\perp} = \mathcal{K}$ .

**Лемма 1.1.2** Код  $\mathcal{K}^\perp$  является линейным кодом над полем  $\mathbb{F}_q$  и имеет размерность  $n - k$ , где  $k = \dim \mathcal{K}$ .

**Доказательство.** Очевидно, что если векторы  $\mathbf{x}, \mathbf{y}$  ортогональны вектору  $\mathbf{a}$ , то их сумма с коэффициентами из  $\mathbb{F}_q$  также ортогональна  $\mathbf{a}$ . Отсюда, в частности, следует, что код  $\mathcal{K}^\perp$  состоит из всех векторов  $\mathbf{x}$ , которые ортогональны каждой строке проверочной матрицы  $A$  кода  $\mathcal{K}$ .

Другими словами, векторы  $\mathbf{x} \in \mathcal{K}^\perp$  являются решениями линейной системы однородных уравнений

$$\mathbf{x} A^T = 0, \quad (1.1.7)$$

где  $A^T$  — транспонированная матрица  $A$ .

Как хорошо известно [40], множество решений однородной системы линейных уравнений с  $n$  неизвестными (координаты вектора  $\mathbf{x}$ ) и  $k$  уравнениями (1.1.7) представляет собой линейное пространство размерности  $n - k'$ , если  $k'$  — ранг матрицы  $A$ . Ранг матрицы  $k \times n$  — матрицы  $A$  равен  $k$ , ибо ее строками, по определению, являются базисные векторы пространства  $\mathcal{K}$ .  $\square$

**Определение 1.1.5 (Проверочной матрицы кода  $\mathcal{K}$ )** Порождающая матрица  $(n - k) \times n$  — матрица  $B$  кода  $\mathcal{K}^\perp$  называется проверочной матрицей кода  $\mathcal{K}$ .

Подобное название объясняется тем, что для каждого вектора  $\mathbf{x}$  кода  $\mathcal{K}$  выполнено

$$\mathbf{x} B^T = 0. \quad (1.1.8)$$

В частности, произведение  $A \cdot B^T$  является нулевой  $k \times k$  — матрицей.

Соотношение (1.1.8) в теории кодирования принято рассматривать как набор из  $n - k$  проверок наложенных на координаты вектора  $\mathbf{x}$ . Каждая проверка, определяемая одной из строк матрицы  $B$ , является однородным линейным уравнением, связывающих координаты вектора  $\mathbf{x}$ .

Множество решений уравнения (1.1.8) совпадает с кодом  $\mathcal{K}$ . Имея в виду этот факт, говорят, что код  $\mathcal{K}$  определяется проверочной матрицей  $B$ .

**Теорема 1.1.1** *Предположим, что любые  $d - 1$  столбцов проверочной матрицы  $B$  линейно-независимы над полем  $\mathbb{F}_q$ .*

*Тогда кодовое расстояние  $d(\mathcal{K})$  кода  $\mathcal{K}$ , определяемого проверочной матрицей  $B$ , не меньше, чем  $d$ .*

*Если в дополнение выше выскзанного условия существует линейно-зависимый комплект из  $d$  столбцов проверочной матрицы  $B$ , то  $d(\mathcal{K}) = d$ .*

*Наоборот. Если код имеет кодовое расстояние не меньше, чем  $d$ , то любые  $d - 1$  столбцов его проверочной матрицы  $B$  являются линейно-независимыми.*

**Доказательство.** В виду леммы 1.1.5 достаточно показать, что вес любого ненулевого вектора  $\mathbf{x}$  кода  $\mathcal{K}$  не меньше  $d$ .

Предположим обратное, т.е. предположим, что существует кодовый вектор  $\mathbf{x}$ , вес которого меньше  $d$ . Так как  $\mathbf{x}B^T = 0$ , то комплект столбцов матрицы  $B$ , номера которых совпадают с номерами ненулевых координат вектора  $\mathbf{x}$ , является линейно-зависимым. Это противоречит условию теоремы. Поэтому  $d(\mathcal{K}) \geq d$ .

Предпоследнее и последнее утверждения теоремы очевидны.

□

Эта простая теорема очень широко используется. Обычно молчаливо предполагается, имея в виду теорему 1.1.1, что для построения линейного кода достаточно построить матрицу, у которой каждый комплект из  $d - 1$  столбцов является линейно-независимым.

В качестве примера применения теоремы 1.1.1 рассмотрим двоичный линейный код Хемминга. Проверочная матрица  $B_H$  этого кода имеет размеры  $m \times 2^m - 1$  и образована всеми ненулевыми столбцами  $\mathbf{a}^T$ ,  $\mathbf{a} \in \mathbb{F}_2^m$ , высоты  $m$  с координатами из поля  $\mathbb{F}_2$ . Число таких столбцов, очевидно, равно  $2^m - 1$ .

**Лемма 1.1.3** *Кодовое расстояние двоичного линейного кода Хемминга  $B_H$  с числом элементов  $2^n - m = 2^{n - \log_2(n+1)}$  (см. лемму 1.1.2) длины  $2^m - 1$  равно 3.*

**Доказательство.** Так как любые два столбца матрицы  $B_H$  различны, то они линейно-независимы над полем  $\mathbb{F}_2$ . Заметим, что это утверждение не верно для полей с числом элементов более, чем 2.

С другой стороны, сумма любых двух столбцов  $B_H$  является одним из столбцов  $B_H$ . Следовательно, эти три столбца являются линейно-зависимыми.

Из теоремы 1.1.1 следует утверждение леммы. □

Код Хемминга обладает рядом замечательных свойств, некоторые из которых мы будем рассматривать ниже.

Кроме кода Хемминга мы рассмотрим расширенный код Хемминга длины  $2^m$  с проверкой на четность. Проверочная матрица этого кода образована проверочной матрицей кода Хемминга, к которой добавлен нулевой столбец, а затем и строка, состоящая из единиц. Этот код, как нетрудно проверить, имеет кодовое расстояние 4, длину  $2^m$  и число информационных разрядов  $2^m - m - 1$ . (Упражнение)

#### 1.1.4 Пространство, образованное равновесными двоичными векторами

Обычно пространство из заголовка называют пространством Джонсона и обозначают символом  $J_{w,n}$ , где  $w$  — вес каждого вектора длины  $n$  этого пространства. Кодовое расстояние Хемминга между векторами  $\mathbf{a}$  и  $\mathbf{b}$  из  $J_{w,n}$  всегда четное и, очевидно, равно

$$d(\mathbf{a}, \mathbf{b}) = 2w - 2u, \quad (1.1.9)$$

где  $u$  — число  $j$  таких, что  $a_j = b_j = 1$ . Функцию  $j(\mathbf{a}, \mathbf{b}) = \frac{1}{2}d(\mathbf{a}, \mathbf{b})$  называют расстоянием Джонсона между векторами  $\mathbf{a}, \mathbf{b} \in J_{w,n}$ .

В пространстве Джонсона изучаются примерно те же задачи, что и в пространстве Хемминга.

## 1.2 Сфера $S^{n-1}$

Другим стандартным метрическим пространством, который мы будем подробно изучать в настоящей книге, является  $n-1$ -мерная сфера  $S^{n-1}$  в евклидовом пространстве  $\mathcal{R}^n$ . Чтобы охарактеризовать круг рассматриваемых далее задач, необходимо короткое введение. К нему мы и переходим.

### 1.2.1 Метрика на сфере

Рассмотрим  $n$ -мерное евклидово пространство  $\mathbf{R}^n$  со скалярным произведением

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \cdots + x_n y_n. \quad (1.2.1)$$

Нормой  $|\mathbf{x}|$  (или длиной) вектора  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{R}^n$  называется число  $|\mathbf{x}| = \sqrt{x_1^2 + \cdots + x_n^2} = \sqrt{(\mathbf{x}, \mathbf{x})}$ . Евклидова метрика  $\lambda(\mathbf{a}, \mathbf{b})$  на  $\mathbf{R}^n$  с помощью скалярного произведения определяется как обычно:

$$\lambda(\mathbf{x}, \mathbf{y}) = |\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}. \quad (1.2.2)$$

Очевидно, если  $\mathbf{x}, \mathbf{y} \in S^{n-1}$ , то

$$\lambda(\mathbf{x}, \mathbf{y}) = 2 - 2(\mathbf{x}, \mathbf{y}). \quad (1.2.3)$$

Множество точек евклидова пространства  $\mathbf{R}^n$ , находящихся на расстоянии  $r$  от начала координат, называется  $(n-1)$ -мерной евклидовой сферой радиуса  $r$ . Для ее обозначения используется символ  $S^{n-1}(r)$ . Сферу радиуса  $r = 1$  обозначаем через  $S^{n-1}$ .

Очень похожим образом определяется  $(n-1)$ -мерная унитарная сфера  $U^{n-1}(r)$  радиуса  $r$  в унитарном пространстве  $\mathbf{C}^n$ . Вместо (1.2.1) в качестве билинейной формы  $(\mathbf{x}, \mathbf{y})$  на  $\mathbf{C}^n$  используется форма

$$(\mathbf{x}, \mathbf{y})_{\mathbf{C}} = (\mathbf{x}, \mathbf{y}) = x_1 \bar{y}_1 + \cdots + x_n \bar{y}_n, \quad (1.2.4)$$

где "черта" обозначает сопряжение в  $\mathbf{C}$ , т.е.  $\overline{a + ia'} = a - ia'$ ,  $a, a' \in \mathbf{R}$ , где  $i = \sqrt{-1}$ . Нормой  $|\mathbf{x}|$  (или длиной) вектора  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{C}^n$  называется число  $|\mathbf{x}| = \sqrt{|x_1|^2 + \cdots + |x_n|^2} = \sqrt{(\mathbf{x}, \mathbf{x})_{\mathbf{C}}}$ , где  $x_j = x'_j + ix''_j$  и  $|x_j| = \sqrt{x'^2_j + x''^2_j}$ .

Унитарная метрика  $\lambda_C$  определяется точно также как метрика  $\lambda$  (см. первое равенство в (1.2.2)). Унитарная сфера  $U^{n-1}(r)$  радиуса  $r$  — это множество точек пространства  $C^n$ , отстоящих в метрике  $\lambda_C$  от начала координат на расстояние  $r$ . Таким образом,

$$U^{n-1}(r) = \{\mathbf{x}; |\mathbf{x}| = \lambda_C(0, \mathbf{x}) = r\}. \quad (1.2.5)$$

Если  $\mathbf{x}, \mathbf{y} \in U^{n-1}(r)$ , то расстояние  $\lambda_C(\mathbf{x}, \mathbf{y})$  между точками  $\mathbf{x}, \mathbf{y}$  может быть выражена через их скалярное произведение  $(\mathbf{x}, \mathbf{y})_C$  следующим образом

$$\lambda_C(\mathbf{x}, \mathbf{y}) = \sqrt{2r^2 - 2\Re(\mathbf{x}, \mathbf{y})_C}, \quad (1.2.6)$$

где  $\Re z$  — действительная часть комплексного числа  $z$ . Действительно,

$$\lambda_C^2(\mathbf{x}, \mathbf{y}) = (\mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y}) = |\mathbf{x}|^2 + |\mathbf{y}|^2 - (\mathbf{x}, \mathbf{y})_C - (\mathbf{y}, \mathbf{x})_C = 2r^2 - 2\Re(\mathbf{x}, \mathbf{y})_C, \quad (1.2.7)$$

Как легко убедиться, метрическое пространство  $C^n$  изометрически вкладывается в евклидово пространство  $R^{2n}$  удвоенной размерности с помощью покоординатного отображения (овеществления)  $x' + ix'' \rightarrow (x', x'')$  его точек в точки  $R^{2n}$ . И наоборот, евклидово пространство  $R^{2n}$  четной размерности изометрически вкладывается в унитарное пространство  $C^n$  с помощью отображения  $(x', x'') \rightarrow x' + ix''$  пар координат  $R^{2n}$  в отдельные координаты пространства  $C^n$ . Таким образом, сферы  $U^{n-1}$  и  $S^{2n-1}$  — являются метрически одинаковыми пространствами.

## 1.2.2 Ортогональные и унитарные преобразования

Матрица  $A$  (см. [39], стр. 162), является ортогональной (унитарной), тогда и только тогда, когда выполнено следующее соотношение

$$A^T A = E, \text{ (ортогональная матрица)}, \quad U^* U = E \text{ (унитарная матрица)}, \quad (1.2.8)$$

где  $A^T$  — транспонированная матрица  $A$ ,  $U^* = \bar{U}^T$  — сопряженная и транспонированная матрица  $U$  и  $E$  — единичная матрица. Заметим, что соотношение (1.2.8) означает, что строки матриц  $A$  и  $U$  имеют норму равную 1 и ортогональны относительно скалярного произведения евклидова и унитарного пространств, соответственно.

Мы будем рассматривать действие на сферах  $S^{n-1}$  и  $U^{n-1}$  ортогональных и унитарных преобразований пространств  $R^n$  и  $C^n$ , которые реализуются с помощью ортогональных и унитарных матриц  $A$  и  $U$ . Важнейшим свойством подобных преобразований является "сохранение" (инвариантность) евклидовой или унитарной метрики  $\lambda$  относительно их действия. А именно, если  $A$  ( $U$ ) — ортогональная (унитарная) матрица, то

$$\lambda(\mathbf{x}, \mathbf{y}) = \lambda(\mathbf{x}A, \mathbf{y}A) \quad (\lambda_C(\mathbf{x}, \mathbf{y}) = \lambda_C(\mathbf{x}U, \mathbf{y}U)). \quad (1.2.9)$$

Как легко проверить, произведение ортогональных (унитарных) матриц является ортогональной (унитарной) матрицей, т.е. множество всех ортогональных или унитарных матриц является группой, обозначаемой через  $O(n)$  и  $U(n)$ , соответственно.

Элементы унитарной группы  $U(n)$  можно преобразовать (отобразить) в ортогональные матрицы удвоенной размерности (овеществить) с помощью следующего приема.



Рассмотрим отображение  $\varphi$  элементов поля  $\mathbf{C}$  в группу матриц вида  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ :

$$\varphi : a + ib \rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \quad (1.2.10)$$

Можно проверить, что отображение  $\varphi$  является изоморфизмом между полем  $\mathbf{C}$  и полем, образованным матрицами вида  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ . А именно,

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(a+b) = \varphi(a) + \varphi(b), \quad a, b \in \mathbf{C}. \quad (1.2.11)$$

Пусть  $U = (a_{i,j})_{i,j=1,\dots,n}$  — унитарная матрица. Отобразим каждый ее элемент  $a_{i,j}$  в  $2 \times 2$ -матрицу с помощью отображения  $\varphi$ . В результате получим  $2n \times 2n$ -матрицу  $\widehat{U}$ , которая, как нетрудно убедиться, является ортогональной. (Упражнение)

Очевидно,  $\widehat{U}\widehat{U}' = \widehat{UU}'$ . Поэтому отображение  $\varphi : U \rightarrow \widehat{U}$  является гомоморфизмом группы  $U(n)$  в группу  $O(2n)$ . В частности, образ  $\varphi(U(n))$  группы  $U(n)$  является подгруппой группы  $O(2n)$ .

Более того, можно показать, что  $\varphi(U(n)) \neq O(2n)$  при  $n > 1$ , т.е. группа  $O(2n)$  "богаче" группы  $\varphi(U(n))$ .

### 1.2.3 Орбитный код

Возвращаемся к обзору теоретико-кодовых задач, рассматриваемым в книге.

Кодом  $\mathfrak{K}$  на единичной сфере  $S^{n-1}$  называется конечное множество точек, расположенных на  $S^{n-1}$ . Расстоянием между точками  $\mathbf{x}, \mathbf{y} \in S^{n-1}$  является евклидово расстояние, определенное в (1.2.2). Кодовое расстояние  $\lambda(\mathfrak{K})$  кода  $\mathfrak{K}$  — это минимальное расстояние между парами его точек:

$$\lambda(\mathfrak{K}) = \min_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}, \mathbf{x} \neq \mathbf{y}} \lambda(\mathbf{x}, \mathbf{y}). \quad (1.2.12)$$

Пусть  $G$  — подгруппа группы  $O(n)$ , возможно, бесконечная и  $\mathbf{a}$  — точка на сфере  $S^{n-1}$  такая, что множество  $\mathfrak{K} = \{\mathbf{a}g | g \in G\} \subset S^{n-1}$  имеет конечное число элементов. Отметим, что последнее свойство выполнено, если  $G$  — конечная группа.

**Определение 1.2.1** Орбитным кодом  $\mathfrak{K} = \mathfrak{K}(G, \mathbf{a})$  с начальной точкой  $\mathbf{a}$  называется множество  $\mathfrak{K} = \{\mathbf{a}g | g \in G\} \subset S^{n-1}$  точек на  $O(n)$ . Т.е.  $\mathfrak{K}(G, \mathbf{a})$  — это орбита, порожденная действиями элементов группы  $G$  на начальную точку  $\mathbf{a}$ .

Отметим, что в качестве начальной точки орбитного кода  $\mathfrak{K}(G, \mathbf{a})$  можно взять любой его элемент. Другими словами,  $\mathfrak{K}(G, \mathbf{a}) = \mathfrak{K}(G, \mathbf{b})$ , если  $\mathbf{b} \in \mathfrak{K}(G, \mathbf{a})$ . (Упражнение)

Мы обозначаем через  $St_{\mathbf{a}}$  стабилизатор точки  $\mathbf{a}$  в группе  $G$ , т.е.  $St_{\mathbf{a}} = \{g | (g \in G) \& (\mathbf{a}g = \mathbf{a})\}$ . Очевидно, что  $St_{\mathbf{a}}$  — подгруппа группы  $G$  и  $St_{\mathbf{b}} = g^{-1}St_{\mathbf{a}}g$ , если  $\mathbf{b} = \mathbf{a}g$ . Таким образом, все подгруппы  $St_{\mathbf{b}}$ ,  $\mathbf{b} \in \mathfrak{K}$ , сопряжены в группе  $G$ .

Если группа  $G$  — конечная, то как легко установить, (Упражнение)

$$|\mathfrak{K}| = \frac{|G|}{|St_{\mathbf{a}}|}. \quad (1.2.13)$$

Орбитный код является аналогом линейного кода (см. раздел 1.1.2). В частности, для весовой функции  $wt(\mathbf{x})$  (см. (1.1.3)) имеется его аналог — функция  $\varpi(\mathbf{x})$ .

**Определение 1.2.2** Весовой функцией орбитного кода  $\mathfrak{K}(G, \mathbf{a})$  называется функция

$$\varpi_{\mathbf{a}}(\mathbf{x}) = \varpi(\mathbf{x}) = \lambda(\mathbf{a}, \mathbf{x}), \mathbf{x} \in \mathfrak{K}(G, \mathbf{a}). \quad (1.2.14)$$

Также как в случае линейного кода расстояние между точками  $\mathbf{x} = \mathbf{a}g$ ,  $\mathbf{y} = \mathbf{a}g'$ ,  $g, g' \in G$ , можно выразить с помощью функции  $\varpi$  следующим образом:

$$\lambda(\mathbf{x}, \mathbf{y}) = \lambda(\mathbf{a}g, \mathbf{y}) = \lambda(\mathbf{a}, \mathbf{y}g^{-1}) = \varpi(\mathbf{y}g^{-1}) = \varpi(\mathbf{a}g'g^{-1}). \quad (1.2.15)$$

**Лемма 1.2.1** Кодовое расстояние орбитного кода  $\mathfrak{K} = \mathfrak{K}(G, \mathbf{a})$  равно минимальному ненулевому весу кодового вектора  $\varpi(\mathbf{x})$ ,  $\mathbf{x} \in \mathfrak{K}$ , отличного от  $\mathbf{a}$ . Другими словами,

$$\lambda(\mathfrak{K}) = \min_{\mathbf{x} \in \mathfrak{K}, \mathbf{x} \neq \mathbf{a}} \varpi(\mathbf{x}). \quad (1.2.16)$$

**Доказательство** непосредственно вытекает из (1.2.15).  $\square$

Следовательно, вместо рассмотрения совокупности взаимных расстояний между парами векторов  $\mathbf{a}, \mathbf{b}$  (функции от двух аргументов) достаточно рассмотреть совокупность весов ненулевых элементов орбитного кода  $\mathfrak{K}$  (функции одного аргумента).

### 1.3 Метрическое вложение кода в пространстве Хемминга на единичную сферу евклидова пространства

Линейный код  $\mathfrak{K} \subset \mathbb{F}_p^n$  в пространстве Хемминга можно превратить в орбитный, отображая все его элементы на единичную сферу  $S^{n'-1}$  с подходящим значением  $n'$ . Основная проблема, которая возникает при этом, состоит в согласовании метрики на  $S^{n'-1}$  с метрикой Хемминга на  $\mathbb{F}_p^n$  и сохранение алгебраической структуры кода  $\mathfrak{K}$  (его линейности) с некоторой новой операцией сложения точек образа кода  $\mathfrak{K}$ , которая действует на  $S^{n'-1}$ . Эту новая операция должна быть реализована с помощью действия на образе  $\mathfrak{K}$  некоторой группы  $G$  отображений со следующими свойствами.

**Определение 1.3.1** [Изоморфное вложение кода  $\mathfrak{K} \leq \mathfrak{G} = X^n$  в орбитный код]

Предположим, что пространство Хемминга  $X^n$  является группой  $\mathfrak{G}$  с групповой операцией, которую мы обозначаем символом  $\cdot$ , и единичным элементом  $\mathbf{e}$ . Пусть  $\mathfrak{K}$  — подгруппа группы  $(\mathfrak{K} \leq X^n)$ . Например, если  $X^n$  —  $n$ -мерное линейное пространство над полем  $\mathbb{F}_p$  (в данном случае групповой операцией  $\cdot$  в  $G$  является покомпонатное сложение ее векторов), тогда  $\mathfrak{K}$  — обычный линейный над  $\mathbb{F}_p$  код.

Пусть  $\pi$  — взаимно-однозначное отображение пространства  $X^n$  на сферу  $S^{n'-1}$ .

Предположим, что множество  $\pi(\mathfrak{K}) \subset S^{n'-1}$  является орбитным кодом, т.е.  $\pi(\mathfrak{K})$  — орбита с начальным вектором  $\pi(\mathbf{e}) \in S^{n'-1}$ , порожденная некоторой группой  $G$  (не обязательно конечной) ортогональных преобразований сферы  $S^{n'-1}$  в себя (см. определение 1.2.1).

Предположим, что стабилизатор  $St_{\mathbf{e}}$  точки  $\mathbf{e}$  в группе  $G$  является нормальной подгруппой группы  $G$ . Пусть  $\pi(\mathbf{x}) = \pi(\mathbf{e})g$ ,  $\pi(\mathbf{y}) = \pi(\mathbf{e})g'$  и  $\pi(\mathbf{x} \cdot \mathbf{y}) = \pi(\mathbf{e})g''$ .

Если для всех  $\mathbf{x}, \mathbf{y} \in \mathfrak{G}$  группа  $G$  обладает следующим свойством

$$g \cdot g' \in St_{\mathbf{e}} g'', \quad (1.3.1)$$

тогда мы говорим, что орбитный код  $\pi(\mathfrak{K})$  реализует изоморфное вложением подгруппы  $\mathfrak{K}$  группы  $\mathfrak{G} = X^n$  на единичную сферу  $S^{n'-1}$ .

Отметим, что если стабилизатор  $St_e$  точки  $e$  в группе  $G$  тривиальный, то соотношение (1.3.1) превращается в равенство  $g \cdot g' = g''$ . Последнее соотношение определяет изоморфизм  $\tau$  группы  $\mathfrak{G}$  и группы преобразований  $G$  следующим образом

$$\tau : \mathbf{x} \leftrightarrow g, \text{ если } \pi(\mathbf{x}) = \pi(e)g. \quad (1.3.2)$$

Если же стабилизатор  $St_e \trianglelefteq G$  не является тривиальным, то, как нетрудно увидеть, отображение (1.3.2) определяет изоморфизм групп  $\mathfrak{K}$  и факторгруппы  $G/St_e$  (Упражнение).

Таким образом, соотношение (1.3.1) превращает групповой код  $\pi(\mathfrak{K})$  в группу, изоморфную группе  $\mathfrak{G}/St_e$ . Это свойство объясняет название изоморфное вложение группы  $\mathfrak{K}$  в орбитный код  $\pi(\mathfrak{K})$ , расположенный на единичной сфере.

**Определение 1.3.2** (Метрическое вложение кода  $\mathfrak{K} \subseteq X^n$  (подмножества метрического пространства Хемминга) на единичную евклидову сферу  $S^{n'-1}$ .)

Множество точек  $\hat{\mathfrak{K}} \subset S^{n'-1}$ ,  $|\hat{\mathfrak{K}}| = |\mathfrak{K}|$ , (вообще говоря,  $n' \neq n$ , обычно  $n'$  кратно  $n$ ) называется метрическим вложением кода  $\mathfrak{K} \subseteq X^n$  на единичную евклидову сферу  $S^{n'-1}$ , если существуют взаимно-однозначное отображение  $f : \mathfrak{K} \rightarrow \hat{\mathfrak{K}}$  и строго возрастающая функция  $\rho$  такие, что

$$\lambda(f(\mathbf{x}), f(\mathbf{y})) = \rho(d(\mathbf{x}, \mathbf{y})), \quad (1.3.3)$$

где  $d(\cdot, \cdot)$  и  $\lambda(\cdot, \cdot)$  — расстояния Хемминга на  $X^n$  и евклидово расстояние на  $S^{n'-1}$ , соответственно.

Совершенно также мы определим метрическое вложение кода  $\mathfrak{K} \subseteq X^n$  (подмножества метрического пространства Хемминга) на единичную унитарную сферу  $U^{n'-1}$ .

Метрическое вложение мы называем изометрическим, если в равенстве (1.3.3) функция  $\rho$  имеет вид  $\rho(x) = cx$ ,  $c > 0$ .

**Определение 1.3.3** (Изоморфное метрическое вложение кода  $\mathfrak{K} \subseteq X^n$  на единичную евклидову сферу  $S^{n'-1}$ .)

Как и в определении 1.3.1, предположим, что код  $\mathfrak{K} \subseteq \mathfrak{G} = X^n$  является подгруппой группы  $\mathfrak{G}$ . Множество точек  $\hat{\mathfrak{K}} = \pi(\mathfrak{K})$ ,  $|\hat{\mathfrak{K}}| = |\mathfrak{K}|$ , сферы  $S^{n'-1}$  называется изоморфным метрическим вложением группы  $\mathfrak{G}$  на сферу  $S^{n'-1}$ , если оно одновременно является метрическим вложением и орбитным кодом, который реализует изоморфное вложение группы  $\mathfrak{G}$  на сферу  $S^{n'-1}$ .

Изоморфное метрическое вложение группы  $\mathfrak{G}$  на сферу  $S^{n'-1}$   $\hat{\mathfrak{K}}$  называется изоморфным изометрическим вложением, если оно является не только изоморфным, но и изометрическим вложением кода  $\mathfrak{K}$ .

Заметим, что в определении 1.3.2 вместо кода  $\mathfrak{K}$  можно рассматривать пространство Хемминга  $X^n$ , т.е. заменить в 1.3.2 множество  $\mathfrak{K}$  на множество  $X^n$ . В этом случае речь идет о метрическом вложении на евклидову сферу пространства Хемминга  $X^n$ .

Таким образом, метрическое вложение пространства Хемминга  $X^n$ , обозначаемое далее символом  $\mathcal{Y}$ , обладает следующим свойством:  $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x}', \mathbf{y}')$  тогда и только тогда, когда  $\lambda(\pi(\mathbf{x}), \pi(\mathbf{y})) = \lambda(\pi(\mathbf{x}'), \pi(\mathbf{y}'))$  и наоборот. Это свойство, не совсем точно выражаясь, позволяет утверждать, что взаимные расположения точек в метрических пространствах  $X^n$  и  $\widehat{X}^n$  являются подобными.

Естественно рассматривать такие вложения, для которых размерность  $n' = n'(n)$  была бы минимальной.

Кроме того для некоторых  $n'$ , а именно, тех значений  $n'$ , для которых существуют метрические вложения  $X^n$  на единичную сферу  $S^{n'-1}$ , естественно рассмотреть те метрические вложения, которые максимизируют евклидово расстояние  $\lambda(f(\mathbf{x}), f(\mathbf{y}))$  между образами  $\pi(\mathbf{x}), \pi(\mathbf{y})$  ближайших векторов  $\mathbf{x}, \mathbf{y}$  из  $X^n$ . Другими словами, мы рассматриваем число

$$\lambda_n(n') = \max \lambda(\pi(\mathbf{x}), \pi(\mathbf{y})) \quad (1.3.4)$$

где  $d(\mathbf{x}, \mathbf{y}) = 1$  и максимум берется по всем метрическим вложениям  $\mathcal{Y}$  пространства Хемминга  $X^n$  на единичную сферу  $S^{n'-1}$ . Число  $\lambda_n(\mathcal{Y}) = \lambda(\pi(\mathbf{x}), \pi(\mathbf{y})), d(\mathbf{x}, \mathbf{y}) = 1$ , для заданного вложения  $\mathcal{Y}$  будем называть диаметром изометрического вложения  $\mathcal{Y}$  пространства  $\mathbb{F}_q^n$  на сферу  $S^{n'-1}$ .

Следует отметить, что понятие метрическое вложение является достаточно естественным с физической точки зрения, ибо, в конечном итоге, в физическом мире любое макрособытие происходит в метрическом пространстве, которое в большинстве случаев считают евклидовым. Таким образом, по нашему мнению любое пространство Хемминга, в конечном итоге, в физическом пространстве реализуется как некоторое множество векторов (сигналов) евклидового пространства.

К этому стоит добавить, что использование метрического вложения позволяет получать и некоторые полезные результаты, относящиеся к пространству Хемминга, в частности, позволяет рассматривать его как код на сфере  $S^{n'-1}$ . Последнее свойство позволяет, например, получать оценки объема кодов в пространстве Хемминга, рассматривая их как коды на сфере  $S^{n'-1}$  с евклидовой метрикой.

## Вложения одномерные пространства Хемминга на евклидову сферу

Построим функцию  $\pi$ , которая реализует одно из возможных изометрических вложений  $\mathcal{Y}_1$  одномерного пространства Хемминга  $X = \{0, \dots, q-1\}$  на унитарную сферу  $U^{n'-1}$ ,  $n' = q-1$ . Элементы множества  $X$  будем трактовать как элементы кольца  $\mathbf{Z}_q$  вычетов по mod  $q$ .

Каждому элементу  $a \in X$  сопоставим в соответствие  $q-1$ -мерный вектор

$$\pi(a) = \frac{1}{\sqrt{q-1}} \left( \exp\left(\frac{2\pi i a}{q}\right), \exp\left(\frac{2\pi i 2a}{q}\right), \dots, \exp\left(\frac{2\pi i (q-1)a}{q}\right) \right) \quad (1.3.5)$$

на унитарной сфере  $U^{q-2} \subset \mathbf{C}^{p-1}$ .

Очевидно,

$$(\pi(a), \pi(b)) = \frac{1}{q-1} \sum_{k=1}^{p-1} \exp\left(\frac{2\pi i (a-b)k}{q}\right) = \begin{cases} \frac{-1}{q-1}, & \text{если } a \neq b; \\ 1, & \text{если } a = b, \end{cases} \quad (1.3.6)$$

Следовательно,

$$\lambda^2(\pi(a), \pi(b)) = |a - b, a - b|^2 = 2 - 2\Re(a, b) = \begin{cases} \frac{2q}{q-1}, & \text{если } a \neq b; \\ 0, & \text{если } a = b. \end{cases} \quad (1.3.7)$$

где  $\Re x$  — вещественная часть комплексного числа  $x$ .

Таким образом, если в качестве функции  $\rho$  в (1.3.3) взять функцию  $\rho(x) = \frac{q-1}{2q}x$ , то мы получим изометрическое вложение одномерного пространства Хемминга на унитарную сферу  $U^{q-2}$   $q-1$ -мерного унитарного пространства ( $n' = q-1$ ).

Как следует из результатов раздела 1.2.1, это изометрическое вложение одномерного пространства Хемминга на унитарную сферу  $U^{q-2}$  одновременно является изометрическим вложением  $\mathcal{Y}_1$  одномерного пространства Хемминга на  $2(q-1)$ -мерную евклидову сферу  $S^{2q-3}$ . Диаметр этого вложения равен  $\lambda_1(\mathcal{Y}_1) = \sqrt{\frac{2q}{q-1}}$  (см. (1.3.7)).

Таким образом, в одномерном случае рассмотренное изометрическое вложение, обозначаемое через  $\mathcal{Y}_1$ , позволяет реализовать метрическое пространство Хемминга  $X$ ,  $q > 2$ , как пространство, образованное  $q$  точками, которые расположены на единичной сфере в унитарном пространстве размерности  $q-1$  или, что эквивалентно, как множество точек на единичной сфере  $2(q-1)$ -мерного евклидова пространства. Этот вид вложения, как будет видно ниже, хотя и не обеспечивает минимальную размерность евклидова пространства, в которое производится вложение, но имеет ряд полезных свойств. В частности, в некоторых случаях ( $X$  — циклическая группа) он позволяет реализовать изоморфное изометрическое вложение одномерного пространства Хемминга  $X$  на орбитный код  $\hat{X}$ .

В качестве, упомянутого выше, орбитного кода  $\hat{X}$ , реализующего изометрическое вложение, возьмем орбитный код  $\mathfrak{K}(G, \mathbf{a})$ , порожденный группой  $G$ , состоящей из всех диагональных матриц вида

$$g_a = \text{diag} \left( \exp \left( \frac{2\pi i a}{q} \right), \exp \left( \frac{2\pi i 2a}{q} \right), \dots, \exp \left( \frac{2\pi i (q-1)a}{q} \right) \right), \quad a \in \mathbf{Z}_q.$$

В качестве начального вектора  $\mathbf{a}$  возьмем вектор  $\mathbf{a} = \frac{1}{\sqrt{q-1}}(1, \dots, 1) \in U^{q-2}$ . Очевидно, орбитный код  $\mathfrak{K}(G, \mathbf{a})$  обеспечивает требуемое изоморфное метрическое вложение для всех целых чисел  $q$ .

Если  $X$  — циклическая группа, то рассмотренное выше вложение  $\mathcal{Y}_1$ , очевидно, является метрическим изоморфным вложением группы  $X$  на поверхность унитарной сферы  $U^{q-2}$ .

Отобразим теперь унитарное пространство  $\mathbf{C}^{q-1}$  в евклидово пространство удвоенной размерности с помощью отображения  $\varphi$  (см. (1.2.10)). Как было показано в разделе 1.2.2 отображение  $\varphi$  позволяет изоморфно отобразить группу  $G$  в группу  $G'$  ортогональных  $2(q-1) \times 2(q-1)$ -матриц. Группа  $G'$  и начальный вектор  $\mathbf{a}' = \frac{1}{\sqrt{q-1}}(\varphi(1), \dots, \varphi(1)) = \frac{1}{\sqrt{q-1}}(1, 0, 1, 0, \dots, 1, 0) \in S^{2(q-1)-1}$  определяют орбитный код  $\mathfrak{K}(G', \mathbf{a}')$  на единичной евклидовой сфере  $S^{2(q-1)-1}$ . Заметим, что группа  $G'$  является группой диагональных матриц, на диагонали которых расположены  $2 \times 2$ -матрицы вида  $\varphi(\exp(\frac{2\pi i ab}{q}))$ ,  $a, b \in \mathbf{Z}_q$ .

Так как группы  $G$  и  $G'$  изоморфны, а отображение  $\varphi$  сохраняет метрику, то орбитные коды  $\mathfrak{K}(G, \mathbf{a}) \subset U^{q-2}$  и  $\mathfrak{K}(G', \mathbf{a}') \subset S^{2(q-1)-1}$  эквивалентны в естественном понимании этого термина, т.е. код  $\mathfrak{K}(G', \mathbf{a}')$  реализует изоморфное метрическое вложение циклической группы  $X$ , на которой задана метрика Хемминга, на поверхность единичной сферы  $S^{2(q-1)-1}$ .

В двоичном случае ( $p = 2$ ) вложение  $\mathcal{U}_1$  позволяет вложить пространство Хемминга  $\mathbb{F}_2$  на сферу одномерного евклидова пространства, ибо корнями второй степени из единицы являются вещественные числа.

### Универсальный способ вложения одномерного пространства Хемминга

Отметим, что существуют универсальный способ, обозначаемый далее через  $\mathcal{U}$ , метрического вложения одномерного пространства Хемминга  $X$ ,  $|X| = q$ , на единичную сферу  $S^{q-2}$   $q - 1$ -мерного евклидова пространства.

В качестве образов  $\pi(x)$  точек  $x \in X$  возьмем вершины правильного симплекса, вписанного в единичную сферу  $q - 1$ -мерного евклидова пространства. Например, в качестве вершин симплекса можно взять точки вида  $\mathbf{a}_j = e_j - \frac{1}{q} \sum_{s=1}^q e_s$ ,  $j = 1, \dots, q$ , где  $e_j = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbf{R}^q$  (единица на  $j$ -ом месте). Это множество точек, расположено на  $q - 1$ -мерной гиперплоскости  $x_1 + \dots + x_q = 0$ , т.е. его элементы можно рассматривать как точки, лежащие в  $q - 1$ -мерном евклидовом пространстве. Очевидно, длины всех векторов  $\mathbf{a}_j$  одинаковы. Одинаковы и евклидовы расстояния между парами элементов множества  $\{\mathbf{a}_1, \dots, \mathbf{a}_q\}$ . Поэтому точки этого множества после их нормирования и сдвига можно взять в качестве вершин правильного симплекса, расположенного в шаре с центром в нулевой точке евклидова пространства  $\mathbf{R}^{q-1}$ . Это вложение является изометрическим вложением пространства  $X$  на единичную сферу  $S^{q-1}$   $q - 1$ -мерного евклидова пространства. Это вложение мы будем обозначать через  $\mathcal{U}$ .

У метрического вложения  $\mathcal{U}$  отсутствует какая-либо алгебраическая структура. Вместе с тем довольно просто найти конечную группу  $G$  ортогональных преобразований, с помощью которой может быть реализовано изоморфное изометрическое вложение произвольной группы  $X$  на сферу  $S^{q-2}$ , т.е. изометрически отобразить группу  $X$  в орбитный код  $\pi(X)$ .

**Теорема 1.3.1** *Предположим, что одномерное пространство Хемминга  $X$  является конечной группой  $\mathfrak{G}$  порядка  $q$  с групповой операцией  $+$  (сложение).*

*Тогда существует изоморфное изометрическое вложение  $\pi$  пространства Хемминга  $X$  на евклидову сферу  $S^{q-2}$  (см. определения 1.3.1 и 1.3.3).*

**Доказательство.** Рассмотрим ортонормированный базис  $\omega = \{\omega_1, \dots, \omega_q\}$   $q$ -мерного евклидова пространства  $\mathbf{R}^q$ , где  $\omega_1 = \frac{1}{\sqrt{q}}(1, \dots, 1)$ . На остальные векторы  $\omega_j$ ,  $j > 1$ , базиса мы не накладываем никаких ограничений. Пусть

$$\mathbf{R}^q = L_1 \oplus L_{q-1} \quad (1.3.8)$$

— разложение  $q$ -мерного пространства  $\mathbf{R}^q$  в прямую сумму одномерного пространства  $L_1$ , натянутого на вектор  $e_1 + \dots + e_q = \sqrt{q}\omega_1$ , и  $q - 1$ -мерного пространства  $L_{q-1}$  с базисом  $\omega_2, \dots, \omega_q$ .

В базисе  $\omega$ , очевидно, векторы  $\mathbf{a}_j$  будут иметь вид  $\alpha'_j = (0, \alpha_2^{(j)}, \dots, \alpha_q^{(j)}) = \mathbf{a}_j A$ , где  $A$  — ортогональная матрица перехода от ортонормированного базиса  $e = \{e_1, \dots, e_q\}$  к ортонормированному базису  $\omega$ .

Пусть  $\alpha_j = (\alpha_2^{(j)}, \dots, \alpha_q^{(j)})$ . Очевидно, что  $(\mathbf{a}_j, \mathbf{a}_j) = (\alpha_j, \alpha_j) = \frac{q-1}{q}$ . Поэтому все  $q - 1$ -мерные векторы  $\alpha_j$  лежат на евклидовой сфере радиуса  $\sqrt{\frac{q-1}{q}}$ , а все векторы

$$\mathbf{b}_j = \sqrt{\frac{q}{q-1}} \alpha_j \quad (1.3.9)$$

— на единичной сфере  $S^{q-2}$ . Очевидно,  $(\mathbf{b}_i, \mathbf{b}_j) = \frac{q}{q-1}(\alpha_i, \alpha_j) = \frac{q}{q-1}(e_i, e_j) = -\frac{1}{q-1}$ . Отсюда следует, что евклидово расстояние  $\lambda(\mathbf{b}_i, \mathbf{b}_j) = \sqrt{(\mathbf{b}_i - \mathbf{b}_j, \mathbf{b}_i - \mathbf{b}_j)} = \sqrt{2 - 2(\mathbf{b}_i, \mathbf{b}_j)}$  между векторами  $\mathbf{b}_i, \mathbf{b}_j$ ,  $i \neq j$ , равно  $\sqrt{\frac{2q}{q-1}}$ .

Таким образом, мы представили в явном виде эквидистантное множество  $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_q\}$  точек сферы  $S^{q-2}$ , который реализует изометрическое вложение пространства Хемминга  $X$ . Для того чтобы завершить доказательство теоремы достаточно представить  $\mathcal{B}$  в виде орбитного кода.

Предположим, что  $G$  — конечная группа ортогональных матриц, действующих на евклидовом пространстве  $\mathbf{R}^q$  и  $g \in G$  и  $L_1$  и  $L_{q-1}$  — ее инвариантные подпространства размерности 1 и  $q-1$ , соответственно. Последнее означает, что если  $\mathbf{a} \in L_j$ ,  $j = 1, q-1$ , то  $\mathbf{a}g \in L_j$  для всех  $g \in G$ .

Будем полагать, что  $G$  является точным представлением некоторой абстрактной группы  $\mathfrak{G}$ . В рассматриваемом случае представление  $G$  является приводимым. Из общей теории следует (см. например, [15]), что в некотором ортогональном базисе  $\omega = \{\omega_1, \dots, \omega_q\}$  каждую матрицу  $g \in G$  можно представить в виде

$$g(\mathfrak{g}) = \begin{pmatrix} g_1(\mathfrak{g}) & 0 \\ 0 & g_{q-1}(\mathfrak{g}) \end{pmatrix}, \quad (1.3.10)$$

где  $g_1$  —  $1 \times 1$ —матрица, а  $g_{q-1}$  —  $q-1 \times q-1$ —матрица с вещественными элементами, которые действуют на пространствах  $L_1$  и  $L_{q-1}$ . Будем обозначать через  $G_{q-1}$  группу  $q-1 \times q-1$ —матриц, порожденную матрицами всеми  $g_{q-1}$  —  $q-1 \times q-1$ —матрицами  $g_{q-1}$ . В дальнейшем мы будем полагать, что  $G_{q-1}$  — точное представление группы  $\mathfrak{G}$  на пространстве  $L_{q-1}$ .

Пусть  $\mathfrak{G}$  — конечная группа порядка  $q$  с групповой операцией  $+$  и  $G = \{g(\mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$  — ее регулярное представление. Последнее означает, что каждая  $g(\mathfrak{g}) = g \in G$  является подстановочной  $q \times q$ —матрицей, строки и столбцы которой индексированы элементами группы  $\mathfrak{G}$ , и которая реализует перестановку  $\sigma_{\mathfrak{g}}$ , действующую на множестве единичных векторов  $\mathcal{E} = \{e_{\mathfrak{h}} | \mathfrak{h} \in \mathfrak{G}\}$  пространства  $\mathbf{R}^q$ , следующим образом:

$$e_{\mathfrak{h}}g(\mathfrak{g}) = e_{\mathfrak{h}+\mathfrak{g}}. \quad (1.3.11)$$

Элементы  $G$  переставляют элементы множества  $\mathcal{E}$  и, более того, действует на  $\mathcal{E}$  транзитивно.

Более подробно о представлениях групп, в частности, о свойствах регулярных представлениях можно ознакомиться по книгам [14] или [15].

Очевидно, одномерное пространство  $L_1$ , натянутое на вектор  $e_1 = \sum_{\mathfrak{h} \in \mathfrak{G}} e_{\mathfrak{h}} = (1, 1, \dots, 1) \in \mathbf{R}^q$ , является инвариантным относительно действия группы  $G$  на евклидовом пространстве  $\mathbf{R}^q$ . Более того,  $e_1g(\mathfrak{g}) = e_1$ .

Ортогональное к  $L_1$  пространство  $L_{q-1}$  размерности  $q-1$  также является инвариантным относительно действия  $G$ . Таким образом, пространство  $\mathbf{R}^q$  мы представили в виде прямой суммы инвариантных подпространств:  $\mathbf{R}^q = L_1 \oplus L_{q-1}$ .

Заметим, что группа  $G_{q-1}$ , порожденная всеми матрицами  $g_{q-1} = g_{q-1}(\mathfrak{g})$  из (1.3.10), является точным представлением группы  $\mathfrak{G}$  на  $q-1$ -мерном евклидовом пространстве. Эти утверждения являются очевидными и ключевыми для дальнейшего изложения.

Группа преобразований  $G$  отображает множество векторов  $\mathcal{A} = \{\mathbf{a}_1, \dots, \mathbf{a}_q\}$ , где  $\mathbf{a}_j = e_j - \frac{1}{q} \sum_{s=1}^q e_s$ ,  $j = 1, \dots, q$ , по его построению в себя. Аналогично тому как это сделано для множества  $\mathcal{E}$ , элементы множества  $\mathcal{A}$  будем индексировать элементами группы  $\mathfrak{G}$ .

Отсюда следует, что элементы группы  $G_{q-1}$  также отображают множество векторов  $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_q\} \subset L_{q-1}$  в себя. Его элементы также как элементы  $\mathcal{A}$  будем индексировать элементами группы  $\mathfrak{G}$  таким образом, что  $\mathbf{b}_{\mathfrak{h}g_{q-1}(\mathfrak{g})} = \mathbf{b}_{\mathfrak{h}+\mathfrak{g}}$ .

Таким образом, множество  $\mathcal{B}$  является орбитным кодом, порожденным группой  $G_{q-1}$  следующим образом:  $\mathcal{B} = \{\mathbf{b}_1 h | h \in G_{q-1}\}$ .

Положим  $\pi(\mathfrak{h}) = \mathbf{b}_{\mathfrak{h}} = \mathbf{b}_1 \hat{g}(\mathfrak{h})$ ,  $\mathfrak{h} \in \mathfrak{G} = X$ . Из определения вектора  $\mathbf{b}_{\mathfrak{h}}$  вытекает, что отображение  $\pi$  является изоморфным изометрическим вложением одномерного пространства  $X = \mathfrak{G}$  на сферу  $S^{q-2}$ . Теорема доказана.  $\square$

Следует отметить, что доказанную теорему надо рассматривать как математический фольклёр, ибо ее доказательство использует только общеизвестные результаты из теории линейных представлений конечных групп.

Очень интересно, что в случае  $q = p = 4t + 1$  (простое число) можно довольно просто явно указать изоморфное изометрическое вложение  $\mathcal{Y}_3$  одномерного пространства Хемминга  $X = (\mathbb{F}_p, +)$ ,  $p > 2$ , являющееся циклической группой порядка  $p$ , на единичную сферу  $\frac{p-1}{2}$ -мерного унитарного пространства, которое сохраняет групповую структуру  $\mathbb{F}_p$ . Другими словами, на образе  $\pi(\mathbb{F}_p) \subset U^{\frac{p-3}{2}}$  одномерного пространства Хемминга  $\mathbb{F}_p$ ,  $p > 2$ , можно построить конечную группу  $G$  линейных унитарных преобразований пространства  $\mathcal{C}^{\frac{p-1}{2}}$ , относительно которой множество  $\pi(\mathbb{F}_p)$  является орбитным кодом и выполнен изоморфизм (1.3.2).

Как следует из результатов раздела 1.2.2 и это уже обсуждалось выше, группу  $G$  можно реализовать как группу ортогональных преобразований в евклидовом пространстве удвоенной размерности. Тем самым в рассматриваемом случае мы можем изоморфно и изометрически отобразить пространство Хемминга  $\mathbb{F}_p$  в орбитный код в  $p-1$ -мерном евклидовом пространстве с сохранением его алгебраической структуры. В отличие от теоремы 1.3.1 в данном случае группу  $G$ , как будет показано ниже, образуют диагональные матрицы, на диагонали которой находятся  $2 \times 2$ -матрицы.

Для построения указанного вложения  $\mathcal{Y}_3$  достаточно в качестве  $\pi(a)$  (см. (1.3.5)) взять функцию

$$\pi(a) = \left(\frac{p-1}{2}\right)^{-\frac{1}{2}} \left( \exp\left(\frac{2\pi i z_1 a}{p}\right), \exp\left(\frac{2\pi i z_2 a}{p}\right), \dots, \exp\left(\frac{2\pi i z_{\frac{p-1}{2}} a}{p}\right) \right), \quad (1.3.12)$$

где  $\{z_1, \dots, z_{\frac{p-1}{2}}\}$  — множество всех ненулевых квадратичных вычетов поля  $\mathbb{F}_p$ .

Легко показать, используя известные значения сумм Гаусса, что при  $a \neq b$  реальная часть скалярного произведения  $(\pi(a), \pi(b))$  равна  $\frac{-1}{p-1}$ . Поэтому, как следует из (1.2.6),

$$\lambda(\pi(a), \pi(b)) = \sqrt{\frac{2p}{p-1}}. \quad (1.3.13)$$

Орбитный код  $\mathfrak{K}(G, \mathbf{a})$ , порожденный группой диагональных  $\frac{p-1}{2} \times \frac{p-1}{2}$ -матриц



$$g_a = \text{diag} \left( \exp \left( \frac{2\pi i z_1 a}{p} \right), \exp \left( \frac{2\pi i z_2 a}{p} \right), \dots, \exp \left( \frac{2\pi i z_{\frac{p-1}{2}} a}{p} \right) \right), \quad a \in \mathbb{F}_p, \quad (1.3.14)$$

где  $\{z_1, \dots, z_{\frac{p-1}{2}}\}$  — множество всех ненулевых квадратичных вычетов поля  $\mathbb{F}_p$  и начальным  $\frac{p-1}{2}$ -мерным вектором  $\mathbf{a} = \left(\frac{p-1}{2}\right)^{-\frac{1}{2}} (1, \dots, 1)$ , очевидно, совпадает с  $\pi(\mathbb{F}_p)$  — образом одномерного пространства  $\mathbb{F}_p$ .

**Метрические вложения пространства Хемминга  $X^n$  на евклидову сферу в многомерном случае ( $n \geq 1$ )**

Пусть  $\mathbf{a} = (a_1, \dots, a_n) \in X^n$  и  $\pi$  — функция, которая осуществляет метрическое вложение  $\mathcal{Y}_i$ ,  $i = 1, 2, 3$ , одномерного пространства Хемминга  $X$ ,  $|X| = q$ , на евклидову (или унитарную) сферу  $S^{n'} (U^{n'})$ , для которого выполнено соотношение (1.3.3). Очевидно, функция

$$\pi(\mathbf{a}) = \frac{1}{\sqrt{n}} (\pi(a_1), \dots, \pi(a_n)) \in S^{n'n-1}, (U^{n'n-1}) \quad (1.3.15)$$

осуществляет метрическое покоординатное вложение всего пространства Хемминга  $X^n$  на сферу  $S^{n'n-1}$ . Действительно, из соотношения (1.2.6) следует, что

$$\begin{aligned} \lambda^2(\pi(\mathbf{a}), \pi(\mathbf{b})) &= 2 - \frac{2}{n} \Re \{ (\pi(a_1), \pi(b_1))_{\mathcal{C}} + \dots + (\pi(a_n), \pi(b_n))_{\mathcal{C}} \} = \\ &= \frac{1}{n} (\lambda^2(\pi(a_1), \pi(b_1)) + \dots + \lambda^2(\pi(a_n), \pi(b_n))) = \frac{1}{n} d(\mathbf{a}, \mathbf{b}), \end{aligned} \quad (1.3.16)$$

где  $(\cdot, \cdot)_{\mathcal{C}}$  — скалярное произведение в унитарном пространстве  $\mathcal{C}^{n'}$  и  $\Re x$  — действительная часть комплексного числа  $x$ .

Заметим, что при  $n > 1$  покоординатное метрическое вложение (1.3.12), вообще говоря, не является изометризм, если даже вложение каждой координаты и является изометрическим. Вместе с тем отображение (1.3.12) реализует вложение любого кода  $\mathfrak{K} \subseteq \mathbb{F}_q^n$  на сферу  $S^{n'n-1}$ . В общем случае при таком вложении алгебраическая структура пространства  $\mathbb{F}_q^n$  не сохраняется.

Класс покоординатных вложений кода  $\mathfrak{K}$  является наиболее естественным и очевидным классом метрического вложения. Вложения этого класса применимы для любого кода  $\mathfrak{K} \in X^n$ . Вместе с тем они реализуется только в евклидовых пространствах, размерность которых равна  $n \cdot n'$ . Естественно попытаться метрически вложить коды в евклидово пространство, размерность которых меньше, чем  $n \cdot n'$ . Этот вопрос к настоящему времени мало проработан, хотя известен, по крайней мере, один класс кодов, которые можно метрически вложить в евклидово пространство размерности меньшкй  $n \cdot n'$ .

Этим классом является эквидистантные коды  $\mathfrak{K} \in X^n$  (коды, у которых расстояния Хемминга между парами различных векторов одинаковы). Код из этого класса можно изометрически вложить на евклидову сферу  $S^{m-2}$  в евклидовом пространстве  $\mathbf{R}^{m-1}$ , где  $m = |\mathfrak{K}|$ .

Действительно, пусть  $\mathbf{a}_j$ ,  $j = 1, \dots, m$  — вершины правильного симплекса, вписанного в единичную сферу пространства  $\mathbf{R}^{m-1}$ . Функция  $\pi(\mathbf{x})$  сопоставляет произвольным образом элементы кода  $|\mathcal{K}|$  вершинам симплекса  $\mathbf{a}_j$ ,  $j = 1, 2, \dots, m$ . Очевидно,  $d(\mathbf{x}, \mathbf{y}) = c\lambda(\pi(\mathbf{x}), \pi(\mathbf{y}))$ , т.е. вложение кода  $\mathcal{K}$  является изометрическим.

Отметим, что можно показать, что  $|\mathcal{K}| \leq n + 1$  для  $q$ -ичного эквидистантного кода  $|\mathcal{K}|$  длины  $n$  с кодовым расстоянием  $d < n$ . Как нетрудно увидеть, если  $n > 1$  и  $q > 2$ , то число  $|\mathcal{K}|$  меньше числа  $(q-1)n$  — размерности пространства одномерного вложения, т.е. в этом случае рассматриваемое вложение кода на евклидову сферу "лучше" одномерного вложения.

Если эквидистантный код  $\mathcal{K}$  является группой  $\mathfrak{G}$ , например,  $\mathcal{K}$  — линейный код, то теорема (1.3.1) позволяет изоморфно и изометрически вложить его на сферу  $S^{m-2} \subset \mathbf{R}^{m-1}$ . Очевидно, для этого, достаточно трактовать вектор  $\mathbf{x} \in \mathcal{K}$  как одномерный элемент группы  $\mathfrak{G}$ .

Возвратимся опять к рассмотрению одномерных вложений. Если метрическое вложение  $\mathcal{Y}$  каждой координаты вектора линейного кода  $\mathcal{K} \subseteq \mathbb{F}_q^n$  с помощью отображения  $\pi$  (см. (1.3.12)) является изоморфным, т.е. осуществляется с помощью некоторого орбитного кода  $\mathcal{K}(\mathbb{F}_q, \mathbf{a})$  с начальным вектором  $\mathbf{a}$ , то метрическое вложение  $\mathcal{Y}_n$  всего кода  $\mathcal{K}$  с помощью отображения  $\pi$ , очевидно, является изоморфным вложением. Это очень важное свойство всех покоординатных изоморфных метрических вложений.

Как следует из теоремы 1.3.1, любой линейный код  $\mathcal{K} \subseteq \mathbb{F}_q^n$  можно изоморфно и метрически вложить с помощью покоординатного изоморфного и метрического отображения  $\pi$  на евклидову сферу  $S^{n'-1}$  с сохранением его алгебраической структуры.

Вопрос о существовании метрических вложений для какого-либо пространства Хемминга  $X^n$ ,  $n > 1$ , на сферу  $S^{N-1}$  в евклидовом пространстве размерности  $N$ , меньшей, чем  $n'n$ , где  $n'$  — размерность одномерного метрического вложения пространства  $X$ , является открытым. Это же самое справедливо и для изоморфных метрических вложений.

### 1.3.1 Вложение двоичного пространства Джонсона на евклидову сферу

В настоящем разделе мы рассматриваем покоординатное метрическое вложение (см. раздел 1.3, определение 1.3.2) пространства Джонсона  $J_{w,n}$  на единичную евклидову сферу, определяемые параметрами  $a$  и  $b$ . Затем выберем значения этих параметров так, чтобы минимальное расстояние между образами точек сферы пространства  $J_{w,n}$  было максимальным. Отметим, что в рассматриваемом случае  $n' = n$  (см. определение 1.3.2).

Точки пространства Джонсона  $J_{w,n}$ ,  $0 < 2w \leq n$ , отобразим на поверхность единичной евклидовой сферы следующим образом.

Пусть  $a, b$  — действительные неотрицательные числа такие, что  $wa^2 + (n-w)b^2 = 1$  и  $\mathbf{x} \in J_{w,n}$ . Отображение  $\pi : \mathbf{x} \rightarrow \pi(\mathbf{x})$ , состоящее в замене каждой нулевой координаты вектора  $\mathbf{x}$  числом  $-b$ , а единичной — числом  $a$ , отображает пространство  $J_{w,n}$  в множество точек  $\pi(J_{w,n})$ , принадлежащее единичной сфере  $S^{n-1}$ .

Пусть  $\mathbf{x}, \mathbf{y} \in J_{w,n}$ . Из определения отображения  $\pi$  следует, что

$$(\pi(\mathbf{x}), \pi(\mathbf{y})) = (w - \frac{d(\mathbf{x}, \mathbf{y})}{2})a^2 + (n - w - \frac{d(\mathbf{x}, \mathbf{y})}{2})b^2 - d(\mathbf{x}, \mathbf{y})ab = 1 - \frac{d(\mathbf{x}, \mathbf{y})}{2}(a+b)^2. \quad (1.3.17)$$

Отсюда, имея в виду равенство (1.2.3), получим

$$\lambda(\pi(\mathbf{x}), \pi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})(a+b)^2 = 2j(\mathbf{x}, \mathbf{y})(a+b)^2, \quad (1.3.18)$$

где  $j(\mathbf{x}, \mathbf{y})$  — расстояние Джонсона.

Как легко проверить, функция  $(a+b)^2$  при условии  $wa^2 + (n-w)b^2 = 1$  принимает максимальное значение, равное  $\frac{n}{w(n-w)}$ , если  $a = \sqrt{\frac{n-w}{wn}}$  и  $b = \sqrt{\frac{w}{n(n-w)}}$ . (Упражнение)

Отображение  $\pi$  будем всегда использовать при указанных значениях параметров  $a, b$ , которые максимизируют функцию  $(a+b)^2$ .

**Лемма 1.3.1** *Если  $\mathfrak{K} \subseteq J_{w,n}$  — код с кодовым расстоянием  $j$  в метрике Джонсона, тогда  $\pi(\mathfrak{K})$  — код на единичной евклидовой сфере с кодовым расстоянием  $\frac{2jn}{w(n-w)}$ .*

**Доказательство** леммы очевидно.  $\square$



# Глава 2

## Оценки

В начале этого раздела мы рассматриваем оценки числа элементов кода с заданным кодовым расстоянием в пространстве Хемминга. Также хорошо известны (см. например, [84], [37], [16]), подобные оценки для числа элементов кода на евклидовой сфере, но они не будут представлены в данном издании книги.

В этой главе мы рассматриваем относительно простые и давно известные оценки. Некоторые из них (оценка Варшамова-Гилберта в двоичном случае) не улучшены до сих пор. В то время как другие (оценка Хемминга) существенно усилены в определенных областях изменения параметров. Асимптотический анализ рассматриваемых оценок проводится только в простейших случаях.

Оценка линейного программирования изложена в новой авторской трактовке в главе 4 книги.

### 2.0.2 Оценка Хемминга (Граница сферической упаковки)

Мы обозначаем через  $M_q(n, d)$  максимальное число элементов  $q$ -значного кода  $\mathcal{K} \subseteq X^n$ ,  $|X| = q$ , длины  $n$  с кодовым расстоянием  $d$ .

#### Шар в пространстве Хемминга

Шаром  $V_{t,n}(\mathbf{x})$  радиуса  $t$  с центром в точке  $\mathbf{x}$  в пространстве Хемминга  $X^n$  называется множество точек отстоящих от  $\mathbf{x}$  на расстояние не большее, чем  $t$ .

Как легко вычислить,

$$|V_{t,n}(\mathbf{x})| = \sum_{s=0}^t (q-1)^s \binom{n}{s}. \quad (2.0.1)$$

(Упражнение)

Отметим, что число элементов шара  $V_{t,n}(\mathbf{x})$  не зависит от расположения его центра. Заметим, что это свойство выполняется не для всех метрических пространств, рассматриваемых в теории кодирования.

#### Оценка Хемминга

**Теорема 2.0.2 (Оценка Хемминга)** Для нечетного  $d = 2t + 1$  справедлива оценка

$$M_q(n, d) \leq \frac{q^n}{|V_{t,n}(\mathbf{x})|} = \frac{q^n}{\sum_{s=0}^t (q-1)^s \binom{n}{s}}. \quad (2.0.2)$$

**Доказательство.** Пусть  $d(\mathbf{x}, \mathbf{x}') \geq 2t + 1$ ,  $\mathbf{x}, \mathbf{x}' \in X^n$ . Тогда шары  $V_{t,n}(\mathbf{x})$  и  $V_{t,n}(\mathbf{x}')$  не пересекаются. Это утверждение непосредственно следует из неравенства треугольника, которое справедливо для метрики Хемминга  $d$ .

Пусть  $\mathcal{K} = \{\mathbf{x}_1, \dots, \mathbf{x}_M\}$  — код с кодовым расстоянием  $d = 2t + 1$ . Тогда с одной стороны шары  $V_{t,n}(\mathbf{x}_i)$  и  $V_{t,n}(\mathbf{x}_j)$ ,  $i \neq j$ , не пересекаются, а с другой —

$$\bigcup_{s=1}^M V_{t,n}(\mathbf{x}_s) \subseteq X^n. \quad (2.0.3)$$

Отсюда следует

$$\sum_{s=1}^M |V_{t,n}(\mathbf{x}_s)| = M|V_{t,n}(\mathbf{x}_s)| \leq |X^n| = q^n, \quad (2.0.4)$$

что доказывает оценку (2.0.2).  $\square$

Код  $\mathcal{K}$ , на котором достигается оценка (2.0.3), называется совершенным.

Совершенный код обладает следующим замечательным свойством: шары радиуса  $t$  с центрами в кодовых точках совершенного кода не пересекаются и одновременно заполняют всё пространство Хемминга  $X^n$ . Это утверждение вытекает из соотношения (2.0.4), которое для совершенного кода обращается в равенство. Заметим, что в евклидовом пространстве подобных расположений точек быть не может.

Пример. В случае  $d = 3$ ,  $q = 2$ , правая часть (2.0.2), очевидно, равна  $U_n = \frac{2^n}{n+1}$ . Если  $n = 2^m - 1$ , то  $U_n = 2^{n-\log_2(n+1)}$  равно числу элементов кода Хемминга (см. лемму 1.1.2) длины  $n$ . Отсюда следует, что код Хемминга является совершенным.

Кроме рассмотренного линейного кода Хемминга известно еще довольно большое число нелинейных совершенных кодов с кодовым расстоянием 3. Все они имеют ту же длину и то же число элементов, что и код Хемминга, но обладают некоторыми дополнительными свойствами. Исследования совершенных кодов посвящены многолетние работы новосибирских математиков (см. [1]).

Коды четной длины, которые состоят из двух векторов — нулевого  $(0, \dots, 0)$  и единичного  $(1, \dots, 1)$ , также являются совершенными.

Известны (см., например, [7]) также два очень интересных совершенных кода: первый — двоичный код длины 23 с кодовым расстоянием 7 и с числом элементов  $2^{12}$  и второй — троичный код длины 11 с кодовым расстоянием 5 и числом элементов  $3^6$ , которые носят название двоичного и троичного кодов Голея.

Заметим, что шары  $V_{3,23}(\mathbf{x})$  и  $V_{2,11}(\mathbf{x})$  радиусов 3 и 2 в двоичном и троичном пространстве имеют объем  $2^{11} = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}$  и  $3^5 = 1 + 2\binom{11}{1} + 2^2\binom{11}{2}$ , соответственно.

Эти коды являются спорадическими: в их "окрестности" нет кодов похожих или родственных им. Двоичный код Голея имеет очень интересные комбинаторные свойства. Изучение этих свойств выпадает из содержания данной книги.

Двоичные совершенные коды Хемминга с кодовым расстоянием 3, коды с двумя антиподными кодовыми векторами и двоичный код Голея образуют семейство всех совершенных двоичных кодов. Других двоичных совершенных кодов не существует.

### 2.0.3 Оценки сверху для числа элементов равновесных кодов

Максимальное число элементов равновесного двоичного кода  $\mathfrak{K} \subseteq J_{w,n}$  с кодовым расстоянием Джонсона  $j$ ,  $2j = d$ , где  $d = d(\mathfrak{K})$  — кодовое расстояние Хемминга кода  $\mathfrak{K}$ , мы обозначаем через  $A(n, j, w)$ .

Оценки сверху для функции  $A(n, j, w)$  интересны сами по себе, а также они используются при получении некоторых оценок  $M_2(n, d)$  — максимального числа элементов двоичного кода с кодовым расстоянием  $d$ .

**Теорема 2.0.3 (Оценка Джонсона)** *Справедлива оценка*

$$A(n, d, w) \leq \frac{jn}{jn - w(n - w)}, \quad (2.0.5)$$

если  $jn - w(n - w) > 0$ .

**Доказательство.** Равновесный код  $\mathfrak{K}$  на пространстве Джонсона  $J_{w,n}$  с метрикой Джонсона  $j(\mathbf{x}, \mathbf{y}) = \frac{d(\mathbf{x}, \mathbf{y})}{2}$  (см. раздел 1.1.4), отображим на поверхность единичной евклидовой сферы с помощью отображения  $\pi$  (см. раздел 1.3.1).

Пусть  $\mathbf{x}, \mathbf{y} \in J_{w,n}$ . Из равенства (1.3.17) следует, что

$$(\pi(\mathbf{x}), \pi(\mathbf{y})) = 1 - \frac{j(\mathbf{x}, \mathbf{y})n}{w(n - w)} \leq 1 - \frac{jn}{w(n - w)}. \quad (2.0.6)$$

Последнее неравенство вытекает из соотношения  $j(\mathbf{x}, \mathbf{y}) \geq j$  и из соотношения  $1 - \frac{jn}{w(n - w)} < 0$ , которое является следствием из условия теоремы.

С другой стороны имеем

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\pi(\mathbf{x}), \pi(\mathbf{y})) = \sum_{s=1}^n \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \hat{x}_s \hat{y}_s = \left( \sum_{\mathbf{x} \in \mathfrak{K}} \hat{x}_s \right)^2 \geq 0, \quad (2.0.7)$$

где  $\hat{x}_s$  и  $\hat{y}_s$   $s$ -ая координата векторов  $\pi(\mathbf{x})$  и  $\pi(\mathbf{y})$ .

Из неравенства (2.0.7) и неравенства (2.0.6) следует, что

$$0 \leq \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\pi(\mathbf{x}), \pi(\mathbf{y})) \leq |\mathfrak{K}| + |\mathfrak{K}|(|\mathfrak{K}| - 1) \left(1 - \frac{jn}{w(n - w)}\right), \quad (2.0.8)$$

ибо  $(\pi(\mathbf{x}), \pi(\mathbf{y})) = 1$ , если  $\mathbf{x} = \mathbf{y}$ , и  $(\pi(\mathbf{x}), \pi(\mathbf{y})) \geq 1 - \frac{jn}{w(n - w)}$ , если  $\mathbf{x} \neq \mathbf{y}$ .

Отсюда следует, что

$$|\mathfrak{K}| \leq \frac{jn}{jn - w(n - w)}. \quad (2.0.9)$$

Теорема доказана.  $\square$

## 2.0.4 Оценка Элайса-Бассалыго

**Теорема 2.0.4** (Бассалыго Л.А., [34]) *Имеет место оценка*

$$M_2(n, d) \leq \frac{2^n A(n, d, w)}{\binom{n}{w}}. \quad (2.0.10)$$

**Доказательство.** Пусть  $\mathfrak{K} \subset \mathbb{F}_2^n$  — двоичный код с кодовым расстоянием Хемминга  $d$ . Опишем вокруг каждой точки  $\mathfrak{K}$  сферу радиуса  $w$ . Пусть  $\chi(\mathbf{x})$  — кратность, с которой покрыта точка  $\mathbf{x} \in \mathbb{F}_2^n$  указанными сферами. Как легко увидеть,  $\chi(\mathbf{x})$  — это число кодовых точек  $\mathbf{y} \in \mathfrak{K}$ , находящихся на расстоянии  $w$  от  $\mathbf{x}$ . (Упражнение)

Очевидно,  $\chi(\mathbf{x}) \leq A(n, d, w)$ . Отсюда  $|\mathfrak{K}| \binom{n}{w} = \sum_{\mathbf{y} \in \mathfrak{K}} \binom{n}{w} = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi(\mathbf{x}) \leq A(n, d, w) 2^n$ , что доказывает соотношение (2.0.10).  $\square$

## 2.0.5 Оценка Плоткина и матрицы Адамара

### Оценка Плоткина

Рассматриваемая оценка справедлива для двоичных кодов с "большим" кодовым расстоянием  $d \geq \frac{n}{2}$ .

**Теорема 2.0.5** (Оценка Плоткина) *Если  $d \geq \frac{n}{2}$ , то*

$$M_2(n, d) \leq \begin{cases} \frac{2d}{2d-n}, & \text{если } 2d - n > 0 \\ 4d, & \text{если } n - 2d = 0 \end{cases}. \quad (2.0.11)$$

*Если некоторый двоичный код  $\mathfrak{K}$  лежит на второй границе в (2.0.11), то все кодовые расстояния  $d(\mathbf{x}, \mathbf{y})$ ,  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$ , принимают при  $\mathbf{x} \neq \mathbf{y}$  одно из двух значений:  $n$  и  $d = \frac{n}{2}$ .*

**Доказательство** похоже на доказательство теоремы 2.0.3. Рассмотрим отображение  $\phi : \mathbf{x} \rightarrow \phi(\mathbf{x})$ , состоящее в замене каждой нулевой координаты вектора  $\mathbf{x} \in \mathbb{F}_2^n$  числом  $-\frac{1}{\sqrt{n}}$ , а единичной — числом  $\frac{1}{\sqrt{n}}$ . Отображение  $\phi$  отображает множество  $\mathbb{F}_2^n$  в множество точек  $\phi(\mathbb{F}_2^n)$ , принадлежащее единичной сфере  $S^{n-1}$  евклидова пространства  $R^n$ , ибо, очевидно,  $(\phi(\mathbf{x}), \phi(\mathbf{x})) = |\phi(\mathbf{x})|^2 = 1$ .

Пусть  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ , тогда, как легко проверить, (Упражнение)

$$(\phi(\mathbf{x}), \phi(\mathbf{y})) = \frac{1}{n}(n - 2d(\mathbf{x}, \mathbf{y})). \quad (2.0.12)$$

Пусть  $\mathfrak{K} \subseteq \mathbb{F}_2^n$  — код с кодовым расстоянием  $d \geq \frac{n}{2}$ . С одной стороны имеем,

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\phi(\mathbf{x}), \phi(\mathbf{y})) = \sum_{s=1}^n \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \hat{x}_s \hat{y}_s = \sum_{s=1}^n \left( \sum_{\mathbf{x} \in \mathfrak{K}} \hat{x}_s \right)^2 \geq 0, \quad (2.0.13)$$

где  $\hat{x}_s$  —  $s$ -ая координата вектора  $\phi(\mathbf{x})$ .



С другой стороны,

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathcal{K}} (\phi(\mathbf{x}), \phi(\mathbf{y})) = |\mathcal{K}| + \sum_{\mathbf{x}, \mathbf{y} \in \mathcal{K}, \mathbf{x} \neq \mathbf{y}} (\phi(\mathbf{x}), \phi(\mathbf{y})) \leq |\mathcal{K}| + |\mathcal{K}|(|\mathcal{K}| - 1) \frac{n - 2d}{n}, \quad (2.0.14)$$

ибо  $(\phi(\mathbf{x}), \phi(\mathbf{y})) = 1$ , если  $\mathbf{x} = \mathbf{y}$ , и, как следует из (2.0.12),  $(\phi(\mathbf{x}), \phi(\mathbf{y})) = \frac{1}{n}(n - 2d(\mathbf{x}, \mathbf{y})) \leq \frac{1}{n}(n - 2d)$ , если  $\mathbf{x} \neq \mathbf{y}$ .

Из последних двух соотношений вытекает, что

$$|\mathcal{K}| + |\mathcal{K}|(|\mathcal{K}| - 1) \frac{n - 2d}{n} \geq 0. \quad (2.0.15)$$

Если  $2d - n > 0$ , то последнее неравенство эквивалентно первому неравенству в (2.0.11).

Если же  $n - 2d = 0$ , то рассмотрим код  $\mathcal{K}'$ , полученный из кода  $\mathcal{K}$  следующим образом. Предположим, что число векторов кода  $\mathcal{K}$ , у которых 1 является первой координатой больше или равно  $\frac{|\mathcal{K}|}{2}$ . Если это не так, то инвертируем все координаты векторов кода  $\mathcal{K}$  и получим код  $\mathcal{K}'$  с указанным свойством и с тем же кодовым расстоянием и тем же числом элементов, что и код  $\mathcal{K}$ .

В качестве вспомогательного кода возьмем все векторы кода  $\mathcal{K}'$  с единичной первой координатой, а в качестве кода  $\mathcal{K}''$  — все векторы вспомогательного кода, у которых выброшена первая координата. Очевидно, кодовое расстояние кода  $\mathcal{K}''$  равно  $d$ , а его длина равна  $n'' = n - 1$ , т.е.  $2d - n'' > 0$ .

К коду  $\mathcal{K}''$  применим первую оценку в (2.0.11). В результате с учетом соотношения  $|\mathcal{K}| \leq 2|\mathcal{K}''|$  получим вторую оценку в (2.0.11).

Переходим к доказательству второго утверждения теоремы. Так как код  $\mathcal{K}$  лежит на второй границе (2.0.11), то код  $\mathcal{K}''$  длины  $n'' = n - 1$  лежит на первой границе (2.0.11), т.е. для него соотношение (2.0.15) обращается в равенство, т.е.

$$|\mathcal{K}''| - |\mathcal{K}''|(|\mathcal{K}''| - 1) \frac{n'' - 2d}{n''} = 0, \quad (2.0.16)$$

т.е.  $|\mathcal{K}''| = \frac{|K|}{2} = n$ .

С другой стороны, из соотношения, которое в данном случае обращается в равенство, и соотношения (2.0.14) вытекает, что

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathcal{K}''} (\phi(\mathbf{x}), \phi(\mathbf{y})) = n + \sum_{\mathbf{x}, \mathbf{y} \in \mathcal{K}'', \mathbf{x} \neq \mathbf{y}} (\phi(\mathbf{x}), \phi(\mathbf{y})) = n - n(n - 1) \frac{1}{n - 1} = 0. \quad (2.0.17)$$

Так как  $(\phi(\mathbf{x}), \phi(\mathbf{y})) \leq 0$ , то из (2.0.17) следует, что  $(\phi(\mathbf{x}), \phi(\mathbf{y})) = 0$  для всех  $\mathbf{x}, \mathbf{y} \in \mathcal{K}'', \mathbf{x} \neq \mathbf{y}$ .  $\square$

В качестве примера кода, лежащего на первой границе (2.0.11), рассмотрим двоичный линейный код  $\mathcal{K}$  размерности  $m$  и длины  $n = 2^m - 1$ , двойственный к коду Хемминга. Другими словами, рассмотрим код с порождающей матрицей  $B_H$  (см. раздел 1.1.3). Этот код, как будет показано далее, имеет кодовое расстояние  $2^{m-1}$ , т.е. лежит на границе Плоткина. Между прочим, приведенное утверждение о кодовом расстоянии кода  $\mathcal{K}$  совсем нетрудно доказать непосредственно. (Упражнение)

## Матрицы Адамара

Кроме указанного кода, известно еще очень много классов кодов с параметрами, лежащими на границе (2.0.11). Важнейшие из них это коды с параметрами  $n = 4t, d = \frac{n}{2}, M = 2n$ . Эти коды эквивалентны такому понятию как матрицы Адамара :

**Определение 2.0.4** *Ортогональная  $n \times n$ -матрица  $A$  с элементами  $\pm 1 \in R$  называется матрицей Адамара.*

Рассмотрим код  $\hat{\mathcal{K}}$  длины  $n$ , образованный всеми строками матрицы  $A$  и их обращениями, т.е. строками  $A$ , умноженными на  $-1$ . В виду того, что для любых  $\hat{x}, \hat{y} \in \hat{\mathcal{K}}, \hat{x} \neq \hat{y}$ , скалярное произведение  $(\hat{x}, \hat{y})$  принимает одно из двух значений  $0$ , когда  $\hat{x} \neq -\hat{y}$ , и  $-n$ , когда  $\hat{x} = -\hat{y}$ , код  $\hat{\mathcal{K}}$  имеет кодовое расстояние  $d = \frac{n}{2}$ , число элементов, равное  $2n$ , т.е. он лежит на границе (2.0.5). Таким образом, из существования  $n \times n$ -матрицы Адамара  $A$  следует существование двоичного кода длины  $n$  с кодовым расстоянием  $d = \frac{n}{2}$ , лежащие на границе (2.0.11).

Локажем теперь, что двоичный код  $\mathcal{K}$  длины  $n$  с кодовым расстоянием  $d = \frac{n}{2}$ , лежащий на границе (2.0.11), определяет  $n \times n$ -матрицу Адамара  $A$ .

Для этого рассмотрим множество векторов  $\hat{\mathcal{K}} = \{\phi(x) | x \in \mathcal{K}\}$ ,  $|\hat{\mathcal{K}}| = 2n$ , длины  $n$  с кодовым расстоянием  $d = \frac{n}{2}$  и числом элементов  $2n$ . Как следует из второго утверждения теоремы 2.0.5 и его доказательства, матрица  $A(\hat{\mathcal{K}})$ , образованная всеми векторами из  $\hat{\mathcal{K}}$  является матрицей Адамара, ибо  $(\phi(x), \phi(y)) = \frac{2-2d(x,y)}{n} = 0, x \neq y$ .

**Лемма 2.0.2** *Необходимым условием существования матрицы Адамара размерности  $n > 2$  является условие  $n = 4t$ .*

**Доказательство.** Очевидно, матриц Адамара нечетной размерности не существует.

Предположим, что  $n = 4t + 2 > 2$ , и докажем, что матриц Адамара такой размерности не существует.

Пусть  $a, b, c$  — три попарно различных строк матрицы  $A$ . Векторы  $a, b$  ортогональны, поэтому вектор  $a + b$  имеет нечетное число, равное  $\frac{n}{2} = 2t + 1$ , ненулевых координат, принимающих значение  $\pm 2$ . (Упражнение)

Очевидно, с одной стороны  $(a + b, c) = (a, c) + (b, c) = 0$ , а с другой —  $(a + b, c) \neq 0$ , ибо вектор  $a + b$  содержит нечетное число ненулевых координат с одинаковым модулем.  $\square$

Матрицы Адамара предположительно существуют для всех значений  $n = 4t$  вида, хотя в действительности они построены только для некоторых значений  $t$ , в число которых входят и несколько бесконечных семейств  $t$ .

Имеется многочисленная литература, описывающая методы построения матриц Адамара или, что одно и то же, кодов, лежащих на границе Плоткина.

Два из таких бесконечных семейств матриц Адамара размерности  $n = 4t = p + 1$ , где  $p$  — простое число вида  $p = 4t - 1$ , и  $n = 2^m$  рассмотрено в параграфе 8.5 (разделы "Рекуррентные последовательности максимального периода" и "Последовательности, получаемые с помощью символов Лежандра"). Еще одно семейство строится следующим образом.

**Определение 2.0.5** Тензорным произведением  $A \otimes B$  матриц  $A = (a_{i,j})_{i,j=1,\dots,n}$  и  $B$  размеров  $n$  и  $m$ , соответственно, называется матрица

$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}B & a_{n,2}B & \cdots & a_{n,n}B \end{pmatrix}. \quad (2.0.18)$$

**Лемма 2.0.3** Если  $A$  и  $A'$  — матрицы Адамара размерностей  $n$  и  $n'$ , соответственно, то  $A \otimes A'$  — также матрица Адамара размерности  $n \cdot n'$ .

**Доказательство.** (Упражнение)

Лемма 2.0.3 позволяет построить матрицу  $A_1^{\otimes n} = A_1 \otimes \cdots \otimes A_1$  ( $n$  раз) Адамара размерности  $2^n$ , исходя из  $2 \times 2$ -матрицы Адамара

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.0.19)$$

## Быстрое умножение вектора на матрицу Адамара

Алгоритмы быстрого умножения вектора на матрицу Адамара находят широкое применение при обработке сигналов, а также используются в некоторых разделах криптографии.

Внутреннее произведение  $\langle \mathbf{x}, \mathbf{y} \rangle$  между векторами  $\mathbf{x} = (x_1, \dots, x_m)$  and  $\mathbf{y} = (y_1, \dots, y_m)$  пространства  $\mathbb{F}_2^m$  определим следующим образом

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^m x_i y_i, \quad (2.0.20)$$

где сложение и умножение выполняются в поле  $\mathbb{F}_2$ .

Далее строки и столбцы матрицы  $B$  с действительными элементами будем индексировать элементами пространства  $\mathbb{F}_2^m$ . Таким образом элемент  $v_{\mathbf{x}, \mathbf{y}}$ ,  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m$  матрицы  $B = \|v_{\mathbf{x}, \mathbf{y}}\|$  расположен на пересечении строки, индексированной элементом  $\mathbf{x}$ , и столбца индексированным элементом  $\mathbf{y}$ .

**Лемма 2.0.4** Матрица

$$A_m = \|(-1)^{\langle \mathbf{x}, \mathbf{y} \rangle}\|. \quad (2.0.21)$$

размера  $2^m \times 2^m$  — является матрицей Адамара.

**Доказательство.** (Упражнение)

Лемма 2.0.4 доставляет еще один способ построения матрицы Адамара размера  $2^m \times 2^m$ .

Очевидно, пространство  $\mathbb{F}_2^m$  можно представить в виде  $\mathbb{F}_2^m = \{(x_1, \dots, x_{m-1}, 0) | (x_1, \dots, x_{m-1}) \in \mathbb{F}_2^{m-1}\} \cup \{(x_1, \dots, x_{m-1}, 1) | (x_1, \dots, x_{m-1}) \in \mathbb{F}_2^{m-1}\}$ . Поэтому матрицу можно представить в виде

$$A_m = \begin{pmatrix} A_{m-1} & A_{m-1} \\ A_{m-1} & -A_{m-1} \end{pmatrix}. \quad (2.0.22)$$

Как легко проверить, выполнено следующее равенство

$$\begin{pmatrix} A_{m-1} & A_{m-1} \\ A_{m-1} & -A_{m-1} \end{pmatrix} = \begin{pmatrix} A_{m-1} & 0 \\ 0 & A_{m-1} \end{pmatrix} \cdot \begin{pmatrix} I_{m-1} & I_{m-1} \\ I_{m-1} & -I_{m-1} \end{pmatrix}, \quad (2.0.23)$$

где  $I_j$  — единичная  $2^j \times 2^j$  — матрица.

Из последнего равенства вытекает, что

$$A_m = I_1 \otimes A_{m-1} \cdot A_1 \otimes I_{m-1} \quad (2.0.24)$$

где через  $\otimes$  обозначено тензорное произведение матриц.

Используя (2.0.24), представим матрицу  $A_{m-1}$  в виде (2.0.24). В результате получим

$$A_m = I_2 \otimes A_{m-2} \cdot I_1 \otimes A_1 \otimes I_{m-2} \cdot A_1 \otimes I_{m-1} \quad (2.0.25)$$

Продолжая этот процесс, получим

$$A_m = I_{m-1} \otimes A_1 \cdot I_{m-2} \otimes A_1 \otimes I_1 \cdots I_{m-j} \otimes A_1 \otimes I_{j-1} \cdots I_1 \otimes A_1 \otimes I_{m-2} \cdot A_1 \otimes I_{m-1} \prod_{j=1}^m I_{m-j} \otimes A_1 \otimes I_{j-1}. \quad (2.0.26)$$

Очевидно, каждая матрица  $B_j = I_{m-j} \otimes A_1 \otimes I_{j-1}$  содержит в каждой строке и каждом столбце только два ненулевых элемента  $\pm 1$ . Поэтому равенство (2.0.26) можно рассматривать как разложение матрицы  $A_m$  в произведение разреженных матриц  $B_j$ , каждая из которых имеет в каждой строке и каждом столбце два ненулевых элемента  $\pm 1$ .

Подобное разложение позволяет существенно уменьшить число умножений и сложений, требуемых для вычисления произведения вектора  $\mathbf{a}$  с действительными координатами на матрицу Адамара  $A_m$ .

Действительно, чтобы умножить вектор  $\mathbf{a}$  на матрицу  $A_m$  обычным способом необходимо порядка  $n^2 = 2^{2m}$  операций сложения и умножения в поле действительных чисел, где  $n = 2^m$  — размерность матрицы  $A_m$ .

Если вычислять  $\mathbf{a}A_m$  как  $m$  последовательных умножений  $\mathbf{a}B_m \cdot B_{m-1} \cdots B_1$ , то число операций сложения и умножения в поле действительных чисел будет равным по порядку числу  $m2^m = \log_2 n \cdot n$  операций, в виду того, что умножение вектора на матрицу  $B_j$  требует  $2^m$  операций умножения и  $2^m - 1$  операции сложения в поле действительных чисел.

## 2.0.6 Оценки Синглтона и Грайсмера

### Оценка Синглтона

**Теорема 2.0.6 (Оценка Синглтона)** Для линейного кода  $\mathcal{K} \subseteq \mathbb{F}_q^n$  длины  $n$ , размерности  $k$  и с кодовым расстоянием  $d$  имеет место оценка

$$d \leq n - k + 1. \quad (2.0.27)$$

**Доказательство.** Пусть  $A$  — порождающая матрица кода  $\mathfrak{K}$ . Так как  $k = \dim \mathfrak{K}$ , то в  $A$  найдется  $k$  линейно независимых столбцов. (Упражнение). Без ограничения общности, будем полагать, что это первые  $k$  столбцов матрицы  $A$ .

Так как первые  $k$  столбцов  $A$  линейно независимы, то найдется линейная комбинация  $\mathbf{a}$  строк матрицы  $A$ , у которой в первых  $k$  координатах находится любой наперед заданный  $k$ -мерный вектор. В качестве такого вектора возьмем вектор, у которого только одна координата является ненулевой.

Очевидно, кодовый вектор  $\mathbf{a}$  с указанным началом имеет вес  $wt(\mathbf{a}) \leq 1 + n - k$ , что доказывает лемму.  $\square$

Следует сказать, что при большом  $k$  оценка Синглтона достигается только при больших значениях значности кода  $q$ . Коды, для которых достигается оценка (8.6.3) называются MDR-кодами (английская транскрипция. Перевод: разделимый код с максимальным расстоянием).

Известно много конструкций MDR-кодов. В частности,  $q$ -значные коды Рида-Соломона, о которых речь пойдет ниже, являются MDR-кодами.

Основная задача этого направления теории: при заданных  $d$  и  $q$  найти MDR-код максимальной длины. Предположительно,  $n \leq q + 1$  при  $2 \leq k \leq q$ , но при  $q = 2^l$  и  $d = 2, n = 2, n = q + 2$ .

MDR-коды имеют глубокую связь с некоторыми комбинаторными конструкциями: конечными проективными геометриями, ортогональными таблицами (дизайнами) и др.

## Оценка Грайсмера

Рассматриваемая оценка показывает, что двоичный линейный код с кодовым расстоянием  $d$  не может быть слишком коротким.

Обозначим через  $N(k, d)$  минимальную длину линейного двоичного кода размерности  $k$  с минимальным кодовым расстоянием  $d$ .

### Теорема 2.0.7 (Оценка Грайсмера)

$$N(k, d) \geq \left\lfloor \frac{d}{2^{k-1}} \right\rfloor + \dots + \left\lfloor \frac{d}{2} \right\rfloor + d, \quad (2.0.28)$$

где  $\lfloor x \rfloor$  — наименьшее целое число такое, что  $x \leq \lfloor x \rfloor$ .

**Доказательство.** Пусть  $\mathfrak{K}$  — двоичный линейный код длины  $n$  с кодовым расстоянием  $d$ . Покажем, что

$$n \geq d + N\left(k - 1, \left\lfloor \frac{d}{2} \right\rfloor\right). \quad (2.0.29)$$

Без ограничения общности мы полагаем, что порождающая матрица  $A$  кода  $\mathfrak{K}$  имеет вид

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 \\ & & A_1 & & & & B_1 & \end{pmatrix}, \quad (2.0.30)$$

где  $A_1$  — матрица с  $n - d$  столбцами и  $k - 1$  строками и  $B_1$  — матрица с  $d$  столбцами и  $k - 1$  строками.

Ранг матрицы  $A_1$  равен  $k - 1$ . Если он меньше, то мы путем сложения строк  $A_1$  обратим ее первую строку в нулевую. В этом случае вторая строка матрицы  $A$  будет иметь вес меньший, чем  $d$ , что невозможно в виду того, что ее сумма с первой строкой будет, очевидно, иметь вес меньший, чем  $d$ .

Матрица  $A_1$  является порождающей матрицей кода  $\mathcal{K}_1$  длины  $n - d$  и некоторым кодовым расстоянием  $d_1$ . Предположим, что  $\mathbf{v} \in \mathcal{K}_1$  и вектор  $(\mathbf{v}|\mathbf{u}) \in \mathcal{K}$  ( $(\mathbf{v}|\mathbf{u})$  — конкатенация векторов  $\mathbf{v}$  и  $\mathbf{u} \in \mathbb{F}_2^d$ ).

В виду того, что  $(\mathbf{v}|\bar{\mathbf{u}}) = (\mathbf{v}|\mathbf{u}) + \mathbf{a}$ , где  $\bar{\mathbf{u}}$  — вектор  $\mathbf{u}$  с инвертированными координатами и  $\mathbf{a}$  — первая строка матрицы  $A$ ), мы имеем

$$\begin{aligned} d_1 + wt(\mathbf{u}) &\geq d \\ d_1 + \bar{\mathbf{u}} &= d_1 + d - wt(\mathbf{u}) \geq d. \end{aligned} \quad (2.0.31)$$

Отсюда вытекает, что  $2d_1 \geq d$  или  $d_1 \geq \lceil \frac{d}{2} \rceil$ . Следовательно,

$$n - d \geq N \left( k - 1, \left\lceil \frac{d}{2} \right\rceil \right), \quad (2.0.32)$$

что доказывает неравенство (2.0.29)

Заметим, что  $\left\lceil \frac{\lceil \frac{d}{2^s} \rceil}{2} \right\rceil = \left\lceil \frac{d}{2^{s+1}} \right\rceil$ . Отсюда, многократно применяя неравенство (2.0.32), получим (2.0.28).  $\square$

Следует сказать, что приведенное доказательство незначительно отличается от доказательства соответствующей теоремы из книги [7].

В качестве примера, рассмотрим код размерности  $m$  и длины  $n = 2^m - 1$  с кодовым расстоянием  $2^{m-1}$ , двойственный к коду Хемминга.

Из теоремы 2.0.7 вытекает, что

$$N(m, 2^{m-1}) \geq 2^{m-1} + 2^{m-2} + \dots + 2 + 1 = 2^m - 1, \quad (2.0.33)$$

т.е. этот код лежит не только на границе Плоткина, но и на границе Граймера.

## 2.0.7 Оценка для числа элементов антиподального кода

Двоичный код  $\mathcal{K}$  называется антиподальным, если он удовлетворяет следующему свойству: если  $\mathbf{x} \in \mathcal{K}$ , то антиподальный вектор  $\bar{\mathbf{x}} = \mathbf{x} + (1, 1, \dots, 1)$  также принадлежит коду  $\mathcal{K}$ . Очевидно, кодовое расстояние любого антиподального кода не выше  $\frac{n}{2}$ .

Расстояние между различными векторами  $\mathbf{x}, \mathbf{y}$  антиподального кода с кодовым расстоянием  $d$  принимает значения из интервала  $[d, n - d]$ , либо оно равно  $n$  (в том случае, когда  $\mathbf{y} = \bar{\mathbf{x}}$ ).

Так как взаимные расстояния антиподального кода должны принадлежать ограниченному множеству значений по сравнению с общим случаем, то верхний оценки их объема, вообще говоря, должны быть сильнее оценок для общего случая. Как будет видно ниже, это действительно так.

Будем обозначать максимальное число элементов двоичного антиподального кода длины  $n$  с кодовым расстоянием  $d$  через  $M_A(n, d)$ .

**Теорема 2.0.8 (Сидельников, 1971, [35, 66])** *Справедлива оценка*

$$M_A(n, d) \leq \frac{2n^3 - 2n(n-2d)^2}{3n - (n-2d)^2 - 2}, \quad (2.0.34)$$

если  $3n - (n-2d)^2 - 2 > 0$  и  $n \geq 4$ .

**Доказательство.** Пусть  $\mathfrak{K}$  — антиподальный код с кодовым расстоянием  $d$  и  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  и пусть  $\phi : \mathfrak{K} \rightarrow S^{n-1}$  — отображение, определенное в доказательстве теоремы 2.0.5. Очевидно,

$$|(\pi(\mathbf{x}), \pi(\mathbf{y}))| = |n - 2d(\mathbf{x}, \mathbf{y})| \leq n - 2d, \quad (2.0.35)$$

если  $\mathbf{x} \neq \mathbf{y}; \mathbf{y} \neq \bar{\mathbf{x}}$ . Если же  $\mathbf{x} = \mathbf{y}$ , либо  $\mathbf{y} = \bar{\mathbf{x}}$ , то  $|(\pi(\mathbf{x}), \pi(\mathbf{y}))| = n$ . Заметим, что последнее неравенство в (2.0.35) для кода  $\mathfrak{K}$ , не являющегося антиподальным, может быть не выполненным.

Отсюда вытекает, что

$$\begin{aligned} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\pi(\mathbf{x}), \pi(\mathbf{y}))^4 &= 2n^4 |\mathfrak{K}| + \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}; \mathbf{x} \neq \mathbf{y}; \mathbf{y} \neq \bar{\mathbf{x}}} (\pi(\mathbf{x}), \pi(\mathbf{y}))^4 \leq \\ &2n^4 |\mathfrak{K}| + (n-2d)^2 \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}; \mathbf{x} \neq \mathbf{y}; \mathbf{y} \neq \bar{\mathbf{x}}} (\pi(\mathbf{x}), \pi(\mathbf{y}))^2 = \\ &2n^4 |\mathfrak{K}| - 2(n-2d)^2 n^2 |\mathfrak{K}| + (n-2d)^2 \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\pi(\mathbf{x}), \pi(\mathbf{y}))^2. \end{aligned} \quad (2.0.36)$$

Пусть  $n \geq 4$  и  $P_4(x)$  — многочлен Кравчука степени 4 (он определен равенством (3.2.13), в котором  $p = 2$ ). Многочлен  $P_4(x)$  далее в работе также имеет другое обозначение:  $K_4^{(2,n)}(x)$ . Нетрудно вычислить (автор вычислял с помощью программы Mathematica5), что

$$P_4(x) = \frac{1}{24}((n-2x)^4 + (8-6n)(n-2x)^2 + 3n(n-2)) \quad (2.0.37)$$

Как следует из следствия 4.1.1 (равенство (4.1.10))

$$\begin{aligned} \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} P_4(x)(d(\mathbf{x}, \mathbf{y})) &= \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} P_4(x) \left( \frac{n - (\pi(\mathbf{x}), \pi(\mathbf{y}))}{2} \right) = \\ \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \frac{1}{24} ((\pi(\mathbf{x}), \pi(\mathbf{y}))^4 + (8-6n)(\pi(\mathbf{x}), \pi(\mathbf{y}))^2 + 3n(n-2)) &\geq 0, \end{aligned} \quad (2.0.38)$$

для любого кода  $\mathfrak{K} \subset \mathbb{F}_p^n$ .

Положим  $T(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} (\pi(\mathbf{x}), \pi(\mathbf{y}))^2$ . Так как  $K_2^{(2,n)}(x) = \frac{1}{2}((n-2x)^2 - n)$ , то из Следствия 4.1.1 (неравенство (4.1.10)) следует, что  $T(\mathfrak{K}) \geq n$  для любого кода  $\mathfrak{K}$ .

Из соотношений (2.0.36), (2.0.38) и того, что  $T(\mathfrak{K}) \geq n$ , вытекает

$$\begin{aligned} 0 \leq \frac{2n^4}{|\mathfrak{K}|} - \frac{2n^2(n-2d)^2}{|\mathfrak{K}|} + (n-2d)^2 T(\mathfrak{K}) + (8-6n)T(\mathfrak{K}) + 3n(n-2) \leq \\ \frac{2n^4}{|\mathfrak{K}|} - \frac{2n^2(n-2d)^2}{|\mathfrak{K}|} + (n-2d)^2 n + 2n - 3n^2 \end{aligned} \quad (2.0.39)$$

при  $(n - 2d)^2 + (8 - 6n) \leq 0$ . Последняя оценка эквивалентна оценке (2.0.34).  $\square$

Следует сказать, что оценка (9.2.3) достигается на коде Кердока (см. параграф 8.2) и на некоторых других, например, антиподальном линейном коде  $\mathfrak{K}$  теоремы 8.4.1 (параграф 8.4). Последний код имеет следующие параметры:  $n = 2^m$  ( $m$  — нечетное), число элементов  $2^{2m+1} = 2n^2$  и кодовое расстояние  $d = 2^{m-1} - 2^{\frac{1}{2}(m+1)} = \frac{1}{2}(n - \sqrt{2n})$ .

Антиподальный код Кердока  $\mathfrak{K}_{Ker}$  является одной из самых замечательных конструкций теории кодирования. Он имеет следующие параметры:  $n = 2^{2m}$ ,  $|\mathfrak{K}_{Ker}| = n^2 = 2^{4m}$  и  $d = \frac{1}{2}(n - \sqrt{n}) = 2^{2m-1} - 2^{m-1}$ .

После небольшого размышления, можно установить, что оценка (9.2.3) может достигаться только на кодах  $\mathfrak{K}$ , у которых множество значений расстояний  $d(\mathbf{x}, \mathbf{y})$ ,  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$ , (спектр кода) состоит из пяти элементов:  $0, \frac{n}{2}, \frac{1}{2}(n \pm \sqrt{rn})$ ,  $0 < r < 3$ . При  $r = 1$  (код Кердока) и  $r = 2$  известны коды, на которых достигается оценка (2.0.34) (см. раздел 8.4, теорема (8.4.1)).

## 2.0.8 Оценка Варшамова-Гилберта

В отличие от верхних оценок числа элементов кода, рассматриваемая оценка является оценкой существования, а именно она устанавливает границы для чисел  $n, d, M$ , в пределах которых заведомо существует линейный код с этим параметрами.

**Теорема 2.0.9** *Существует линейный код над полем  $\mathbb{F}_q$  длины  $n$ , с кодовым расстоянием  $d$  и размерностью  $k = n - r$ , если параметры  $n, d, r$  удовлетворяют следующему условию*

$$\sum_{s=1}^{d-1} (q-1)^s \binom{n-1}{s} \leq q^r - 1. \quad (2.0.40)$$

**Доказательство.** Как следует из теоремы 1.1.1, нам надо построить матрицу  $B$  с  $r$  строчками и  $n$  столбцами, у которой любой комплект из  $d-1$  столбцов является линейно независимым.

Предположим, что мы построили матрицу  $B'$  с  $r$  строчками и  $n'$  столбцами, у которой любой комплект из  $d-1$  столбцов является линейно независимым. В каком случае мы к матрице  $B'$  сможем добавить ещё один ненулевой столбец, сохраняя свойство независимости столбцов?

Для ответа на этот вопрос рассмотрим множество столбцов  $\mathfrak{B}$ , каждый из которых является суммой не более, чем из  $d-1$  столбцов матрицы  $B'$ . Если число элементов в  $\mathfrak{B}$  меньше, чем  $q^r - 1$ , то в пространстве  $\mathbb{F}_q^r \setminus \mathfrak{B}$  найдется ненулевой элемент (столбец), который может быть добавлен к матрице  $B'$  с сохранением свойства независимости.

Оценим число элементов множества  $\mathfrak{B}$ . Очевидно, элементы, которые являются суммами с ненулевыми коэффициентами столбцов определенного комплекта с  $s$ ,  $1 \leq s \leq d-1$  из столбцов порождают  $(q-1)^s$  ненулевых элементов (столбцов) множества  $\mathfrak{B}$ . Заметим, что различные комплекты столбцов могут порождать пересекающиеся подмножества множества  $\mathfrak{B}$ .

Отсюда вытекает, что

$$|\mathfrak{B}| \leq \sum_{s=1}^{d-1} (q-1)^s \binom{n'}{s}. \quad (2.0.41)$$



Следовательно, если

$$\sum_{s=1}^{d-1} (q-1)^s \binom{n'}{s} < q^r - 1, \quad (2.0.42)$$

то в  $r$ -мерном пространстве  $\mathbb{F}_q^r$  существует элемент, который может быть добавлен к матрице  $B'$  с сохранением свойства независимости комплектов из  $d-1$  столбцов.

Таким образом, существует код длины  $n$ , если выполнено условие (2.0.40).  $\square$

## 2.0.9 Асимптотические границы

Мы получим асимптотические выражения ( $n \rightarrow \infty$ ) правых частей оценок (2.0.2) и (2.0.10) в двоичном случае.

Нам далее понадобятся оценки биномиальных коэффициентов  $\binom{n}{j}$ . Эти оценки включают функцию энтропии  $H_2(x)$ , определяемую равенством

$$H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x), \quad 0 < x < 1. \quad (2.0.43)$$

Эта широко известная функция используется в теории информации как мера неопределенности вероятностного источника информации. Нам она понадобится как функция, с помощью которой приближаются биномиальные коэффициенты.

**Лемма 2.0.5 (Оценка биномиального коэффициента [7])** Пусть  $\lambda n$  — целое число, где  $0 < \lambda < 1$  — функция энтропии. Тогда

$$\frac{1}{\sqrt{8n\lambda(1-\lambda)}} 2^{nH_2(\lambda)} \leq \binom{n}{\lambda n} \leq \frac{1}{\sqrt{2\pi n\lambda(1-\lambda)}} 2^{nH_2(\lambda)} \quad (2.0.44)$$

**Доказательство** основано на формуле Стирлинга для  $n!$ , которая широко используется во многих других задачах по вычислению асимптотического поведения комбинаторных функций.

$$\sqrt{2\pi n} n^{n+\frac{1}{2}} e^{-n+\frac{1}{12n}-\frac{1}{360n^3}} < n! < \sqrt{2\pi n} n^{n+\frac{1}{2}} e^{-n+\frac{1}{12n}} \quad (2.0.45)$$

Следовательно,

$$\binom{n}{\lambda n} = \frac{n!}{\lambda n! (n-\lambda n)!} = \frac{1}{\sqrt{2\pi n\lambda(1-\lambda)}} 2^{nH_2(\lambda)} \quad (2.0.46)$$

Отсюда следует справедливость неравенства в левой части (2.0.44). Доказательство справедливости неравенства в правой части производится аналогично.  $\square$

**Следствие 2.0.1** В условиях леммы 2.0.5

$$\binom{n}{[\lambda n]} = \frac{1}{\sqrt{2\pi n\lambda(1-\lambda)}} 2^{nH_2(\lambda)(1+\varepsilon_n)}, \quad n \rightarrow \infty, \quad \varepsilon_n \rightarrow 0. \quad (2.0.47)$$

Число

$$R(n, d) = \frac{1}{n} \log_2 M_2(n, d) \quad (2.0.48)$$

называется *скоростью передачи с помощью кода длины  $n$  с кодовым расстоянием  $d$* . Обоснование этого термина следующее.

Двоичный код с числом элементов  $M(n, d) \geq 2$  "переносит" информацию, которая может быть закодирована с помощью  $\log_2 M(n, d)$  информационных битов. Каждый информационный бит исходной информации при передаче его по каналу связи с помощью кода использует в среднем  $\frac{n}{\log_2 M(n, d)}$  кодовых символов кода. Поэтому скоростью передачи одного бита исходной информации естественно назвать величину, обратную к указанной.

Пусть  $n, d, w$  стремятся к бесконечности таким образом, что

$$\frac{d}{n} \rightarrow \delta, \quad n \rightarrow \infty, \quad \frac{w}{n} \rightarrow \omega, \quad n \rightarrow \infty, \quad 0 < \delta, \omega < \frac{1}{2},$$

где  $\delta$  и  $\omega$  — постоянные величины.

Величины  $\delta$  и  $\omega$  называются *относительным кодовым расстоянием и относительным весом*.

Функция

$$R(\delta) = \overline{\lim}_{n \rightarrow \infty, \frac{d}{n} \rightarrow \delta} R(n, d), \quad (2.0.49)$$

где  $\overline{\lim}$  — верхний предел, называется *относительной скоростью передачи с помощью кода с относительным кодовым расстоянием  $\delta$* .

**Лемма 2.0.6** (Асимптотическое поведение оценок (2.0.2) и (2.0.10)) *Имеют место оценки*

$$R(\delta) \leq 1 - H_2\left(\frac{\delta}{2}\right) \quad (\text{оценка Хемминга}) \quad (2.0.50)$$

и

$$R(\delta) \leq 1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}\right) \quad (\text{оценка Бассалыги-Элайса}) \quad (2.0.51)$$

**Доказательство** непосредственно следует из лемм 2.0.2 и 2.0.4 и полученных выше асимптотических выражений для биномиальных коэффициентов.  $\square$

Как легко установить, функция  $1 - H_2\left(\frac{\delta}{2}\right)$  на интервале  $0 < \delta \leq \frac{1}{2}$  всегда больше функции  $1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}\right)$ . Поэтому оценка Хемминга при "больших" значениях кодового расстояния  $d$  слабее оценки Элайса-Бассалыги. Более того, при  $\delta = \frac{1}{2}$  правая часть (2.0.51) обращается в нуль в то время, как правая часть (2.0.50), равная  $1 - H_2\left(\frac{1}{4}\right)$ , больше нуля. В "защиту" оценки Хемминга следует сказать, что она, в отличие от оценки Элайса-Бассалыги, достигается или почти достигается при малых значениях  $d$ .

Следует также заметить, что рассматривая ниже оценка линейного программирования, позволяет усилить оценку Элайса-Бассалыги (2.0.51) на всем интервале  $0 < \delta < \frac{1}{2}$  изменения  $\delta$ .

**Лемма 2.0.7** (Асимптотическое поведение оценки Варшамова-Гилберта) *Имеют место оценки*

$$R(\delta) \geq 1 - H_2(\delta) \quad (\text{оценка Варшамова-Гилберта}) \quad (2.0.52)$$

Как нетрудно установить, разность между функцией  $1 - H_2(\delta)$  и функцией  $1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}\right)$  (оценка Бассалыги) всегда положительна, т.е. имеется существенный зазор между верхней и нижней оценками скорости кода с данным относительным кодовым расстоянием. Сужение этого зазора между верхними и нижними оценками является одной из основных задач теории кодирования.

Следует сказать, что оценка линейного программирования несколько ссужает указанный зазор, но не сводит его к нулю ни в одной точке интервала  $(0, \frac{1}{2})$  изменения  $\delta$ .

Заметим, что выписать оценку подобную (2.0.7) для линейных  $q$ -значных кодов также достаточно просто. Очень интересно, что эта оценка при  $q > 7$  может быть усилена с помощью построения хороших алгебро-геометрических кодов. Обсуждение этого вопроса выходит за рамки этой книги. (см. [1])

## 2.0.10 Основные задачи теории кодирования

В заключение вводной части мы скажем несколько общих слов о задачах решаемых в теории кодов, корректирующих ошибки.

Пространство, на котором естественно строить и изучать коды, корректирующие ошибки, обязательно должно быть компактным. Ибо в том случае, когда пространство некомпактно, на нем могут существовать коды с бесконечным числом элементов, что не очень естественно для их физической реализации.

Например, если число элементов кода в  $\mathcal{R}^n$  с ограниченным снизу евклидовым кодовым расстоянием является бесконечным, то физические сигналы, которые соответствуют кодовым последовательностям, должны иметь либо произвольно высокую энергию либо/и бесконечную длительность.

Вместе с тем "теория кодирования" на некоторых некомпактных пространствах давно и очень плодотворно изучается в рамках других направлений математики. Например, изучение протнейших упаковок шаров в  $n$ -мерном евклидовом пространстве (которое не является компактным) является одной из основных задач геометрии (см. [70]).

Мы рассматриваем коды, корректирующие ошибки, на компактном метрическом пространстве  $R$  с метрикой  $\lambda$ . Одной из главных задач в теории является задача построения кода  $\mathcal{K} \subset R$  с заданным кодовым расстоянием  $\lambda(\mathcal{K})$ , который имеет наибольшее число элементов.

Эту задачу можно сформулировать и несколько иначе: построить код  $\mathcal{K}$  с заданным числом элементов  $M$ , который имеет наибольшее кодовое расстояние  $\lambda(\mathcal{K})$ .

Эта задача часто уточняется. Например, требуется построить код, который является линейным, групповым или имеет легкое декодирование и т.п.

Коды имеют определенное число элементов, определяемое алгоритмом их построения. Вопрос о том насколько это число близко к максимально возможному весьма не прост. Стандартным способом ответа на этот вопрос являются оценки сверху числа элементов кода с заданным кодовым расстоянием.

В некоторых редких случаях оценка и число элементов конкретного кода совпадают, т.е. в этих случаях мы устанавливаем, что число элементов кода максимально. В общем же случае обычно наблюдается расхождение между числом элементов кода и верхней оценкой. Но и в этом случае это наблюдение имеет определенную ценность.

Перечислим некоторые важнейшие задачи общего плана теории кодов, корректирующих ошибки.

- Разработка методов построения кодов на различных компактных метрических пространствах.
- Разработка эффективных алгоритмов декодирования кодов, корректирующих ошибки.
- Вычисление отдельных параметров и свойств конкретных кодов, корректирующих ошибки. Например, вычисление спектра линейного кода или его группы автоморфизмов и т.п.
- Получение оценок (как верхних так и нижних) числа элементов кодов, корректирующих ошибки. В частности, было бы интересно сократить зазор между асимптотическими нижней оценкой скорости передачи и наилучшей известной ее верхней оценкой. В настоящее время этими оценками являются оценка Варшамова-Гилберта и оценка линейного программирования.

Без сомнения, вышеприведенный перечень задач теории кодирования может быть расширен.

## Глава 3

# Центральные функции на линейном пространстве Хемминга

### 3.1 Специальные функции

#### 3.1.1 Характеры

Мы рассматриваем конечную группу  $\mathfrak{G}$ . В настоящем разделе в большинстве случаев  $\mathfrak{G}$  — абелева группа. В начале этого раздела, когда мы еще не конкретизировали группу  $\mathfrak{G}$ , с которой мы работаем, в качестве групповой операции мы рассматриваем умножение  $\cdot$  элементов. В конце раздела, когда мы работаем с конкретными группами, например с группой  $\mathbb{F}_q^l$  ( $l$ – мерное пространство над конечным полем  $\mathbb{F}_q$ ), в качестве групповой операции мы, следуя традиции, используем операцию  $+$  (сложение).

Обозначим через  $S$  множество точек унитарного пространства  $\mathbb{C}$  с нормой равной 1. По другому,  $S$  — окружность радиуса 1 в комплексном пространстве  $\mathbb{C}$ . Множество  $S$ , очевидно, является группой, в которой групповой операцией является умножение комплексных чисел.

Пусть  $\mathfrak{G}$  — абелева группа. Функция  $\varpi : \mathfrak{G} \rightarrow S$  называется *характером группы  $\mathfrak{G}$* , если для нее выполнено следующее свойство

$$\varpi(\mathfrak{g}\mathfrak{h}) = \varpi(\mathfrak{g})\varpi(\mathfrak{h}) \text{ для всех } \mathfrak{g}, \mathfrak{h} \in \mathfrak{G}. \quad (3.1.1)$$

Произведение двух характеров  $\varpi, \varpi'$ , т.е. функция  $\varpi(\mathfrak{g})\varpi'(\mathfrak{g})$ , очевидно также является характером группы  $\mathfrak{G}$ . Поэтому множество  $\tilde{\mathfrak{G}}$  всех характеров группы  $\mathfrak{G}$  является абелевой группой, в которой групповой операцией является умножение функций.

Хорошо известно, что группы  $\mathfrak{G}$  и  $\tilde{\mathfrak{G}}$  являются изоморфными [41].

Пусть  $\mathfrak{h}$  — элемент  $\mathfrak{G}$ , который является прообразом элемента  $\varpi(\mathfrak{g}) \in \tilde{\mathfrak{G}}$  при некотором изоморфном отображении  $\mathfrak{G}$  в  $\tilde{\mathfrak{G}}$ . В этом случае элемент  $\varpi(\mathfrak{g})$  будем обозначать через  $\varpi_{\mathfrak{h}}(\mathfrak{g})$ .

**Лемма 3.1.1** Пусть  $\mathfrak{G}$  — абелева группа. В этом случае существует изоморфизм  $\rho$  группы  $\mathfrak{G}$  в группу характеров  $\tilde{\mathfrak{G}}$  такой, что

$$\varpi_{\mathfrak{h}}(\mathfrak{g}) = \varpi_{\mathfrak{g}}(\mathfrak{h}). \quad (3.1.2)$$

**Доказательство.** Представим требуемый изоморфизм  $\varrho$  в явном виде.

Хорошо известно [41], что любую конечную абелеву группу  $\mathfrak{G}$  можно представить как прямое произведение циклических групп  $\mathfrak{G}_1, \dots, \mathfrak{G}_k$  порядков  $r_1, \dots, r_k$ , соответственно. Таким образом, элемент  $\mathfrak{g} \in \mathfrak{G}$  можно записать как  $\mathfrak{g} = \mathfrak{g}_1 \cdots \mathfrak{g}_k$ , где  $\mathfrak{g}_j \in \mathfrak{G}_j$ . Каждая циклическая группа  $\mathfrak{G}_j$  порядка  $r_j$  изоморфна группе  $(\mathbb{Z}_{r_j}, +)$  (группа вычетов по mod  $r_j$ ). Поэтому мы можем полагать, что  $\mathfrak{G}_j = (\mathbb{Z}_{r_j}, +)$ .

Отсюда следует, что любой характер  $\varpi(\mathfrak{g}) \in \tilde{\mathfrak{G}}$  имеет вид  $\varpi(\mathfrak{g}) = \varpi^{(1)}(\mathfrak{g}_1) \cdots \varpi^{(k)}(\mathfrak{g}_k)$ , где  $\varpi^{(j)}$  — характер  $\mathfrak{G}_j$ . Каждый характер  $\varpi^{(j)}$  циклической группы  $\mathfrak{G}_j$  можно представить как

$$\varpi^{(j)}(\mathfrak{g}_j) = \varpi_{\mathfrak{h}_j}^{(j)}(\mathfrak{g}_j) = \exp\left(\frac{2\pi i \mathfrak{g}_j \mathfrak{h}_j}{r_j}\right), \quad \mathfrak{g}_j, \mathfrak{h}_j \in \mathbb{Z}_{r_j}, \quad (3.1.3)$$

с некоторым элементом  $\mathfrak{h}_j \in (\mathbb{Z}_{r_j}, +)$ . Для изоморфизма  $\varrho$ , реализующего отображение  $\varrho : \mathfrak{h}_1 \cdots \mathfrak{h}_k \rightarrow \varpi(\mathfrak{g}) = \varpi^{(1)}(\mathfrak{g}_1) \cdots \varpi^{(k)}(\mathfrak{g}_k)$  из  $\tilde{\mathfrak{G}}$  в  $\mathfrak{G}$ , очевидно, выполнено (3.1.2).  $\square$

### 3.1.2 Автоморфизмы группы $\mathfrak{G}$

Пусть  $\sigma$  — эндоморфизм группы  $\mathfrak{G}$ , т.е.  $\sigma$  — отображение  $\mathfrak{G}$  в себя, для которого выполнено

$$(\mathfrak{g}\mathfrak{h})^\sigma = \mathfrak{g}^\sigma \mathfrak{h}^\sigma \text{ для всех } \mathfrak{g}, \mathfrak{h} \in \mathfrak{G}. \quad (3.1.4)$$

На множестве  $\text{End}(\mathfrak{G})$  всех эндоморфизмов имеется естественная полугрупповая операция: суперпозиция двух эндоморфизмов. Таким образом,  $\text{End}(\mathfrak{G})$  является полугруппой, которая называется полугруппой эндоморфизмов группы  $\mathfrak{G}$ .

Подгруппа  $\text{End}(\mathfrak{G})$ , состоящая из всех взаимно однозначных функций со свойством (3.1.4), называется группой автоморфизмов группы  $\mathfrak{G}$  и обозначается через  $\text{Aut}(\mathfrak{G})$ . Отметим, что единицей группы  $\text{Aut}(\mathfrak{G})$  является тождественное отображение  $\sigma_0$ .

Примером автоморфизма является отображение  $\sigma : \mathfrak{g} \rightarrow \mathfrak{h}^{-1}\mathfrak{g}\mathfrak{h}$ , которое называется внутренним автоморфизмом группы  $\mathfrak{G}$ . Если  $\mathfrak{G}$  — некоммутативная группа, для некоторых  $\mathfrak{h}$  автоморфизм  $\sigma$  не является тождественным отображением, т.е. в этом случае группа  $\text{Inn}(\mathfrak{G})$ , порожденная указанными автоморфизмами, является нетривиальной (состоит из более, чем одного элемента). Группа  $\text{Inn}(\mathfrak{G})$  называется группой внутренних автоморфизмов. Для абелевой группы  $\mathfrak{G}$  группа  $\text{Inn}(\mathfrak{G})$  состоит из одного тождественного отображения. Следует сказать, что обычно группа  $\text{Inn}(\mathfrak{G})$  не исчерпывает все автоморфизмы даже для некоммутативной группы  $\mathfrak{G}$ . В коммутативном же случае это заведомо так.

Отображение  $\sigma : \mathfrak{g} \rightarrow \mathfrak{g}^r$  является эндоморфизмом для абелевой группы  $\mathfrak{G}$ . Если число  $r$  взаимно просто с порядком  $|\mathfrak{G}|$  группы  $\mathfrak{G}$ , то отображение  $\sigma$  является автоморфизмом  $\mathfrak{G}$ . Более того, если  $\mathfrak{G}$  — циклическая группа порядка  $N$ , то рассмотренные отображения  $\sigma$  исчерпывают все её автоморфизмы, т.е. в этом случае  $|\text{Aut}(\mathfrak{G})| = \varphi(|\mathfrak{G}|)$ , где  $\varphi(N)$  — функция Эйлера (число чисел  $r$ ,  $1 \leq r \leq N$ , взаимно простых с  $N$ ).

**Автоморфизмы группы характеров  $\tilde{\mathfrak{G}}$ , индуцируемые автоморфизмами абелевой группы  $\mathfrak{G}$**

Пусть  $\sigma \in \text{Aut}(\mathfrak{G})$ . Отображение

$$\tilde{\sigma} : \varpi(\mathfrak{g}) \rightarrow \varpi(\mathfrak{g}^\sigma) = \varpi^{\tilde{\sigma}}(\mathfrak{g}), \quad (3.1.5)$$

очевидно, является автоморфизмом группы характеров  $\tilde{\mathfrak{G}}$ . Отображение  $\tilde{\sigma}$  будем называть автоморфизмом группы  $\tilde{\mathfrak{G}}$ , индуцированным автоморфизмом  $\sigma$  группы  $\mathfrak{G}$ .

Если  $H$  — подгруппа  $\text{Aut}(\mathfrak{G})$ , то через  $\tilde{H}$  будем обозначать подгруппу  $\text{Aut}(\tilde{\mathfrak{G}})$ , состоящую из всех  $\tilde{\sigma}$ , определенных соотношением (3.1.5), для которых  $\sigma \in H$ . Из леммы 3.1.1 следует, что  $H$  и  $\tilde{H}$  — изоморфные группы.

Далее мы для простоты ограничимся рассмотрением только двух типов абелевых групп  $\mathfrak{G}$ :

- i.  $\mathfrak{G}$  — элементарная абелева группа.
- ii.  $\mathfrak{G}$  — циклическая группа.

Изучение других абелевых групп в конечном итоге сводится к изучению вышеуказанных типов групп.

### 3.1.3 Скалярное произведение

Элементы абелевой  $\mathfrak{G}$  и группы ее характеров  $\tilde{\mathfrak{G}}$  мы обозначаем через  $\mathfrak{g}$  и  $\varpi = \varpi_{\mathfrak{h}}$ , где  $\mathfrak{h}$  — элемент  $\mathfrak{G}$ , который является образом элемента  $\varpi(\mathfrak{g}) \in \tilde{\mathfrak{G}}$  при некотором фиксированном изоморфном отображении  $\tilde{\mathfrak{G}}$  в  $\mathfrak{G}$ .

Пусть  $f_1(\mathfrak{g})$  и  $f_2(\mathfrak{g})$  — функции, определенные на группе  $\mathfrak{G}$  со значениями в унитарном пространстве  $\mathbb{C}$ . Скалярное произведение функций  $f_1(\mathfrak{g})$ ,  $f_2(\mathfrak{g})$  определим соотношением

$$(f_1, f_2) = \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{g} \in \mathfrak{G}} f_1(\mathfrak{g}) \overline{f_2(\mathfrak{g})}, \quad (3.1.6)$$

где  $\bar{a}$ ,  $a \in \mathbb{C}$ , — число, комплексно сопряженное числу  $a$ .

**Лемма 3.1.2** Пусть

$$f_D(\mathfrak{g}) = \sum_{\varpi \in D} \varpi(\mathfrak{g}), \quad (3.1.7)$$

где  $D$  — подмножество элементов группы  $\tilde{\mathfrak{G}}^n$ .

Тогда

$$(f_D, f_{D'}) = |D \cap D'|. \quad (3.1.8)$$

В частности, если  $D \cap D' = \emptyset$ , то функции  $f_D, f_{D'}$  являются ортогональными:  $(f_D, f_{D'}) = 0$ .

**Доказательство.** Как хорошо известно, характеры  $\varpi$  и  $\varpi'$  являются ортонормированными функциями, т.е.  $(\varpi, \varpi') = 0$ , если  $\varpi \neq \varpi'$ , и  $(\varpi, \varpi) = 1$ . Отсюда непосредственно следует соотношение (3.1.8).  $\square$

В дальнейшем изложении в качестве подмножеств  $D \subset \tilde{\mathfrak{G}}$  будем рассматривать классы сопряженных элементов по некоторым подгруппам  $\tilde{H}$  группы автоморфизмов  $\text{Aut}(\tilde{\mathfrak{G}})$ . Объясним, что это такое.

### 3.1.4 Классы сопряженных элементов

**Определение 3.1.1** Пусть  $H$  — подгруппа группы автоморфизмов  $\text{Aut}(\mathfrak{G})$  и  $\mathfrak{g} \in \mathfrak{G}$ .

Множество  $A_{\mathfrak{g}} = \{\mathfrak{g}^\sigma \mid \sigma \in H\}$  называется классом сопряженных элементов относительно подгруппы автоморфизмов  $H$ .

Любой элемент  $\mathfrak{g}' \in A_{\mathfrak{g}}$  называется представителем класса  $A_{\mathfrak{g}}$ .

Очевидно классы  $A_{\mathfrak{g}}$  и  $A_{\mathfrak{g}'}$  либо совпадают, либо не пересекаются.

Предположим, что группа  $\mathfrak{G}$  распадается на  $1 + m$  различных классов сопряженных элементов относительно подгруппы автоморфизмов  $H$ , т.е.  $\mathfrak{G} = \bigcup_{s=0}^m A_{\mathfrak{g}_s}$ , где  $\mathfrak{g}_s$ ,  $s = 0, \dots, m$ , — представители различных классов сопряженных элементов. Занумерем каким-либо образом числами  $0, \dots, m$  эти классы, т.е. положим  $A_{\mathfrak{g}_s} = A_s$ . Условимся классу  $A_{\mathfrak{e}}$ , состоящему из одного элемента  $\mathfrak{e}$  (единица группы  $\mathfrak{G}$ ) сопоставлять число 0.

Как уже отмечалось, группы  $\mathfrak{G}$  и  $\tilde{\mathfrak{G}}$  являются изоморфными. Поэтому изоморфны их группы автоморфизмов  $\text{Aut}(\mathfrak{G})$  и  $\text{Aut}(\tilde{\mathfrak{G}})$ . Зафиксируем какой-либо изоморфизм  $\tilde{\rho} : \text{Aut}(\mathfrak{G}) \rightarrow \text{Aut}(\tilde{\mathfrak{G}})$ . Тогда подгруппе  $H$  будет соответствовать подгруппа  $\tilde{H} = \tilde{\rho}(H)$  группы автоморфизмов  $\text{Aut}(\tilde{\mathfrak{G}})$ .

Группа характеров  $\tilde{\mathfrak{G}}$  распадается на  $1 + m$  классов сопряженных элементов  $\tilde{A}_s = \tilde{\rho}(A_w)$ ,  $w \in \{0, \dots, m\}$ , относительно группы автоморфизмов  $\tilde{H}$ . Представителя класса  $\tilde{A}_w$ ,  $w \in \{0, \dots, m\}$ , будем обозначать через  $\varpi_w$ . Таким образом,  $\tilde{A}_w = \tilde{A}_{\varpi_w}$ , где  $\varpi_w$  — представитель класса  $\tilde{A}_w$ .

### 3.1.5 Центральные функции относительно подгруппы $H$ группы $\text{Aut}(\mathfrak{G})$

Рассмотрим линейное пространство  $W(\mathfrak{G})$  функций  $f(\mathfrak{x}) : \mathfrak{G} \rightarrow \mathbb{C}$ .

Очевидно, с одной стороны размерность линейного пространства  $W(\mathfrak{G})$  над  $\mathbb{C}$  равна  $|\mathfrak{G}|$  так как каждая функция из  $W(\mathfrak{G})$  однозначно задается своим значением на каждом элементе  $\mathfrak{G}$ .

С другой стороны, функции  $\varpi$  из группы характеров  $\tilde{\mathfrak{G}}$ ,  $|\tilde{\mathfrak{G}}| = |\mathfrak{G}|$ , являются линейно-независимыми, ибо они, как хорошо известно, являются попарно ортогональными. Поэтому в качестве базиса пространства  $W(\mathfrak{G})$  можно взять все элементы (характеры) группы  $\tilde{\mathfrak{G}}$ .

Таким образом, любую функцию  $f(\mathfrak{x}) \in W(\mathfrak{G})$  можно представить в виде

$$f(\mathfrak{x}) = \sum_{\varpi \in \tilde{\mathfrak{G}}} a_{\varpi} \varpi(\mathfrak{x}), \quad a_{\varpi} \in \mathbb{C}. \quad (3.1.9)$$

Так как характеры  $\varpi(\mathfrak{x})$  являются ортонормированными функциями, то коэффициенты  $a_{\varpi}$  определяются соотношением (Упражнение)

$$a_{\varpi} = (f(\mathfrak{x}), \varpi(\mathfrak{x})). \quad (3.1.10)$$



**Определение 3.1.2** Пусть  $H$  — подгруппа группы  $\text{Aut}(\mathfrak{G})$ . Функция  $f(\mathfrak{x})$ ,  $f(\mathfrak{x}) \in W(\mathfrak{G}^n)$ , называется центральной относительно группы  $H$ , если  $f(\mathfrak{x}) = f(\mathfrak{x}^\varphi)$  для всех  $\varphi \in H$  и всех  $\mathfrak{x} \in \mathfrak{G}$ .

Другими словами, пусть  $A_g = \{g^\varphi | \varphi \in H\}$  — класс сопряженных элементов группы  $\mathfrak{G}^n$  относительно группы  $H$  с представителем  $g \in \mathfrak{G}_l$  и пусть  $A_g = A_s$ . По определению, функция  $f$  является центральной тогда и только тогда, когда она принимает одно и то же значение на всех элементах каждого смежного класса  $A_s$ ,  $s = 0, \dots, m$ .

Пример. Пусть  $\mathfrak{G} = \mathbb{F}_p^l$  —  $l$ -мерное пространство над простым полем  $\mathbb{F}_p$  (групповой операцией в этой группе является сложение) и  $H = \text{Aut}(\mathfrak{G})$ . Напомним, что действия элементов из  $\text{Aut}(\mathfrak{G})$  могут быть реализованы как умножение векторов из  $\mathbb{F}_p^l$  на матрицы из  $M_l(\mathbb{F}_p)$  (группа невырожденных  $l \times l$ -матриц, в которой групповой операцией является умножение матриц). Группа  $\mathbb{F}_p^l$  относительно группы всех ее автоморфизмов  $\text{Aut}(\mathbb{F}_p^l)$  разбивается на два класса сопряженных элементов:  $A_0 = \{0\}$  и  $A_1 = \mathbb{F}_p^l \setminus \{0\}$ , т.е.  $m = 1$ . (Упражнение)

Продолжим этот пример. Для того, чтобы аддитивная группа  $\mathbb{F}_p^l$  разбивалась на два класса сопряженных элементов  $A_0$  и  $A_1$  совсем не обязательно использовать всю группу автоморфизмов  $\text{Aut}(\mathbb{F}_p^l)$ . Можно использовать ее подгруппу. Например, указанное разбиение реализуется с помощью подгруппы  $\overline{\mathbb{F}}_q^*$  группы  $\text{Aut}(\mathbb{F}_p^l)$ . Группа  $\overline{\mathbb{F}}_q^*$  образована всеми автоморфизмами вида  $\mathbf{x} \rightarrow \mathbf{a}\mathbf{x}$ ,  $\mathbf{a} \in F_q^*$ , где ненулевые векторы  $\mathbf{x}$  и  $\mathbf{a}$  трактуются как элементы конечного поля  $\mathbb{F}_{p^l}$  (расширения степени  $l$  поля  $\mathbb{F}_p$ ). Эта подгруппа имеет  $q-1$  элементов и изоморфна мультипликативной группе  $\mathbb{F}_q^*$  поля  $\mathbb{F}_q$ .

Легко также установить, что классы  $\tilde{A}_w$  сопряженных элементов относительно группы характеров  $\tilde{H} = \overline{\mathbb{F}}_p^l$  имеют вид  $\tilde{A}_0 = \{1\}$  (характер тождественно равный 1 на  $\mathfrak{G}_l$ , который является единицей группы  $\overline{\mathbb{F}}_p^l$ ) и  $\tilde{A}_1 = \overline{\mathbb{F}}_p^l \setminus \{1\}$ . (Упражнение) Эта тема более подробно будет рассмотрена в разделе 3.2.1. Переходим к изложению необходимых результатов в общем случае.

Определим функцию  $\Phi_H(\mathfrak{x}, \varpi)$  с помощью соотношения

$$\Phi_H(\mathfrak{x}, \varpi) := \sum_{\varphi \in H} \varpi(\mathfrak{x}^\varphi) \quad (3.1.11)$$

Легко установить, что (Упражнение)

$$\Phi_H(\mathfrak{x}, \varpi) = |St(\mathfrak{x})| \sum_{\mathfrak{y} \in A_s} \varpi(\mathfrak{y}), \text{ если } \mathfrak{x} \in A_s, \quad (3.1.12)$$

где  $St(\mathfrak{x})$  — стабилизатор элемента  $\mathfrak{x}$  в группе  $H$ , т.е.  $St(\mathfrak{x})$  — подгруппа  $H$ , элементы которой оставляют на месте элемент  $\mathfrak{x}$ . Отметим, что  $St(\mathfrak{x}) = St(\mathfrak{y})$ , если  $\mathfrak{x}$  и  $\mathfrak{y}$  принадлежат одному и тому же классу сопряженных элементов  $A_s$ . (Упражнение)

Очевидно, функция  $\Phi_H(\mathfrak{x}, \varpi)$  от переменного  $\mathfrak{x}$  при любом  $\varpi \in \tilde{\mathfrak{G}}$  является центральной относительно группы  $H$ . Это очевидный и важный факт.

Предположим, что  $\varpi \in \tilde{A}_w$  и  $\mathfrak{x} \in A_s$ ,  $w, s \in \{0, \dots, m\}$ ,  $\varpi^{\tilde{\varphi}}(\mathfrak{x}) = \varpi(\mathfrak{x}^\varphi)$  — характер, индуцированный автоморфизмом  $\varphi \in H$  (см. раздел 3.1.2), и  $\tilde{H} = \tilde{\rho}(H)$  (см. раздел 3.1.4). Как следует из (3.1.11) функцию  $\Phi_H(\mathfrak{x}, \varpi)$  (см. (3.1.11) и (3.1.12)) можно представить в виде

$$\Phi_H(\mathfrak{x}, \varpi) = \sum_{\varphi \in H} \varpi(\mathfrak{x}^\varphi) = |St(\mathfrak{x})| \sum_{\mathfrak{y} \in A_s} \varpi(\mathfrak{y}) = \sum_{\tilde{\varphi} \in \tilde{H}} \varpi^{\tilde{\varphi}}(\mathfrak{x}) = |St(\varpi)| \sum_{\varpi' \in \tilde{A}_w} \varpi'(\mathfrak{x}), \quad (3.1.13)$$

где  $St(\mathfrak{x})$  — стабилизатор элемента  $\mathfrak{x}$  в группе  $H$  и  $St(\varpi)$  — стабилизатор элемента  $\varpi$  в группе  $\tilde{H}$ .

Как нетрудно установить (Упражнение), значение функции  $\Psi_H(s, \varpi) = \sum_{\mathfrak{y} \in A_s} \varpi(\mathfrak{y})$  зависит только от класса сопряженных элементов  $\tilde{A}_w$ , к которому принадлежит характер  $\varpi$ , а значение  $|St(\mathfrak{x})|$  — только от класса сопряженных элементов  $A_s$ , к которому принадлежит элемент  $\mathfrak{x}$ . Эти значения функций  $\Psi_H(s, \varpi)$  и  $|St(\mathfrak{x})|$  мы обозначим через  $P_H(s, w) = \sum_{\mathfrak{y} \in A_s} \varpi(\mathfrak{y})$  и  $S_H(s)$ , соответственно. Отсюда и из (3.1.13) вытекает

$$\Phi_H(\mathfrak{x}, \varpi) = S_H(s)P_H(s, w) = \tilde{S}_{\tilde{H}}(w)\tilde{P}_{\tilde{H}}(w, s), \text{ если } \mathfrak{x} \in A_s, \varpi \in \tilde{A}_w, \quad (3.1.14)$$

где функции  $\tilde{P}_{\tilde{H}}(w, s)$  и  $\tilde{S}_{\tilde{H}}(w)$ , заданные группами  $\tilde{\mathfrak{G}}$  и  $\tilde{H}$ , определяются также как и функции  $P_H(s, w)$  и  $S_H(s)$ :  $\tilde{P}_{\tilde{H}}(w, s) = \sum_{\varpi \in \tilde{A}_w} \varpi(\mathfrak{x})$ , если  $\mathfrak{x} \in \tilde{A}_w$ , и  $\tilde{S}_{\tilde{H}}(w) = |St(\varpi)|$ .

Заметим, что  $|H| = S_H(s)|A_s| = |\tilde{S}_{\tilde{H}}(w)||\tilde{A}_w|$ . (Упражнение) Отсюда и (3.1.14) непосредственно следует

**Лемма 3.1.3** *Имеет место равенство*

$$|\tilde{A}_w|P_H(s, w) = |A_s|\tilde{P}_{\tilde{H}}(w, s). \quad (3.1.15)$$

Если обозначить через  $s_H(\mathfrak{x})$  целозначную функцию, принимающую значение  $s \in \{0, \dots, m\}$ , если  $\mathfrak{x} \in A_s$ , а через  $w_{\tilde{H}}(\varpi)$  — функцию, принимающую значение  $w \in \{0, \dots, m\}$ , если  $\varpi \in \tilde{A}_w$ , то равенство (3.1.13) с произвольными  $\mathfrak{x} \in \mathfrak{G}, \varpi \in \tilde{\mathfrak{G}}$  можно представить в виде

$$\Phi_H(\mathfrak{x}, \varpi) = S_H(s_H(\mathfrak{x}))P_H(s_H(\mathfrak{x}), w_{\tilde{H}}(\varpi)) = \tilde{S}_{\tilde{H}}(w_{\tilde{H}}(\varpi))\tilde{P}_{\tilde{H}}(w_{\tilde{H}}(\varpi), s_H(\mathfrak{x})), \quad (3.1.16)$$

а функцию

$$Y_w(\mathfrak{x}) = \sum_{\varpi \in \tilde{A}_w} \varpi(\mathfrak{x}) \quad (3.1.17)$$

в виде

$$Y_w(\mathfrak{x}) = \tilde{P}_{\tilde{H}}(w, s_H(\mathfrak{x})). \quad (3.1.18)$$

Отметим, что при любом  $w$  функция  $Y_w(\mathfrak{x})$  является центральной относительно подгруппы автоморфизмов  $H$ , т.е. принимает одинаковые значения на каждом классе сопряженных элементов  $A_s$ .

**Теорема 3.1.1**

*и. Функции  $\tilde{P}_{\tilde{H}}(w, s)$ ,  $w = 0, \dots, m$ , являются ортогональными с весами  $|A_s|$ , где  $A_s$ ,  $s = 0, \dots, m$ , — класс сопряженных элементов группы  $\mathfrak{G}$  относительно группы ее автоморфизмов  $H$ , т.е.*

$$\frac{1}{|\mathfrak{G}|} \sum_{s=0}^m |A_s| \tilde{P}_{\tilde{H}}(w, s) \tilde{P}_{\tilde{H}}(w', s) = \begin{cases} 0, & \text{если } w \neq w' \\ |\tilde{A}_w|, & \text{если } w = w', \end{cases} \quad (3.1.19)$$

ii. Каждая центральная функция  $f(\mathfrak{x})$  относительно группы  $H$  может быть записана в виде

$$f(\mathfrak{x}) = \sum_{w=0}^m b_w \tilde{P}_{\tilde{H}}(w, s), \quad b_w \in \mathbb{C}, \text{ если } \mathfrak{x} \in A_s. \quad (3.1.20)$$

**Доказательство.** Из того, что функция  $Y_w(\mathfrak{x})$  является центральной относительно группы автоморфизмов  $H$ , из определения скалярного произведения  $(f(\mathfrak{x}), f'(\mathfrak{x}))$  функций  $f(\mathfrak{x}) = Y_w(\mathfrak{x})$  и  $f'(\mathfrak{x}) = Y_{w'}(\mathfrak{x})$ , из соотношения (3.1.18) и из равенства  $\mathfrak{G} = \cup_{s=0}^m A_s$  — разбиения группы  $\mathfrak{G}$  на классы сопряженных элементов, следуют соотношения

$$(Y_w(\mathfrak{x}), Y_{w'}(\mathfrak{x})) = \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{x} \in \mathfrak{G}} Y_w(\mathfrak{x}) Y_{w'}(\mathfrak{x}) = \frac{1}{|\mathfrak{G}|} \sum_{s=0}^m \sum_{\mathfrak{x} \in A_s} Y_w(\mathfrak{x}) Y_{w'}(\mathfrak{x}) = \frac{1}{|\mathfrak{G}|} \sum_{s=0}^m |A_s| \tilde{P}_{\tilde{H}}(w, s) \tilde{P}_{\tilde{H}}(w', s). \quad (3.1.21)$$

Если  $w \neq w'$ , то  $\tilde{A}_w \cap \tilde{A}_{w'} = \emptyset$ . Поэтому из леммы 3.1.2 и соотношения (3.1.17) вытекает, что в этом случае  $(Y_w(\mathfrak{x}), Y_{w'}(\mathfrak{x})) = 0$ . Таким образом, мы доказали справедливость первого равенства в (3.1.19).

Второе равенство в (3.1.19) вытекает также из леммы 3.1.2, ибо

$$(Y_w(\mathfrak{x}), Y_w(\mathfrak{x})) = \left( \sum_{\varpi \in \tilde{A}_w} \varpi(\mathfrak{x}), \sum_{\varpi \in \tilde{A}_w} \varpi(\mathfrak{x}) \right) = |\tilde{A}_w|. \quad (3.1.22)$$

Пункт ii. теоремы очевидным образом вытекает из представления (3.1.9).  $\square$

Свойства функций  $P_{\tilde{H}}(w, s)$  могут быть дополнительно конкретизированы для некоторых групп  $H$ . В частности, для элементарной абелевой группы  $\mathfrak{G}$  и некоторых подгрупп  $H$  группы  $\text{Aut}(\tilde{\mathfrak{G}})$  функция  $P_{\tilde{H}}(w, s)$  может быть вычислена в явном виде. При соответствующей нумерации смежных классов  $\tilde{A}_w$  функция  $P_{\tilde{H}}(w, s)$  является многочленом от одного или нескольких переменных степени  $w$ . Эти вопросы будут рассмотрены в следующих разделах.

## 3.2 Ортогональные многочлены

### 3.2.1 Элементарная абелева группа

Элементами элементарной абелевой группы  $\mathfrak{G}_l = (\mathbb{F}_p^l, +)$  являются  $l$ -мерные векторы  $\mathbf{a} = (a_1, \dots, a_l) \in \mathbb{F}_p^l$ . Групповая операция — покомпонатное сложение по  $\text{mod } p$ , где  $p$  — простое число.

Хорошо известно, что группу автоморфизмов  $\text{Aut}(\mathfrak{G})$  группы  $(\mathbb{F}_p^l, +)$  образуют группа невырожденных линейных отображений. Её элементами  $\varpi \in \text{Aut}(\mathfrak{G})$  являются линейные функции  $\varpi : \mathbf{a} \rightarrow \mathbf{a}A$ ,  $A \in M_l(\mathbb{F}_p)$ , где  $M_l(\mathbb{F}_p)$  — мультипликативная группа невырожденных  $l \times l$ -матриц с элементами из поля  $\mathbb{F}_p$ . Таким образом, группа  $\text{Aut}(\mathfrak{G}_l)$  для элементарной абелевой группы изоморфна группе невырожденных матриц  $M_l(\mathbb{F}_p)$ . Отметим, что при  $l > 1$   $\text{Aut}(\mathfrak{G}_l)$  — некоммутативная группа.

В некоторых случаях удобно рассматривать не всю группу  $\text{Aut}(\mathfrak{G}_l)$ , а ее коммутативную подгруппу  $\mathbb{F}(\mathfrak{G}_l)$ , элементы которой реализуют умножение элементов  $\mathbf{a} \in \mathbb{F}_p^l$  на

ненулевые элементы конечного поля  $\mathbb{F}_{p^l}$ . Заметим, что  $\mathbb{F}_p^l$  и  $\mathbb{F}_{p^l}$  — разные объекты: первый — линейное пространство, а второй — конечное поле, аддитивная группа которого совпадает с пространством  $\mathbb{F}_{p^l}$ .

Поясним это подробнее. Мы рассматриваем элемент  $\mathbf{a} = (a_1, \dots, a_l) \in \mathbb{F}_p^l$  как элемент  $\widehat{\mathbf{a}}$  поля  $\mathbb{F}_q$ ,  $q = p^l$ , который имеет представление  $\widehat{\mathbf{a}} = \sum_{i=1}^l a_i \omega_i$  в некотором базисе  $\Omega = \{\omega_1, \dots, \omega_l\}$  поля  $\mathbb{F}_q$  над полем  $\mathbb{F}_p$ . В этом базисе произведению  $\alpha \widehat{\mathbf{a}}$ ,  $\alpha \in \mathbb{F}_q^*$ , очевидно, соответствует вектор  $\mathbf{a} A_\alpha$ , координатами которого являются координаты представления элемента  $\alpha \widehat{\mathbf{a}}$  в базисе  $\Omega$ , где  $A_\alpha$  — некоторая невырожденная матрица. Подгруппа  $\mathbb{F}(\mathfrak{G}_l)$  образована всеми матрицами  $A_\alpha$ ,  $\alpha \in \mathbb{F}_q$ ,  $\alpha \neq 0$ . Очевидно,  $\mathbb{F}(\mathfrak{G}_l) \sim \mathbb{F}_{p^l}^*$  (мультипликативная группа поля  $\mathbb{F}_{p^l}$ ) и, следовательно,  $|\mathbb{F}(\mathfrak{G}_l)| = p^l - 1$ .

Отметим, группа автоморфизмов  $\mathbb{F}(\mathfrak{G}_l)$  действует на множестве ненулевых элементов пространства  $\mathfrak{G}_l = \mathbb{F}_p^l$  транзитивно, т.е. для любых двух ненулевых векторов  $\mathbf{a}, \mathbf{b}$  в группе  $\mathbb{F}(\mathfrak{G}_l)$  найдется элемент  $\sigma$ , который переводит  $\mathbf{a}$  в  $\mathbf{b}$ :  $\sigma : \mathbf{a} \rightarrow \mathbf{b}$ . Отсюда, в частности, следует, что группа  $\mathfrak{G}_l$  разбивается на два класса сопряженных элементов:  $A_0 = \{\mathbf{0}\}$  и  $A_1 = \mathfrak{G}_l \setminus \{\mathbf{0}\}$  относительно группы  $\mathbb{F}(\mathfrak{G}_l)$ .

Рассмотрим прямое произведение  $\mathfrak{G}_l^n$   $n$  групп  $\mathfrak{G}_l$ . Очевидно, это тоже элементарная абелева. Ее элементами являются векторы  $\mathbf{x} = (x_1, \dots, x_n)$ ,  $x_s \in \mathfrak{G}_l$ , длины  $ln$  с координатами из поля  $\mathbb{F}_p$ . Вместе с тем группу  $\mathfrak{G}_l^n$  можно рассматривать и как прямое произведение  $n$  экземпляров аддитивной группы конечного поля  $\mathbb{F}_q$ ,  $q = p^l$ .

На группе  $\mathfrak{G}_l^n$  рассмотрим отображение

$$\sigma : (x_1, \dots, x_n) \rightarrow (x_{i_1} \alpha_1, \dots, x_{i_n} \alpha_n), \quad \alpha_s \in \mathbb{F}_q \setminus \{0\}, \quad (3.2.1)$$

где

$$\lambda = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix} \quad (3.2.2)$$

— перестановка, действующая на множестве индексов векторов из  $\mathbb{F}_q^n$ . Заметим, что в нижней строке  $\lambda$  все элементы  $i_s \in \{1, 2, \dots, n\}$  различны. Множество всех перестановок образует некоммутативную группу, в которой групповой операцией является, определенное очевидным образом, умножение двух перестановок. Эта группа, обозначаемая через  $S_n$ , и называется симметрической. Ее порядок равен  $n!$ .

Элементы  $S_n$  можно рассматривать как взаимно-однозначное отображение множества  $\{1, 2, \dots, n\}$  в себя. Очевидно, группа  $S_n$   $r$ -транзитивна, т.е. для любых двух наборов  $i_1, \dots, i_r$  и  $j_1, \dots, j_r$  каждый с различными элементами существует в  $S_n$  элемент, который переводит один набор в другой.

Отображение  $\sigma$  может быть представлено и несколько иным образом:

$$\sigma : \mathbf{x} \rightarrow \mathbf{x} \Lambda, \quad (3.2.3)$$

где  $\Lambda = \Gamma \cdot D$  и  $D$  — невырожденная диагональная матрица, на диагонали которой находятся ненулевые элементы  $\alpha_s$  поля  $\mathbb{F}_q$ , а  $\Gamma$  — перестановочная  $n \times n$ -матрица, реализующая перестановку  $\lambda$ , т.е. матрица, переставляющая координаты вектора  $\mathbf{x}$ . Другими словами,  $\Lambda$  — матрица, у которых в каждой строке и в каждом столбце имеется только один ненулевой элемент поля  $\mathbb{F}_q$ .

Множество всех матриц  $\Lambda$  является некоммутативной группой, которая обозначается далее через  $\mathfrak{M}_n(\mathbb{F}_q)$ . Она носит название мономиальной и, как нетрудно установить, имеет порядок  $n!(q-1)^n$ .

Очевидно, группа  $\mathfrak{M}_n(\mathbb{F}_q)$  является подгруппой группы  $\text{Aut}(\mathfrak{G}_1^n)$ .

Как уже было отмечено, группа автоморфизмов  $\mathbb{F}(\mathfrak{G}_l)$  действует на множестве ненулевых элементов пространства  $\mathfrak{G}_l = \mathbb{F}_p^l$  транзитивно. Симметрическая группа является  $r$ -транзитивной при любом  $r$ ,  $0 < r \leq n$ . Из этих двух утверждений непосредственно вытекает

**Лемма 3.2.1** *Множество  $A_s$ , состоящее из всех векторов  $\mathbf{a} \in \mathbb{F}_q^n$  веса  $s$ , является классом сопряженных элементов относительно группы  $\mathfrak{M}_n(\mathbb{F}_q)$ . Число элементов класса  $A_s$  равно  $|A_s| = \binom{n}{s}(q-1)^s$ .*

### Характеры группы $\mathfrak{G}_l^n$

Сначала рассмотрим характеры группы  $\mathfrak{G}_l$ . Элементы  $\mathfrak{G}_l$  будем записывать в виде  $l$ -мерного вектора с координатами из поля  $\mathbb{F}_p$ , обозначаемого полужирными буквами из первого или последнего регистра латинского алфавита, например,  $\mathbf{x} = (x_1, \dots, x_l)$ . Элементы двойственного пространства  $\widetilde{\mathfrak{G}}_l$  будем обозначать полужирными греческими буквами.

Очевидно, функция

$$\varpi_{\mathbf{a}}(\mathbf{x}) = \exp\left(\frac{2\pi i \langle \mathbf{a}, \mathbf{x} \rangle}{p}\right), \quad \mathbf{a} \in \mathfrak{G}_l, \quad (3.2.4)$$

где  $\langle \mathbf{a}, \mathbf{x} \rangle = \sum_{k=1}^l a_k x_k$  — скалярное произведение в поле  $\mathbb{F}_p$ , является характером группы  $\mathfrak{G}_l$ . Также очевидно, что все характеры исчерпываются функциями, указанного вида.

Естественно рассматривать (что и мы будем делать всюду далее) в качестве изоморфизма между  $\mathfrak{G}_l$  и  $\widetilde{\mathfrak{G}}_l$  изоморфизм  $\rho$ , который сопоставляет элементу  $\mathbf{a} \in \mathfrak{G}_l$  характер  $\varpi_{\mathbf{a}}(\mathbf{x})$ .

Отметим, что для так определенных характеров выполнено равенство (3.1.2).

В рассматриваемом случае автоморфизм  $\sigma$  из группы  $\mathbb{F}(\mathfrak{G}_l) \subset \text{Aut}(\mathfrak{G}_l)$  действуют на элементах  $\mathbf{a} \in \mathfrak{G}_l$  способом, указанным в соотношении (3.2.1).

Для любого  $\varphi \in \text{Aut}(\mathfrak{G}_l)$

$$\varpi_{\mathbf{a}}(\mathbf{x}^\varphi) = \exp\left(\frac{2\pi i \langle \mathbf{a}, \mathbf{x}^\varphi \rangle}{p}\right) = \exp\left(\frac{2\pi i \langle \mathbf{a}'^\varphi, \mathbf{x} \rangle}{p}\right) = \varpi_{\mathbf{a}'}(\mathbf{x}), \quad (3.2.5)$$

где  $\varphi^T$  сопряженный к  $\varphi$  автоморфизм и  $\mathbf{a}' = \mathbf{a}^{\varphi^T}$ . Если  $\varphi : \mathbf{x} \rightarrow \mathbf{x}A$ , где  $A$  — невырожденная  $l \times l$ -матрица над  $\mathbb{F}_p$ , то, как нетрудно установить,  $\varphi^T : \mathbf{x} \rightarrow \mathbf{x}A^T$ , где  $A^T$  — транспонированная матрица  $A$ .

В качестве упомянутого в разделе 3.1.4 изоморфизма  $\tilde{\rho}$  между  $\mathfrak{G}_l$  и  $\widetilde{\mathfrak{G}}_l$  далее будем рассматривать изоморфизм, который сопоставляет автоморфизму  $\varphi \in \text{Aut}(\mathfrak{G}_l)$  автоморфизм  $\tilde{\varphi} : \varpi_{\mathbf{a}}(\mathbf{x}) \rightarrow \varpi_{\mathbf{a}^\varphi}(\mathbf{x}) = \varpi_{\mathbf{a}'}(\mathbf{x}) = \varpi_{\mathbf{a}'}^\varphi(\mathbf{x})$  группы  $\mathfrak{G}$ , где  $\mathbf{a}' = \mathbf{a}^{\varphi^T}$ . Очевидно, автоморфизм  $\tilde{\varphi}$  реализуется также и с помощью отображения  $\varpi_{\mathbf{a}}(\mathbf{x}) \rightarrow \varpi_{\mathbf{a}}(\mathbf{x}^\varphi)$ .

Характеры группы  $\mathfrak{G}_l^n$ . Очевидно, характерами  $\mathfrak{G}_l^n$  являются все функции вида

$$\varpi_a(x) = \exp\left(\frac{2\pi i \langle a, x \rangle}{p}\right), \quad a \in \mathfrak{G}_l^n, \quad (3.2.6)$$

где скалярное произведение  $\langle a, x \rangle$ ,  $a, x \in \mathfrak{G}_l^n$ ,  $a = (a_1, \dots, a_n)$ , в поле  $\mathbb{F}_p$  удобно записать в следующем виде:  $\langle a, x \rangle = \langle a_1, x_1 \rangle + \dots + \langle a_n, x_n \rangle$ , где слагаемые — скалярные произведения векторов из группы  $\mathfrak{G}_l$ .

Элемент  $\Lambda = \Gamma \cdot D$  мономиальной группы  $\mathfrak{M}_n(\mathbb{F}_p)$  действует на  $\mathfrak{G}_l^n$ , способом указанным в соотношении 3.2.1, где под  $\sigma$  понимается отображение  $\sigma : x \rightarrow x\Lambda$ .

Отметим, что характер  $\varpi_a(x^\sigma) = \varpi_{a'}(x)$ , индуцированный автоморфизмом  $\sigma$ , порождается вектором  $a' = a\Lambda$ . (Упражнение)

**Лемма 3.2.2** Множество  $\tilde{A}_w$ , состоящее из всех характеров  $\varpi_a(x)$ , у которых  $wt(a) = w$ , является классом сопряженных элементов (орбитой) относительно подгруппы  $\tilde{\mathfrak{M}}_n(\mathbb{F}_q)$  группы  $\text{Aut}(\mathfrak{G}_1)$ , где  $\tilde{\mathfrak{M}}_n(\mathbb{F}_q)$  — изоморфный образ мономиальной группы  $\mathfrak{M}_n(\mathbb{F}_q)$  в группе автоморфизмов группы характеров  $\tilde{\mathfrak{G}}_n$ .

Класс сопряженных элементов  $\tilde{A}_w$  имеет  $|\tilde{A}_w| = \binom{n}{w}(q-1)^w$  элементов.

### 3.2.2 Примарная группа порядка $p^l$

#### Примарная группа

Примарная группа  $\mathfrak{P}_l$  определяется как аддитивная группа кольца  $Z_{p^l}$  вычетов по mod  $p^l$ , где  $p$  — простое. Число вида  $p^l$  называется примарным. Группа  $\mathfrak{P}_l = (Z_{p^l}, +)$  имеет  $l-1$  нетривиальных подгрупп, образованных элементами кратными числу  $p^s$ ,  $s = 1, \dots, l-1$ . Соответственно, мы будем рассматривать  $n$ -ую степень группы  $\mathfrak{P}_l$ :  $\mathfrak{P}_l^n = (Z_{p^l}^n, +)$ .

Группа автоморфизмов  $\text{Aut}(\mathfrak{P}_1)$  группы  $\mathfrak{P}_l$ , очевидно, образована отображениями

$$\sigma : x \rightarrow ax, \quad \text{где } a \in \mathfrak{P}_l \text{ и } (a, p) = 1. \quad (3.2.7)$$

Таким образом,  $|\text{Aut}(\mathfrak{P}_1)| = \varphi(p^l) = p^{l-1}(p-1)$ , где  $\varphi$  — функция Эйлера.

Группа  $\mathfrak{P}_l$  разбивается на  $1+l$  классов сопряженных элементов  $A_s$ ,  $s = 0, \dots, l$  относительно группы ее автоморфизмов  $\text{Aut}(\mathfrak{P}_1)$ . Каждый класс  $A_s$  состоит из чисел  $a \in Z_{p^l}$ , которые делятся на  $p^{l-s}$ , но не делятся на  $p^{l-s+1}$ . Очевидно,  $|A_s| = \varphi(p^s)$ . (Упражнение)

Группу автоморфизмов  $\text{Aut}(\mathfrak{P}_1^n)$ ,  $n > 1$ , группы  $\mathfrak{P}_l^n = (Z_{p^l}^n, +)$  мы рассматривать не будем, хотя это сделать и не очень трудно. Мы будем работать только с ее подгруппой  $\mathfrak{M}_n(\mathfrak{P}_l)$ , которая похожа на подгруппу  $\mathfrak{M}_n(\mathfrak{G}_l)$  из предыдущего раздела.

А именно, группа автоморфизмов  $\mathfrak{M}_n(\mathfrak{P}_l)$  состоит из всех отображений вида

$$\sigma : (x_1, \dots, x_n) \rightarrow (x_{i_1}^{\sigma_1}, \dots, x_{i_n}^{\sigma_n}), \quad \sigma_s \in \text{Aut}(\mathfrak{P}_1), \quad x_j \in \mathfrak{P}_1, \quad (3.2.8)$$

где

$$\lambda = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix} \quad (3.2.9)$$

— перестановка, действующая на множестве индексов векторов с координатами из группы  $\mathfrak{P}_l$ . Очевидно,  $|\mathfrak{M}_n(\mathfrak{P}_l)| = (p-1)p^{l-1}n!$ .

Обозначим через  $c_s(\mathbf{x})$ ,  $\mathbf{x} \in \mathfrak{P}_l^n$ , число координат вектора  $\mathbf{x}$ , которые принадлежат классу сопряженных элементов  $A_s$  и через  $\mathbf{c}(\mathbf{x})$  —  $l+1$ -мерный вектор  $\mathbf{c}(\mathbf{x}) = (c_0, c_1(\mathbf{x}), \dots, c_l(\mathbf{x}))$ .

**Лемма 3.2.3** Пусть  $\mathbf{c} = (c_0, \dots, c_l)$ ,  $c_0 + \dots + c_l = n$ , —  $l+1$ -мерный вектор с целыми координатами. Множество  $A_{\mathbf{c}}$ , состоящее из всех векторов  $\mathbf{a} \in \mathfrak{P}_l^n$ , у которых  $\mathbf{c}(\mathbf{x}) = \mathbf{c}$ , является классом сопряженных элементов относительно группы  $\mathfrak{M}_n(\mathfrak{P}_l^n)$ . Орбита (класс сопряженных элементов)  $A_{\mathbf{c}}$  имеет  $|A_{\mathbf{c}}| = \binom{n}{c_0, \dots, c_l} |A_0|^{c_0} \dots |A_l|^{c_l}$  элементов, где  $\binom{n}{c_0, \dots, c_l} = \frac{n!}{c_0! \dots c_l!}$ .

**Доказательство** очевидно.

Отметим, что  $|A_0| = 1$ , поэтому  $|A_{\mathbf{c}}| = \binom{n}{c_0, \dots, c_l} |A_1|^{c_1} \dots |A_l|^{c_l}$ .

### Характеры группы

Каждый характер  $\varpi$  примарной группы  $\mathfrak{P}_l$  имеет вид

$$\varpi_a(\mathbf{x}) = \exp\left(\frac{2\pi i \mathbf{a} \cdot \mathbf{x}}{p^l}\right), \quad \mathbf{a} \in \mathfrak{P}_l. \quad (3.2.10)$$

Группу характеров группы  $\mathfrak{P}_l$  мы обозначаем через  $\widetilde{\mathfrak{P}}_l$ .

Из (3.2.10) вытекает, что функция

$$\varpi_{\mathbf{a}}(\mathbf{x}) = \exp\left(\frac{2\pi i \langle \mathbf{a}, \mathbf{x} \rangle}{p}\right), \quad \mathbf{a} \in \mathfrak{P}_l^n, \quad (3.2.11)$$

где  $\langle \mathbf{a}, \mathbf{x} \rangle$  — скалярное произведение в кольце  $Z_{p^l}$ , является характером группы  $\mathfrak{P}_l^n$ . Для группы  $\widetilde{\mathfrak{P}}_l$ , изоморфной группе  $\mathfrak{P}_l$ , справедлива лемма, аналогичная лемме 3.2.3. Эту лемму мы выписывать не будем. Заметим только, что классы сопряженных элементов группы характеров  $\mathfrak{P}_l$ , будем обозначать символом  $\tilde{A}_{\mathbf{w}}$ ,  $\mathbf{w} = (w_0, \dots, w_l)$ .

В последующих трех разделах для некоторых пространств и их подгрупп автоморфизмов  $H$  мы выпишем в явном виде ортогональные многочлены  $\tilde{P}_{\tilde{H}}(w, s)$ , определенные в разделе 3.1.5.

### 3.2.3 Многочлены Кравчука и мономиальная группа

В этом разделе мы в качестве подгруппы  $H$  группы автоморфизмов  $\text{Aut}(\mathfrak{G}^n)$ ,  $\mathfrak{G} = \mathbb{F}_q$ , рассматриваем группу  $\mathfrak{M}_n(\mathbb{F}_q)$ .

Как нетрудно увидеть, функция

$$f(\mathbf{x}) = wt(\mathbf{x}) — \text{вес Хемминга вектора } \mathbf{x}, \quad \mathbf{x} \in \mathbb{F}_q^n. \quad (3.2.12)$$

является центральной относительно мономиальной группы  $\mathfrak{M}_n(\mathbb{F}_q)$ . Поэтому она может быть представлена в виде (3.1.20). Вычислим для этого случая в равенстве (3.1.20) в явном виде функции  $\tilde{P}_{\tilde{H}}(w, s)$ , а затем и коэффициенты  $b_w$ .

Лемма 3.2.1 и равенства (3.1.13) и (3.1.14) позволяют для группы  $\mathfrak{M}_n(\mathbb{F}_p)$  выписать в явном виде функцию  $\tilde{P}_{\tilde{H}}(w, x)$ : (Упражнение)

$$\tilde{P}_{\tilde{H}}(w, s) = \sum_{j=0}^w \binom{s}{j} \binom{n-s}{w-j} (-1)^s (q-1)^{w-j}. \quad (3.2.13)$$

Для этого необходимо, исходя из определения  $\tilde{P}_{\tilde{H}}(w, s) = \sum_{\varpi \in \tilde{A}_w} \varpi(\mathbf{x})$ , где  $\mathbf{x} \in A_s$ , (см. (3.1.13)), провести простые выкладки, используя легко доказываемое, соотношение (Упражнение)

$$\sum_{\mathbf{a} \in \mathbb{F}_p^l, \mathbf{a} \neq 0} \exp\left(\frac{2\pi i \langle \mathbf{a}, \mathbf{b} \rangle}{p}\right) = \begin{cases} -1, & \text{если } \mathbf{b} \neq 0 \\ q-1, & \text{если } \mathbf{b} = 0 \end{cases}. \quad (3.2.14)$$

Как легко проверить, что (Упражнение)

$$\tilde{P}_{\tilde{H}}(w, x) = \text{coeff}_{x^s y^{n-s}} (y-x)^w (x+(q-1)y)^{n-w}. \quad (3.2.15)$$

Совершенно также можно представить в явном виде функцию  $P_H(s, w) = \sum_{\mathbf{y} \in A_s} \varpi(\mathbf{y})$ , где  $\varpi \in \tilde{A}_w$ . Она имеет вид

$$P_H(w, s) = \sum_{j=0}^s \binom{w}{j} \binom{n-w}{s-j} (-1)^j (q-1)^{s-j} = \tilde{P}_{\tilde{H}}(s, w). \quad (3.2.16)$$

В рассматриваемом случае функция  $\tilde{P}_{\tilde{H}}(w, x)$ , очевидно, является многочленом степени  $w$  от целочисленной переменной  $x$ . Эти многочлены  $\tilde{P}_{\tilde{H}}(w, x)$  называются многочленами Кравчука. Равенство (3.2.13) обычно рассматривается как их определение. Многочлены Кравчука  $\tilde{P}_{\tilde{H}}(w, x)$  обычно обозначаются через  $K_w^{(q,n)}(x)$ .

Из теоремы 3.1.1 и леммы 3.2.1 следует соотношение ортогональности

$$\sum_{x=0}^n \binom{n}{x} (q-1)^x K_w^{(q,n)}(x) K_{w'}^{(q,n)}(x) = \begin{cases} 0, & \text{если } w \neq w' \\ \binom{n}{w} (q-1)^w, & \text{если } w = w' \end{cases}. \quad (3.2.17)$$

Существует интересное и полезное соотношение между значениями многочленов  $K_w^{(q,n)}(s)$  и  $K_s^{(q,n)}(w)$ , которое является следствием леммы 3.1.3 и соотношения (3.1.14):

**Следствие 3.2.1** *Имеет место соотношение*

$$\Phi_H(\mathbf{x}, \varpi) = (q-1)^s \binom{n}{s} K_w^{(q,n)}(s) = \tilde{S}_{\tilde{H}}(w) K_s^{(q,n)}(w) = (q-1)^w \binom{n}{w} K_s^{(q,n)}(w), \quad (3.2.18)$$

Ортогональные многочлены Кравчука были открыты в 30-х годах прошлого столетия украинским математиком и общественным деятелем М.Ф. Кравчуком. Они являются частным случаем очень обширного класса ортогональных многочленов дискретного переменного. Все ортогональные многочлены обладают многими замечательными свойствами. Их изучению посвящена обширная литература (см., например, [28]). Отметим также, что знаменитые русские ученые П.Л. Чебышев и А.А. Марков внесли заметный вклад в исследование свойств ортогональных многочленов, связанных с их приложениями к механике.



В качестве нескольких примеров известных свойств ортогональных многочленов приведем следующие: перемежаемость корней соседних ортогональных многочленов; рекуррентные соотношения, связывающие многочлены  $K_{w-1}^{(p,n)}(x)$ ,  $K_w^{(p,n)}(x)$ ,  $K_{w+1}^{(p,n)}(x)$ , и многие другие. Известны асимптотические выражения для наименьших корней многочлена  $K_w^{(p,n)}(x)$ , когда  $n \rightarrow \infty$ . Эти асимптотические формулы при  $p = 2$  будут использованы (без доказательства) в разделе 5.1.2 при выводе "оценки линейного программирования".

Следует сказать, что соотношение ортогональности (3.2.17) достаточно просто доказать, используя явный вид (3.2.13) многочлена  $K_w^{(q,n)}(x)$ . Мы выбрали другой более сложный способ ее доказательства в виду того, что он применим и для многих других подгрупп  $H$  группы автоморфизмов группы  $\text{Aut}(\mathbb{F}_q^n)$ .

Следует также заметить, что существуют подгруппы  $H < \text{Aut}(\mathbb{F}_q)$ , которые, в отличие от группы  $\mathfrak{M}_1(\mathbb{F}_p)$ , разбивают аддитивную группу  $(\mathbb{F}_q, +)$  поля  $\mathbb{F}_q$  более, чем на два класса сопряженных элементов. Одной из таких подгрупп является подгруппа  $\Phi$  порядка  $\frac{q-1}{2}$ , образованная ненулевыми элементами поля  $\mathbb{F}_q$ , которые являются квадратичными вычетами. Эта подгруппа, очевидно, разбивает поле  $\mathbb{F}_q$  на три класса сопряженных элементов.

Заметим, что в следующем разделе в качестве  $H$  рассматривается тривиальная подгруппа  $E$ ,  $|E| = 1$ , группы  $\mathbb{F}_q^*$ , которая разбивает поле  $\mathbb{F}_q$  на  $q$  классов сопряженных элементов. Можно сказать, что группа  $\Phi$  занимает промежуточное положение между группами  $E$  и  $\mathbb{F}_q^*$ .

Выпишем два первых многочлена  $K_w^{(p,n)}(x)$ :

$$K_1^{(q,n)}(x) = (q-1)n - qx,$$

$$K_2^{(q,n)}(x) = \frac{1}{2}((q-1)^2(n^2 - n) - (2nq(q-1) - q(q-2))x + q^2x^2).$$

Имеется глубокая аналогия между функциями  $P_H(w, s)$ ,  $c, w \in \{0, \dots, m\}$  и специальными функциями классического анализа.

### 3.2.4 Симметрическая группа в качестве группы $H$ и полная весовая функция кода

Мы рассматриваем группу  $\mathfrak{S}_l^n = \mathbb{F}_q^n$  и симметрическую группу  $S_n$  в качестве подгруппы  $H$  группы  $\text{Aut}(\mathfrak{S}_l^n)$ .

Найдем классы сопряженных элементов  $A_w \subset \mathbb{F}_q^n$  относительно действия группы автоморфизмов  $H$ .

Сначала рассмотрим случай  $n = 1$ . В этом случае группа автоморфизмов  $H$  группы  $\mathbb{F}_q$  состоит из одного тождественного автоморфизма. Поэтому каждый класс сопряженных элементов относительно группы  $H$  состоит из одного элемента  $\mathbf{b} \in \mathbb{F}_q$ . Этот класс мы обозначим через  $A_{\mathbf{b}}$ .

Обозначим через  $c_{\mathbf{b}}(\mathbf{x})$ ,  $\mathbf{x} \in \mathfrak{S}_l^n$ ,  $\mathbf{b} \in \mathfrak{S}_l$ , функцию, равную числу координат вектора  $\mathbf{x} \in \mathbb{F}_q^n$ , которые принадлежат классу сопряженных элементов  $A_{\mathbf{b}}$  или, проще говоря, равных  $\mathbf{b}$ . Вектор  $c(\mathbf{x}) = (c_{\mathbf{b}_0}(\mathbf{x}), \dots, c_{\mathbf{b}_{q-1}}(\mathbf{x}))$ , где  $\mathbb{F}_q = \{\mathbf{b}_0, \dots, \mathbf{b}_{q-1}\}$ , называется позицией вектора  $\mathbf{x}$  или полной весовой функцией вектора  $\mathbf{x}$ .

**Лемма 3.2.4** Пусть  $\mathbf{c} = (c_{\mathbf{b}_0}, \dots, c_{\mathbf{b}_{q-1}})$ ,  $c_{\mathbf{b}_0} + \dots + c_{\mathbf{b}_{q-1}} = n$ , — вектор с целочисленными компонентами и  $\mathbf{a} \in \mathbb{F}_q$  — вектор, для которого  $c(\mathbf{a}) = \mathbf{c}$ .

Множество  $A_{\mathbf{c}}$ , состоящее из всех векторов  $\mathbf{x} \in \mathbb{F}_q^n$  таких, что  $c(\mathbf{x}) = \mathbf{c}$ , является классом сопряженных элементов группы  $\mathbb{F}_q^n$  относительно действия симметрической группы  $S_n$  (орбитой действия группы  $S_n$  на вектор  $\mathbf{a}$ , у которого  $c(\mathbf{a}) = \mathbf{c}$ ). Вектор  $\mathbf{a}$  является одним из представителей орбиты  $A_{\mathbf{c}}$ .

Множество  $\tilde{A}_{\mathbf{c}}$ , состоящее из всех характеров  $\varpi_{\mathbf{b}}(\mathbf{x})$  (определение (3.2.4)), у которых  $c(\mathbf{b}) = \mathbf{c}$ , является классом сопряженных элементов (орбитой) относительно симметрической группы  $S_n$ . Характер  $\varpi = \varpi_{\mathbf{a}}(\mathbf{x})$  является одним из представителей орбиты  $\tilde{A}_{\mathbf{c}}$ .

Лемма очевидна.  $\square$

Легко вычислить, что  $|A_{\mathbf{c}}| = |\tilde{A}_{\mathbf{c}}| = \binom{n}{c_0, \dots, c_{q-1}} = \frac{n!}{c_0! \dots c_{q-1}!}$ , где положено  $c_j = c_{\mathbf{b}_j}$ .

Далее для упрощения изложения мы будем рассматривать только случай  $q = p$  ( $l = 1$ ). В этом случае мы индексирем классы  $A_{\mathbf{c}}$  и  $\tilde{A}_{\mathbf{w}}$  сопряженных элементов группы  $\mathfrak{S}_1^n$  и группы характеров  $\tilde{\mathfrak{S}}_1^n$  с помощью векторов  $\mathbf{c} = (c_0, \dots, c_{p-1})$ ,  $c_0 + \dots + c_{p-1} = n$ , и  $\mathbf{w} = (w_0, \dots, w_{p-1})$ ,  $w_0 + \dots + w_{p-1} = n$ , с целыми координатами.

Используя равенство (3.1.14), нетрудно показать, что если  $\mathbf{x} \in A_{\mathbf{c}}$ , то

$$\begin{aligned} \tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{c}) &= \sum_{\varpi \in \tilde{A}_{\mathbf{w}}} \varpi(\mathbf{x}) = \\ &= \sum \binom{c_0}{w_{0,0}, \dots, w_{0,p-1}} \dots \binom{c_{p-1}}{w_{p-1,0}, \dots, w_{p-1,p-1}} \exp \left( \frac{2\pi i (\sum_{k=0}^{p-1} \sum_{s=0}^{p-1} c_k w_{k,s})}{p} \right), \end{aligned} \quad (3.2.19)$$

где суммирование в сумме  $\sum$  производится по всем векторам  $(w_{k,0}, \dots, w_{k,p-1})$ ,  $k = 0, \dots, p-1$ , таким, что  $\sum_{k=0}^{p-1} w_{k,s} = c_s$ ,  $s = 0, \dots, p-1$ ,  $\sum_{s=0}^{p-1} w_{k,s} = w_k$ ,  $k = 0, \dots, p-1$ . Это утверждение хотя и является громоздким, но доказательство его является не особенно сложным.

Многочлены  $\tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{x})$  от  $n$  переменных являются ортогональными многочленами с весами  $\binom{n}{c_0, \dots, c_{p-1}}$  (теорема 3.1.1), т.е. для них справедливо

$$\sum_{c_0 + \dots + c_{p-1} = n} \binom{n}{c_0, \dots, c_{p-1}} \tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{c}) \tilde{P}_{\tilde{H}}(\mathbf{w}', \mathbf{c}) = \begin{cases} 0, & \text{если } \mathbf{w} \neq \mathbf{w}' \\ \binom{n}{w_0, \dots, w_{p-1}}, & \text{если } \mathbf{w} = \mathbf{w}' \end{cases} \quad (3.2.20)$$

Соотношение (3.2.20) будет использовано при выводе, так называемого, соотношения МакВильямс для полной весовой функции линейного кода.

### 3.2.5 Ортогональные многочлены для примарного кольца вычетов

Мы рассматриваем группу  $\mathfrak{P}_l^n = (Z_p^n, +)$  и группу  $\mathfrak{M}(\mathfrak{P}_l^n)$  в качестве подгруппы  $H$  группы автоморфизмов  $\text{Aut}(\mathfrak{P}_l^n)$ . Группа  $\mathfrak{M}(\mathfrak{P}_l^n)$  определена в разделе 3.2.2. Сначала рассмотрим случай  $n = 1$ . Определим структурные постоянные  $r_{t,k}$  группы  $\mathfrak{M}(\mathfrak{P}_l^n)$  с помощью равенства

$$r_{w,s} = \sum_{x \in A_w} \exp \left( \frac{2\pi i a x}{p^l} \right), \quad \text{где } a \in A_s. \quad (3.2.21)$$

Очевидно, значение правой части последнего равенства не зависит от выбора конкретного представителя  $a$  в классе  $A_t$ .

В качестве примера рассмотрим случай  $l = 2$ . В этом примере матрица структурных констант  $R_H = \|r_{w,s}\|$  имеет вид (Упражнение)

$$R_H = \begin{vmatrix} 1 & 1 & 1 \\ p-1 & p-1 & -1 \\ p(p-1) & -p & 0 \end{vmatrix}, \quad (3.2.22)$$

Легко проверить, что  $\sum_{s=0}^2 |A_s| r_{w,s} r_{w',s} = 0$ , если  $w \neq w'$ , где  $|A_0| = 1$ ,  $|A_1| = p-1$ ,  $|A_2| = p(p-1)$ .

Из равенства (3.1.16) и (3.1.17) следует, что при  $n = 1$  в общем случае  $l \geq 1$

$$\tilde{P}_{\tilde{H}}(w, s) = r_{w,s}. \quad (3.2.23)$$

Используя равенство (3.1.14), нетрудно показать, что если  $\mathbf{x} \in A_{\mathbf{c}}$ ,  $\mathbf{c} = (c_0, \dots, c_l)$ ,  $c_0 + \dots + c_l = n$ , то

$$\begin{aligned} \tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{c}) &= \sum_{\mathbf{w} \in \tilde{A}_{\mathbf{w}}} \varpi(\mathbf{x}) = \\ &= \sum \binom{c_0}{w_{0,0}, \dots, w_{0,l}} \dots \binom{c_l}{w_{l,0}, \dots, w_{l,l}} \prod_{0 \leq j, s \leq l} r_{j,s}^{w_{j,s}}, \end{aligned} \quad (3.2.24)$$

где суммирование в сумме  $\sum$  производится по всем векторам  $(w_{k,0}, \dots, w_{k,l})$ ,  $k = 0, \dots, l$ , таким, что  $\sum_{s=0}^{p-1} w_{k,s} = c_k$ ,  $s = 0, \dots, l$ ,  $\sum_{k=0}^{l-1} w_{k,s} = w_s$ ,  $k = 0, \dots, l$ . Это утверждение хотя и является громоздким, но доказательство его является не особенно сложным.

Многочлены  $\tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{x})$  от  $l$  переменных являются ортогональными многочленами с весами  $|A_0|^{c_0} \dots |A_l|^{c_l}$ , т.е. для них справедливо

$$\begin{aligned} &\sum_{c_0 + \dots + c_{p-1} = n} \binom{n}{c_0, \dots, c_l} |A_0|^{c_0} \dots |A_l|^{c_l} \tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{c}) \tilde{P}_{\tilde{H}}(\mathbf{w}', \mathbf{c}) = \\ &= \begin{cases} 0, & \text{если } \mathbf{w} \neq \mathbf{w}' \\ \binom{n}{w_0, \dots, w_l} |A_0|^{w_0} \dots |A_l|^{w_l}, & \text{если } \mathbf{w} = \mathbf{w}' = (w_0, \dots, w_l) \end{cases}. \end{aligned} \quad (3.2.25)$$

Отметим, что целочисленные переменные  $\mathbf{x} = (x_0, \dots, x_l)$  — аргументы многочлена  $\tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{x})$ , связаны соотношением  $x_0 + \dots + x_l = n$ , т.е.  $\tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{x})$  фактически является многочленом от  $l$  целочисленных переменных.  $x_1, \dots, x_l$ ,  $x_1 + \dots + x_l \leq n$ . Общая степень не  $\tilde{P}_{\tilde{H}}(\mathbf{w}, \mathbf{x})$  превосходит  $w_1 + \dots + w_l$ . (Упражнение)

### 3.2.6 Многочлены Кравчука, как зональные сферические функции

В том или ином виде идеи, излагаемые в этом разделе, общеизвестны. В частности, в тексте этого раздела использовались материалы из главы I, § 2 книги [28].

Многочлены Кравчука являются частным случаем, так называемых, зональных сферических функций, определенных на метрическом пространстве  $\mathcal{M}$ , на котором действует некоторая группа преобразований  $\mathfrak{G}$ . В качестве  $\mathcal{M}$  часто рассматривают сферу в евклидовом пространстве  $\mathcal{R}^n$  или дискретное пространство Хемминга  $\mathbb{F}_q^n$ .

Зональная функция — это функция  $\varphi(\mathbf{x})$ ,  $\mathbf{x} \in \mathcal{M}$ , которая инвариантна на смежных классах, порожденной подгруппой  $H \leq \mathfrak{G}$ , т.е.  $\varphi(\mathbf{x}) = \varphi(\mathbf{x}\mathbf{h})$  для всех  $\mathbf{h} \in H$ . В случае  $\mathcal{M} = \mathbb{F}_q^n$  и  $H$  — мономиальная группа смежный класс — это множество точек  $\mathbf{x}$  пространства  $\mathbb{F}_q^n$ , вес которых равен  $s$ . Поясним всё это подробнее на примере  $\mathcal{M} = \mathbb{F}_q^n$ .

Пусть  $Y_n$  —  $q^n$ -мерное пространство функций, отображающих  $\mathbb{F}_q^n$  в  $\mathbb{C}$ . Как уже было отмечено выше, функции (характеры)  $\varpi_{\mathbf{a}}(\mathbf{x})$ ,  $\mathbf{a} \in \mathbb{F}_q^n$  (см. (3.2.4)) является базисом пространства  $Y_n$ .

Пусть  $\varphi \in \text{Aut}(\mathbb{F}_q^n)$ . Отображение  $T_\varphi : f \rightarrow T_\varphi(f)$ , определяемое его действиями

$$T_\varphi : \varpi_{\mathbf{a}}(\mathbf{x}) \rightarrow \varpi_{\varphi(\mathbf{a})}(\mathbf{x}). \quad (3.2.26)$$

на базисных элементах пространства  $Y_n$ , очевидно, является линейным отображением пространства  $Y_n$  в себя. Кроме того,  $T_\varphi T_{\varphi'} = T_{\varphi(\varphi')}$ , т.е. множество линейных отображений  $T_\varphi$ ,  $\varphi \in \text{Aut}(\mathbb{F}_q^n)$ , является группой, обозначаемой далее через  $\mathfrak{Z}(\mathbb{F}_q^n)$ . Очевидно, группу  $\mathfrak{Z}(\mathbb{F}_q^n)$ , элементами которой являются унитарные  $q^n \times q^n$ -матрицы над  $\mathbb{C}$ , можно рассматривать как унитарное представление группы  $\text{Aut}(\mathbb{F}_q^n)$  на векторном пространстве  $\mathbb{C}^{q^n}$ .

Рассмотрим подгруппу  $\mathfrak{Z}(H)$  группы  $\mathfrak{Z}(\mathbb{F}_q^n)$ , образованную всеми элементами  $T_\varphi$ , у которых  $\varphi \in H$ . Очевидно, элемент  $\Phi_H(\mathbf{x}, \mathbf{a}) = \sum_{\varphi \in H} \varpi_{\varphi(\mathbf{a})}(\mathbf{x}) \in Y_n$ ,  $\varpi = \varpi_{\mathbf{a}}(\mathbf{x})$ , является инвариантным относительно группы  $\mathfrak{Z}(H)$ , т.е.

$$\Phi_H(\mathbf{x}, \mathbf{a})T_\varphi = \Phi_H(\mathbf{x}, \mathbf{a}). \quad (3.2.27)$$

В математическом анализе при любом фиксированном векторе  $f(\mathbf{x}) \in Y_n$  функцию

$$\Phi_{\varpi}(\varphi) = (f(\mathbf{x})T_\varphi, \Phi_H(\mathbf{x}, \varpi)), \quad (3.2.28)$$

$(\cdot, \cdot)$  — скалярное произведение, называют зональной сферической функцией, соответствующей инвариантному (относительно подгруппы  $H$ ) вектору  $\Phi_H(\mathbf{x}, \varpi)$ .

Как следует из (3.2.27), зональная сферическая функция  $\Phi_{\varpi}(\varphi)$  инвариантна относительно подгруппы  $H$ , т.е. если  $\varphi' \in H$ , то  $\Phi(\varphi) = \Phi(\varphi'\varphi)$ .

Можно считать, что функция  $\Phi_{\varpi}(\varphi)$  определена на смежных классах группы  $\text{Aut}(\mathbb{F}_q^n)$  по ее подгруппе  $H$ , т.е. на различных классах  $\varphi H$ , где  $\varphi \in \text{Aut}(\mathbb{F}_q^n)$ .

Предположим, что  $\varphi$  переводит ненулевой вектор  $\mathbf{a} \in \mathbb{F}_q^n$  в вектор  $\mathbf{b} = \varphi(\mathbf{a})$ . В этом случае для мономиальной группы  $H$  класс  $\varphi H$  полностью определяется весом вектора  $\mathbf{b}$ . Поэтому функция  $\Phi_{\varpi}(\varphi)$  полностью определяется весом вектора  $\mathbf{b}$ , в который переходит фиксированный вектор  $\mathbf{a}$  под действием отображения  $\varphi$ , т.е. значение  $\Phi_{\varpi}(\varphi)$  совпадает со значением функции  $P_{\varpi}(t)$ , где  $t = wt(\varphi(\mathbf{a}))$ .

Несложный подсчет показывает, что функция  $P_{\varpi}(t)$ , в том случае, когда  $H$  — мономиальная группа, пропорциональна полиному Кравчука  $K_w^{(p,n)}(x)$ ,  $w = wt(\mathbf{h})$ , где элемент  $\mathbf{h} \in \mathbb{F}_p^n$  определяет характер  $\varpi = \varpi_{\mathbf{a}}(\mathbf{x})$ . Если  $H$  — другая группа, то мы получим и другие ортогональные многочлены. Некоторые из них выписаны в разделах 3.2.4 и 3.2.5.

Ценность этих достаточно абстрактных и пространных рассуждений этого раздела о трактовке многочленов Кравчука как зональных сферических функций, состоит в том, что они применимы к очень широкому классу пространств  $\mathcal{M}$  и групп  $\mathfrak{G}$  отображений, действующих на них. Почти все известные ортогональные многочлены возникают указанным способом для подходящих множеств  $\mathcal{M}$  и их групп отображений.

Например, многочлены Гегенбауера возникают в том случае, когда в качестве множества  $\mathfrak{M}$  взята единичная сфера  $S^{n-1}$ , в качестве группы  $\mathfrak{G}$  — группа  $SO(n)$  вращений  $n$ -мерного евклидова пространства и, наконец, в качестве  $H$  — подгруппа  $SO(n)$ , которая оставляет неподвижной выделенную точку  $\mathbf{a}$  сферы  $S^{n-1}$ .

В следующем разделе в качестве  $\mathfrak{M}$  мы будем рассматривать пространство  $\mathbb{F}_q^n$ .



# Глава 4

## Оценка линейного программирования

### 4.1 Положительно определенные функции

**Определение 4.1.1** Пусть  $\mathfrak{K}$  — подмножество элементов абелевой группы  $\mathfrak{G}^n$  с групповой операцией  $+$ . Функция  $g : (\mathbf{x}, \mathbf{y}) \rightarrow \mathbf{R}$ ,  $\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n$ , называется положительно определенной, если для любого подмножества  $\mathfrak{K} \subseteq \mathfrak{G}^n$  справедливо неравенство

$$T(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} g(\mathbf{x}, \mathbf{y}) \geq \frac{1}{|\mathfrak{G}^n|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n} g(\mathbf{x}, \mathbf{y}). \quad (4.1.1)$$

Заметим, что если  $g(\mathbf{x}, \mathbf{y})$  и  $g'(\mathbf{x}, \mathbf{y})$  — положительно определенные функции и  $a, b \geq 0$ , то  $ag(\mathbf{x}, \mathbf{y}) + bg'(\mathbf{x}, \mathbf{y})$  — также положительно определенная функция.

**Лемма 4.1.1** Функция

$$g(\mathbf{x}, \mathbf{y}) = \Re \left( \sum_{\varpi \in \tilde{\mathfrak{G}}^n} a_{\varpi} \varpi(\mathbf{x} - \mathbf{y}) \right), \quad a_{\varpi} \in \mathbf{R}, \quad (4.1.2)$$

где  $\tilde{\mathfrak{G}}^n$  — множество характеров группы  $\mathfrak{G}^n$  и  $\Re(z)$  — действительная часть комплексного числа  $z$ , является положительно определенной, если все коэффициенты  $a_{\varpi}$ , у которых характер  $\varpi$  не равен тождественно 1, являются неотрицательными.

**Доказательство.** Отметим, что в рассматриваемом случае при любом  $\mathfrak{K} \subseteq \mathbb{F}_q^n$  и  $a_{\varpi} \in \mathbf{R}$  величина  $T'(\mathfrak{K}) = \sum_{\varpi \in \tilde{\mathfrak{G}}_q^n} a_{\varpi} \varpi(\mathbf{x} - \mathbf{y})$  является действительным числом. Это следует того, что

$$\overline{T'(\mathfrak{K})} = \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n} \sum_{\varpi \in \mathfrak{G}^n} a_{\varpi} \overline{\varpi(\mathbf{x} - \mathbf{y})} = \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n} \sum_{\varpi \in \mathfrak{G}^n} a_{\varpi} \varpi(\mathbf{y} - \mathbf{x}) = T'(\mathfrak{K}). \quad (4.1.3)$$

Следовательно, мы можем отбросить символ  $\Re$  в правой части равенства (4.1.2).

С одной стороны,

$$T_{\varpi}(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \varpi(\mathbf{x} - \mathbf{y}) = \frac{1}{|\mathfrak{K}|^2} \left| \sum_{\mathbf{x} \in \mathfrak{K}} \varpi(\mathbf{x}) \right|^2 \geq 0, \quad (4.1.4)$$

если  $\varpi$  не равно тождественно 1, и  $T_{\varpi_0}(\mathfrak{K}) = 1$ , если  $\varpi_0(x)$  — характер тождественно равный 1 при всех  $x \in \mathbb{F}_q^n$ .

С другой стороны, очевидно,  $T_{\varpi}(\mathfrak{G}^n) = 0$ , если  $\varpi$  — характер не тождественно равный 1, и  $T_{\varpi_0}(\mathfrak{G}^n) = 1$ . Отсюда следует неравенство (4.1.1), если все коэффициенты  $a_{\varpi}$ ,  $\varpi \in \widetilde{\mathfrak{G}^n} \setminus \{\varpi_0\}$ , являются неотрицательными числами.  $\square$

Следует отметить, что если  $\mathfrak{G} = \mathbb{F}_q$  и  $\mathbb{F}_q$  — поле характеристики 2, то необходимые условия леммы 4.1.1 являются и достаточными. Если же это не так, т.е. характеристика поля  $\mathbb{F}_q$  нечетна, то необходимые условия сильнее достаточных условий, при которых лемма 4.1.1 справедлива.

Например, если  $q = p$ ,  $p \geq 3$ ,  $\mathfrak{G}^n = \mathbb{F}_p^n$  и

$$\begin{aligned} g(\mathbf{x}, \mathbf{y}) &= \exp\left(\frac{2\pi i \langle \mathbf{a}, \mathbf{x} - \mathbf{y} \rangle}{p}\right) - a \exp\left(\frac{-2\pi i \langle \mathbf{a}, \mathbf{x} - \mathbf{y} \rangle}{p}\right) = \\ &= (1 - a) \cos\left(\frac{2\pi \langle \mathbf{a}, \mathbf{x} - \mathbf{y} \rangle}{p}\right), \quad 1 > a > 0, \quad \mathbf{a} \in \mathbb{F}_p^n, \end{aligned} \quad (4.1.5)$$

то, как нетрудно проверить, функция  $g(\mathbf{x}, \mathbf{y})$  является положительно определенной, но для нее не выполнено условие леммы 4.1.1. (Упражнение)

Без сомнения, лемма 4.1.1 может быть обобщена на многие другие пространства. Этим мы заниматься не будем.

В том случае, когда положительно определенная функция  $g(\mathbf{x}, \mathbf{y})$  может быть представлена в виде (4.1.2), непосредственно из неравенства (4.1.1) вытекает

**Следствие 4.1.1** *Если  $g(\mathbf{x}, \mathbf{y})$  — положительно определенная функция, которая может быть представлена в виде (4.1.2), то для любого кода  $\mathfrak{K} \subseteq \mathfrak{G}^n$  выполнено*

$$\frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} g(\mathbf{x}, \mathbf{y}) \geq a_{\varpi_0}, \quad (4.1.6)$$

где  $\varpi_0$  — главный характер группы  $\mathfrak{G}^n$ , т.е.  $\varpi_0$  — характер, принимающий значение 1 на всех элементах группы  $\mathfrak{G}^n$ .

**Доказательство** вытекает из определения 4.1.1 и очевидного равенства

$$\frac{1}{|\mathfrak{G}^n|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n} \varpi(\mathbf{x} - \mathbf{y}) = \begin{cases} 0, & \text{если } \varpi \neq \varpi_0 \\ a_{\varpi_0}, & \text{если } \varpi = \varpi_0 \end{cases}. \quad (4.1.7)$$

$\square$

**Следствие 4.1.2 (из лемм 4.1.1 и 4.1.1)** . Пусть характер  $\varpi$  не равен тождественно 1 и  $\mathfrak{K} \subseteq \mathfrak{G}^n$  — произвольный код. Функция  $g(\mathbf{x}, \mathbf{y}) = \frac{\Phi_{\varpi}(\mathbf{x} - \mathbf{y})}{|St(\varpi)|} = \tilde{P}_{\tilde{H}}(w, s)$ , если  $\varpi \in \tilde{A}_w$  и  $\mathbf{x} - \mathbf{y} \in A_s$  (см. (3.1.13) и (3.1.14)), является положительно определенной и для неё выполнено

$$\begin{aligned} \Psi_{\varpi}(\mathfrak{K}) &= \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \frac{\Phi_{\varpi}(\mathbf{x} - \mathbf{y})}{|St(\varpi)|} = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \tilde{P}_{\tilde{H}}(w, s_H(\mathbf{x} - \mathbf{y})) = \frac{1}{|\mathfrak{K}|^2} \sum_{s=0}^m D_s \tilde{P}_{\tilde{H}}(w, s) \geq \\ &= \frac{1}{|\mathfrak{G}^n|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n} \frac{\Phi_{\varpi}(\mathbf{x} - \mathbf{y})}{|St(\varpi)|} = \frac{1}{|\mathfrak{G}^n|^2} \sum_{s=0}^m |A_s| \tilde{P}_{\tilde{H}}(w, s) = 0, \end{aligned} \quad (4.1.8)$$



где  $D_s$  — число пар  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  таких, что  $s_H(\mathbf{x} - \mathbf{y}) = s$  или, что одно и то же,  $D_s$  — число пар  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  таких, что  $\mathbf{x} - \mathbf{y} \in A_s$ .

Если же характер  $\varpi$  равен тождественно 1, то

$$\Psi_{\varpi}(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \frac{\Phi_{\varpi}(\mathbf{x} - \mathbf{y})}{|St(\varpi)|} = \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} \tilde{P}_{\tilde{H}}(w, s_H(\mathbf{x} - \mathbf{y})) = \frac{1}{|\mathfrak{K}|^2} \sum_{s=0}^m D_s \tilde{P}_{\tilde{H}}(w, s) = 1 \quad (4.1.9)$$

В частности, если  $\mathfrak{G}^n = \mathbb{F}_q^n$  и  $H$  — мономиальная группа  $\mathfrak{M}_n(\mathbb{F}_q^n)$ , то  $D_s$  — число пар  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  таких, что  $d(\mathbf{x}, \mathbf{y}) = s$ , и

$$\frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} K_w^{(q,n)}(d(\mathbf{x}, \mathbf{y})) \geq 0, \text{ если } w \neq 0 \text{ и } \frac{1}{|\mathfrak{K}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} K_0^{(q,n)}(d(\mathbf{x}, \mathbf{y})) = 1, \quad (4.1.10)$$

для любого кода  $\mathfrak{K} \subset \mathbb{F}_p^n$ , где  $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$  расстояние Хемминга между векторами  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ .

## 4.2 Оценка линейного программирования

### 4.2.1 Оценка Дельсарта

Пусть  $V$  — некоторое подмножество всех классов  $\{A_0, \dots, A_m\}$  сопряженных элементов группы  $\mathfrak{G}^n$  относительно подгруппы  $H$  ее группы автоморфизмов.

Код  $\mathfrak{K} \subseteq \mathfrak{G}^n$  называем  $V$ -кодом, если для любых  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  разность  $\mathbf{x} - \mathbf{y}$  не принадлежит ни одному классу сопряженных элементов  $A_s$ , который в свою очередь принадлежит множеству  $V$ . Другими словами, для  $V$ -кода  $\mathfrak{K}$ , если  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  и  $A_s \in V$ , то  $\mathbf{x} - \mathbf{y} \notin A_s$ . Всегда полагаем, что  $A_0 \notin V$ .

Рассмотрим функцию

$$f_{\mathfrak{K}}(s) = \sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}; \mathbf{x} - \mathbf{y} \in A_s} g(\mathbf{x}, \mathbf{y}). \quad (4.2.1)$$

Предположим, что функция  $g(\mathbf{x}, \mathbf{y})$ ,  $\mathbf{x}, \mathbf{y} \in \mathfrak{G}^n$ , обладает следующими двумя свойствами

- $f_{\mathfrak{K}}(s) \leq 0$ , если  $A_s \notin V$  и  $s \neq 0$ .
- Коэффициенты  $a_{\varpi}$ ,  $\varpi \in \tilde{\mathfrak{G}}^n$ , в представлении (4.1.2) функции  $g(\mathbf{x}, \mathbf{y})$  неотрицательны. При этом  $a_0 = a_{\varpi_0} > 0$ , где  $\varpi_0$  — гравный характер группы  $\mathfrak{G}^n$ .

**Теорема 4.2.1** Пусть  $\mathfrak{K}$  —  $V$ -код и функция  $g(\mathbf{x}, \mathbf{y})$  обладают свойствами а. и б. Тогда

$$|\mathfrak{K}| \leq \frac{f_{\mathfrak{K}}(0)}{a_0}. \quad (4.2.2)$$

**Доказательство.** Действительно, с одной стороны из свойства а. функции  $g(\mathbf{x}, \mathbf{y})$  вытекает, что

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} g(\mathbf{x}, \mathbf{y}) = \sum_{s=0}^n D_s f_{\mathfrak{K}}(s) = |\mathfrak{K}| f_{\mathfrak{K}}(0) + \sum_{s \in \bar{v}} D_s f_{\mathfrak{K}}(s) \leq |\mathfrak{K}| f(0), \quad (4.2.3)$$

где  $D_s$  — число пар векторов  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  таких, что  $(\mathbf{x}, \mathbf{y}) \in A_s$  и  $\bar{v}$  — множество чисел  $j, j \neq 0$ , таких, что  $j \notin V$ .

С другой стороны из следствия 4.1.1 вытекает неравенство

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} g(\mathbf{x}, \mathbf{y}) \geq |\mathfrak{K}|^2 a_{\varpi_0} = |\mathfrak{K}|^2 a_0. \quad (4.2.4)$$

Из последних двух неравенств следует утверждение теоремы.  $\square$

В том случае, когда  $\mathfrak{G}^n = \mathbb{F}_q^n$  и  $H$  — мономиальная группа  $\mathfrak{M}_n(\mathbb{F}_p)$  автоморфизмов, действующая на пространстве  $\mathbb{F}_q^n$ , т.е. в случае, когда классами сопряженных элементов являются множества векторов пространства  $\mathbb{F}_q^n$  определенного веса, предудущая теорема может быть уточнена следующим образом.

Пусть  $f(x)$  — многочлен с вещественными коэффициентами, который мы рассматриваем на множестве целых чисел  $\{0, 1, \dots, n\}$  и который обладает следующими свойствами:

- i.  $f(x) \leq 0$ , если  $x \in \{d, \dots, n\}$ .
- ii. Коэффициенты  $a_w, w = 0, 1, \dots, n$ , в представлении

$$f(x) = \sum_{w=0}^n a_w K_w^{(p,n)}(x) \quad (4.2.5)$$

через ортогональные многочлены  $K_w^{(q,n)}(x)$  являются неотрицательными и  $a_0 > 0$ .

**Теорема 4.2.2** Пусть  $\mathfrak{K}$  код с кодовым расстоянием  $d$  и  $f(x)$  — многочлен, для которого выполнены свойства i. и ii. Тогда

$$|\mathfrak{K}| \leq \frac{f(0)}{a_0}, \quad (4.2.6)$$

где  $a_0$  — свободный член в представлении (4.2.5).

**Доказательство.** Действительно, с одной стороны из свойства i. функции  $f(x)$  вытекает, что

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} f(d(\mathbf{x}, \mathbf{y})) = \sum_{s=0}^n D_s f(s) \leq |\mathfrak{K}| f(0), \quad (4.2.7)$$

где  $D_s$  — число пар векторов  $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$  таких, что  $d(\mathbf{x}, \mathbf{y}) = s$ .

С другой стороны, как следует из следствия 4.1.2, функция  $f(d(\mathbf{x}, \mathbf{y}))$  является положительно определенной функцией. Отсюда и из неравенства (4.1.10) вытекает соотношение

$$\sum_{\mathbf{x}, \mathbf{y} \in \mathfrak{K}} f(d(\mathbf{x}, \mathbf{y})) = \sum_{s=0}^n f(s) D_s = \sum_{s=0}^n \sum_{w=0}^n a_w K_w^{(p,n)}(s) D_s \geq a_0 |\mathfrak{K}|^2. \quad (4.2.8)$$

Из последних двух неравенств следует утверждение теоремы.  $\square$

Оценка (4.2.6) называется оценкой Дельсарта для  $q$ –значного кода длины  $n$ . Оценка (4.2.2) является оценкой Дельсарта для более общего случая пространств  $\mathfrak{G}^n$  и более общего случая подгруппы  $H$  группы автоморфизмов  $\text{Aut}(\mathfrak{G}^n)$ . Как представляется автору, оценка (4.2.2) является новой. Далее мы будем рассматривать в качестве  $\mathfrak{G}^n$  только пространства Хемминга  $\mathbb{F}_q^n$ .

Следует сказать, что для получения явной оценки  $|\mathfrak{K}|$  необходимо явно указать многочлен  $f(x)$ , который обладает свойствами i. и ii. Во многих случаях выбор "хорошего" многочлена  $f(x)$  является достаточно сложной задачей.

Пусть

$$\Omega_q(n, d) = \min \frac{f(0)}{a_0}, \quad (4.2.9)$$

где минимум берется по всем многочленам, для которых выполнены свойства i. и ii. (Другая форма оценки Дельсарта.) Вычисление при конкретных значениях  $n$  и  $d$  экстремального значения  $\Omega(n, d)$  отношения  $\frac{f(0)}{a_0}$  является задачей линейного программирования. Поэтому оценка

$$M_q(n, d) \leq \Omega_q(n, d), \quad (4.2.10)$$

где  $M_q(n, d)$  — максимальное число векторов  $q$ –значного кода длины  $n$  с кодовым расстоянием  $d$  (которая является следствием оценки Дельсарта (4.2.6)), называется оценкой линейного программирования.

К сожалению, явно вычислить число  $\Omega(n, d)$  удастся только в редких случаях. Поэтому мы ограничимся вычислением другой функции  $\Omega_q^{(r)}(n, d)$ , которая отличается от  $\Omega_q(n, d)$  тем, что минимум в (4.2.9) берется не по всем многочленам, а только по многочленам, степень которых не превосходит  $r$ .

## 4.2.2 Выбор многочлена в оценке (4.2.6)

Начнем со следующего утверждения.

**Лемма 4.2.1** *Все коэффициенты  $a_s$  в соотношении*

$$K_w^{(q,n)}(x)K_{w'}^{(q,n)}(x) = \sum_{s=0}^{w+w'} a_s K_s^{(q,n)}(x) \quad (4.2.11)$$

*являются неотрицательными.*

**Доказательство.** Имея в виду соотношения (3.1.17) и (3.1.18), произведение  $K_w^{(q,n)}(s)K_{w'}^{(q,n)}(s)$  можно записать в виде

$$K_w^{(q,n)}(s)K_{w'}^{(q,n)}(s) = Y_w(\mathbf{x})Y_{w'}(\mathbf{x}) = \sum_{wt(\mathbf{y})=w, wt(\mathbf{y}')=w'} \varpi_{\mathbf{y}+\mathbf{y}'}(\mathbf{x}), \quad (4.2.12)$$

где  $\mathbf{x}$  — любой элемент класса сопряженных элементов  $A_s$ .

Очевидно, каждый характер  $\varpi_{\mathbf{y}+\mathbf{y}'}(\mathbf{x})$ , у которого  $wt(\mathbf{y} + \mathbf{y}') = r$ , т.е. характер, принадлежащий смежному классу  $\tilde{A}_r$ , входит в левую часть (4.2.12) с кратностью, которая равна числу решений  $N_{w,w'}^{(r)}$  относительно переменных  $\mathbf{y}$  и  $\mathbf{y}'$  системы из трех уравнений

$$wt(\mathbf{y} + \mathbf{y}') = r, \quad wt(\mathbf{y}) = w, \quad wt(\mathbf{y}') = w'. \quad (4.2.13)$$

Таким образом соотношение (4.2.12) можно представить в виде

$$Y_w(\mathbf{x})Y_{w'}(\mathbf{x}) = \sum_{r=|w-w'|}^{w+w'} N_{w,w'}^{(r)} Y_r(\mathbf{x}). \quad (4.2.14)$$

Заметим, что число  $N_{w,w'}^{(r)}$  достаточно просто вычислить в явном виде. (Упражнение) Например, если  $q = 2$  и  $r = w + w' - 2u$ , то  $N_{w,w'}^{(r)} = \binom{n}{w} \binom{w}{u} \binom{n-w}{w'-u}$ .

Равенство (4.2.12) доказывает утверждение леммы, ибо  $N_{w,w'}^{(r)} \geq 0$ .  $\square$

Далее для упрощения изложения мы рассматриваем только двоичный случай, т.е. случай  $q = 2$ .

Приведем некоторые свойства ортогональных многочленов  $K_s^{(2,n)}$ , которые понадобятся далее (см. [?]), которые, впрочем, справедливы для всех ортогональных многочленов.

(а) многочлен  $K_s^{(2,n)}(x)$  на интервале  $(0, n)$  имеет  $s$  различных действительных корней;

(б) если  $x_1^{s-1} < \dots < x_{s-1}^{s-1}$  — корни  $K_{s-1}^{(2,n)}(x)$ , то в каждом интервале  $(0, x_1^{s-1})$ ,  $(x_1^{s-1}, x_2^{s-1})$ ,  $\dots$ ,  $(x_{s-1}^{s-1}, n)$  имеется ровно один корень многочлена  $K_s^{(2,n)}(x)$ .

Свойство (б) называется свойством перемежаемости корней соседних многочленов  $K_s^{(2,n)}(x)$  и  $K_{s-1}^{(2,n)}(x)$ . Как уже было отмечено, оно справедливо не только для многочленов Кравчука, но и для всех систем ортогональных многочленов. Заметим, что вычислить асимптотическое значение, не говоря уже о точном, минимального корня многочлена Кравчука — весьма нетривиальная задача математического анализа. Вместе с тем это асимптотическое значение нам понадобится при выводе оценки линейного программирования.

Из свойства (б) также следует, что наименьший корень  $x_1^s$  многочлена  $K_s^{(2,n)}(x)$  всегда меньше всех корней многочлена  $K_r^{(2,n)}(x)$ , если  $r < s$ . Следовательно, значение  $K_r^{(2,n)}(x_1^s)$  всегда положительно, если  $r < s$ , в виду того, что знак числа  $K_r^{(2,n)}(x_1^s)$  в этом случае, очевидно, совпадает со знаком числа  $K_r^{(2,n)}(0) = \binom{n}{r}$ .

Из свойства (б) следует, что интервал  $(x_1^s, x_1^{s-1})$  не пуст. Будем обозначать через  $c_s$  число, принадлежащее этому интервалу, которое обладает следующим свойством

$$-K_s^{(2,n)}(c_s) = K_{s-1}^{(2,n)}(c_s). \quad (4.2.15)$$

Такое число  $c_s$  всегда существует, ибо при движении переменной  $x$  от точки  $x_1^s$  до точки  $x_1^{s-1}$  непрерывная функция  $K_{s-1}^{(2,n)}(x) + K_s^{(2,n)}(x)$  принимает в точке  $x_1^s$  положительное значение  $K_{s-1}^{(2,n)}(x_1^s)$ , а в точке  $x_1^{s-1}$  — отрицательное значение  $K_s^{(2,n)}(x_1^{s-1})$ . Отсюда следует, что эта функция на интервале  $(x_1^s, x_1^{s-1})$  имеет точку  $c_s$ , для которой выполнено равенство (4.2.15).

**Лемма 4.2.2** Пусть  $x_s$  наименьший корень многочлена Кравчука  $K_s^{(2,n)}(x)$ .

Тогда в представлении

$$F(x) = \frac{K_s^{(2,n)}(x)K_{s-1}^{(2,n)}(c_s) - K_{s-1}^{(2,n)}(x)K_s^{(2,n)}(c_s)}{x_s - x} = \sum_{r=0}^{s-1} b_r K_r^{(2,n)}(x) \quad (4.2.16)$$

многочлена  $F(x)$  все коэффициенты  $b_r$  неотрицательны.

**Доказательство.** Широко известная формула Кристофеля-Дарбу [?] для многочленов Кравчука имеет вид

$$\frac{K_s^{(2,n)}(x)K_{s-1}^{(2,n)}(y) - K_{s-1}^{(2,n)}(y)K_s^{(2,n)}(x)}{y - x} = \frac{2}{s} \binom{n}{s-1} \sum_{r=0}^{s-1} \frac{K_r^{(2,n)}(x)K_r^{(2,n)}(y)}{\binom{n}{r}}. \quad (4.2.17)$$

Эту формулу достаточно просто доказать с помощью, так называемого, рекуррентного соотношения, связывающего многочлены  $K_{s+1}^{(2,n)}(x)$ ,  $K_s^{(2,n)}(x)$ ,  $K_{s-1}^{(2,n)}(x)$ . Это, между прочим, сделано в разделе 6.2.6 для других ортогональных многочленов. Заинтересованный читатель может использовать эти наводящие соображения для доказательства равенства (4.2.17).

Положим теперь в равенстве (4.2.17)  $y = c_s$ . В результате получим

$$F(x) = \frac{2}{s} \binom{n}{s-1} \sum_{r=0}^{s-1} \frac{K_r^{(2,n)}(x)K_r^{(2,n)}(c_s)}{\binom{n}{r}}. \quad (4.2.18)$$

Из свойства перемежаемости корней следует, что наименьший корень  $x_1^s$  всегда меньше всех корней многочлена  $K_r^{(2,n)}(x)$ , если  $r < s$ . Следовательно, значение  $K_r^{(2,n)}(x_1^s)$  всегда положительно, если  $r < s$ , ибо знак числа  $K_r^{(2,n)}(x_1^s)$ , очевидно, совпадает со знаком числа  $K_r^{(2,n)}(0) = \binom{n}{r}$ .

Из этого замечания и (4.2.18) следует утверждение леммы.  $\square$

**Лемма 4.2.3** Пусть  $c_s \leq d$ . Тогда многочлен

$$f(x) = \frac{\left(K_s^{(2,n)}(x)K_{s-1}^{(2,n)}(c_s) - K_{s-1}^{(2,n)}(x)K_s^{(2,n)}(c_s)\right)^2}{c_s - x} \quad (4.2.19)$$

является многочленом, который удовлетворяет свойствам i. и ii. (см. раздел 4.2.1).

**Доказательство.** Многочлен  $f(x)$  удовлетворяет свойству i., ибо функция  $c_s - x$  меняет знак в точке  $c_s$ .

То, что многочлен  $f(x)$  удовлетворяет свойству ii. следует из лемм 4.2.1 и 4.2.2, ибо

$$f(x) = F(x) \left(K_s^{(2,n)}(x)K_{s-1}^{(2,n)}(c_s) - K_{s-1}^{(2,n)}(x)K_s^{(2,n)}(c_s)\right) \quad (4.2.20)$$

и неравенств  $K_{s-1}^{(2,n)}(c_s) > 0$ ,  $K_s^{(2,n)}(c_s) < 0$ , которые являются следствием соотношения (4.2.15).  $\square$

Доказательство следующей леммы можно найти в [7], стр. 543.

**Лемма 4.2.4 (Без доказательства)** Пусть  $x_1^s$  — наименьший корень многочлена  $K_s^{(2,n)}(x)$ ,  $\frac{s}{n} \rightarrow \lambda$ ,  $n \rightarrow \infty$ , и  $\xi = \lim_{n \rightarrow \infty} \frac{x_1^s}{n}$ .

Тогда

$$\xi = \frac{1}{2} - \sqrt{\lambda(1-\lambda)}. \quad (4.2.21)$$

**Теорема 4.2.3 (Оценка Мас-Элиса-Родемича-Рамсея-Велча)** Пусть  $\frac{d}{n} \rightarrow \delta$ ,  $n \rightarrow \infty$ ,  $R(\delta) = \lim_{n \rightarrow \infty} \frac{\log_2 M(n,d)}{n}$ . Тогда справедлива оценка

$$R(\delta) \leq H_2 \left( \frac{1}{2} - \sqrt{\delta(1-\delta)} \right). \quad (4.2.22)$$

**Доказательство.** Пусть  $f(x) = \sum_{j=0}^{2s-1} \alpha_j K_j^{(2,n)}(x)$  — функция, определенная соотношением 4.2.19. Очевидно,

$$\alpha_0 = \frac{1}{2^n} \sum_{j=0}^n \binom{n}{j} f(j). \quad (4.2.23)$$

Отсюда и (4.2.20) вытекает, что

$$\begin{aligned} \alpha_0 &= \frac{1}{2^n} \sum_{j=0}^n \frac{2}{s} \binom{n}{s-1} \left( K_s^{(2,n)}(j) K_{s-1}^{(2,n)}(c_s) - K_{s-1}^{(2,n)}(x) K_s^{(2,n)}(c_s) \right) \sum_{r=0}^{s-1} \frac{K_r^{(2,n)}(j) K_r^{(2,n)}(c_s)}{\binom{n}{r}} \\ &= \frac{1}{2^n} \sum_{j=0}^n \frac{2}{s} \left( -K_{s-1}^{(2,n)}(j) K_s^{(2,n)}(c_s) \right) K_{s-1}^{(2,n)}(j) K_{s-1}^{(2,n)}(c_s) = -\frac{2}{s} \binom{n}{s-1} K_s^{(2,n)}(c_s) K_{s-1}^{(2,n)}(c_s). \end{aligned} \quad (4.2.24)$$

С другой стороны,

$$f(0) = \frac{\left( \binom{n}{s} K_{s-1}^{(2,n)}(c_s) - \binom{n}{s-1} K_s^{(2,n)}(c_s) \right)^2}{c_s}, \quad (4.2.25)$$

ибо  $K_s^{(2,n)}(0) = \binom{n}{s}$ .

Учитывая соотношение (4.2.15) и равенства (4.2.24) и (9.1.16), мы получим соотношение

$$\frac{f(0)}{\alpha_0} = \frac{s \left( \binom{n}{s} + \binom{n}{s-1} \right)^2}{2c_s \binom{n}{s-1}} \leq \frac{(n-s+1) \binom{n}{s}}{2x_1^s}. \quad (4.2.26)$$

В качестве  $s$  выберем наименьшее значение, для которого  $x_1^s \leq d$ . Согласно лемме 4.2.3 в качестве  $\lambda$ ,  $0 < \lambda < \frac{1}{2}$ , надо выбрать наименьшее значение, для которого

$$\delta \geq \sqrt{\lambda(1-\lambda)} \quad (4.2.27)$$

Очевидно, что если положить  $\lambda = \frac{1}{2} - \sqrt{\delta(1-\delta)}$ , то неравенство (4.2.27) будет выполнено. Отсюда, из теоремы 4.2.2 и (2.0.36) вытекает требуемое соотношение (4.2.22), если использовать асимптотическое выражение для биномиальных коэффициентов (соотношение (2.0.47)).  $\square$

*Коментарии.* Можно проверить, что  $H_2\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) < 1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{2\delta}\right)$ , если  $\delta \in (0, \frac{1}{2})$ . Поэтому оценка Мас-Элиса-Родемича-Рамсея-Велча сильнее оценки Бассалыги-Элайса (2.0.51) на интервале  $(0, \frac{1}{2})$ .

Оценка Элайса-Бассалыги (ЭБ-оценка) была получена в 1965 году. С тех пор она неоднократно улучшалась. В 1971 г. В.М. Сидельников [35] (теорема 2) (см. также [36], [37], [38]) усилил ЭБ-оценку на некотором интервале  $(\delta_0, \frac{1}{2})$ ,  $0 < \delta_0 < \frac{1}{2}$ .

Заметным событием стало появление в оценки Дельсарта [72], используя которую Мас-Элис, Родемич, Рамсей и Велч [79], получили оценку (4.2.22). Эту оценку с помощью идеи, которая была использована при получении оценки Бассалыги-Элайса, можно немного усилить. Полное доказательство этой усиленной оценки очень громоздко и пока не опубликовано в достаточно строгом изложении. Вместе с тем результат не вызывает сомнений. Итоговая граница Мас-Элиса, Родемича, Рамсея и Велча до сих пор (2006 г.) не улучшена.

Как уже говорилось, имеется зазор между верхней границей Мас-Элиса, Родемича, Рамсея и Велча и нижней границей Элайса-Бассалыги (2.0.51) для всех  $\delta$ , принадлежащих интервалу  $(0, \frac{1}{2})$ . Сокращение этого зазора является важной и интересной задачей теории кодирования.

Более того, до сих пор не понятно является ли нижняя асимптотическая оценка Варшамова-Гилберта скорости передачи с помощью последовательности двоичных кодов с относительным кодовым расстоянием  $\delta$  одновременно и верхней оценкой этой скорости. Другими словами, не ясно можно ли усилить оценку Мас-Элиса, Родемича, Рамсея и Велча так, чтобы она совпадала с нижней оценкой Варшамова-Гилберта на некотором интервале изменения параметра  $\delta$ .

Весьма естественен также вопрос: возможно ли усилить асимптотическую оценку Варшамова-Гилберта в двоичном случае. Автор и многие другие ученые предполагают, что этого сделать нельзя.





## Глава 5

# Коды Рида-Соломона и БЧХ-коды

Упомянутые в названии этого раздела коды являются одним из основных классов кодов, изучаемы в теории кодирования на протяжении последних 40 лет. Можно сказать, что почти все известные к настоящему времени коды так или иначе являются обобщением кода Рида-Соломона. Рассматриваемые коды являются достаточно простыми, но вместе с тем важными объектами, знакомство с которыми совершенно необходимо читателю, изучающему теорию кодирования.

Следует сказать, что в данной книге мы изучаем лишь весьма небольшую часть кодов, известных в теории кодирования. Мы не рассматриваем алгебро-геометрические коды, сверточные коды, каскадные коды и многие другие. Для ознакомления с ними заинтересованный читатель может обратиться к монографиям по отдельным вопросам теории кодирования. Некоторые из подобных книг приведены в библиографии см., например, [5], [9] и многие другие издания.

С другой стороны, в этом разделе мы затрагиваем вопросы, относящиеся к БЧХ-кодам, которые редко или никогда не затрагивались в учебных изданиях по теории кодирования. Вместе с они имеют большое прикладное значение. К таким вопросам относятся вычисление в явном виде размерности БЧХ-кода при некотором ограничении на величину его гарантированного кодового расстояния  $d$ , представление циклического БЧХ-кода в виде рекуррентной последовательности, а также в виде последовательности значений функции "след". Кроме того, найдены новые методологические подходы к изучению группы автоморфизмов кода, в том числе и кода Рида-Соломона.

### 5.0.3 Определение кода Рида-Соломона

Как следует из теоремы 1.1.1, для построения линейного кода  $\mathcal{K}$  над полем  $\mathbb{F}_q$  с кодовым расстоянием не меньше  $d$  достаточно построить его проверочную матрицу  $B$ , у которой любой комплект из  $d - 1$  различных столбцов является линейно-независимым. Этот способ построения является наиболее распространенным.

Вместе с тем не надо думать, что задание линейного кода с помощью его проверочной матрицы является единственно возможным. Для многих кодов, например, для кода Рида-Соломона естественным является также задание кода с помощью его порождающей матрицы или как идеала некоторого кольца. Часто подобные способы задания упрощают исследования тонких свойств этого кода по сравнению с представлением стандартного

вида. Об этом будет сказано более подробно ниже.

Наиболее известными матрицами  $B$ , у которых любой комплект из  $d - 1$  столбцов является линейно-независимым, является матрица

$$B = B_{\mathcal{A}}^{(d)} = \begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-2} & \alpha_2^{d-2} & \cdots & \alpha_n^{d-2} \end{pmatrix}, \quad d > 2, \quad (5.0.1)$$

где  $n \leq q$  и  $\mathcal{A} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$  — различные ненулевые элементы поля  $\mathbb{F}_q$ . Мы полагаем, что  $\alpha^0 = 1$  при всех  $\alpha \in \mathbb{F}_q$  в том числе и при  $\alpha = 0$ .

Столбцы любого комплекта из  $d - 1$  столбцов матрицы  $B$  является линейно-независимыми. Это следует из того, что определитель

$$\begin{vmatrix} \beta_1^0 & \beta_2^0 & \cdots & \beta_{d-1}^0 \\ \beta_1 & \beta_2 & \cdots & \beta_{d-1} \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{d-1}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^{d-2} & \beta_2^{d-2} & \cdots & \beta_{d-1}^{d-2} \end{vmatrix}, \quad \beta_j \in \{\alpha_1, \alpha_2, \dots, \alpha_n\}, \quad (5.0.2)$$

с попарно различными  $\beta_j$  является определителем Вандермонда, который, как хорошо известно, отличен от 0. Это как раз и означает, что столбцы  $(\beta_1^0, \beta_1, \dots, \beta_1^{d-2})^T, \dots, (\beta_{d-1}^0, \beta_{d-1}, \dots, \beta_{d-1}^{d-2})^T$  являются линейно-независимыми.

Отсюда вытекает, что кодовое расстояние  $d(\mathcal{K})$  кода  $\mathcal{K}$  с проверочной матрицей  $B_{\mathcal{A}}^{(d)}$  не меньше  $d$  (Теорема 1.1.1). В действительности,  $d(\mathcal{K}) = d$ , ибо любой комплект из  $d - 1$ -мерных столбцов матрицы  $B_{\mathcal{A}}^{(d)}$  является линейно-зависимым над полем  $\mathbb{F}_q$ , т.е. код содержит вектор веса  $d$ .

Код с проверочной матрицей  $B_{\mathcal{A}}^{(d)}$  будем обозначать через  $\mathcal{K}(B_{\mathcal{A}}^{(d)})$ .

Множество  $\mathcal{A}$  часто расширяют, а именно, добавляют к нему элементы  $0 \in \mathbb{F}_q$  и особый элемент  $\infty$ . Мы далее будем полагать, что матрица  $B$  в (1.2.2) определена именно для такого расширенного множества  $\mathcal{A}$ . О подробностях такого расширения мы расскажем ниже в разделе 5.0.4.

Нумерацию столбцов матрицы  $B$  будем производить с помощью элементов множества  $\mathcal{A}$ . Так столбец с номером  $\alpha \in \mathcal{A}$  является  $j$ -ым столбцом, если  $\alpha = \alpha_j$ . Совершенно аналогично поступаем с координатами вектора  $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}) \in \mathbb{F}_q^n$ , их также индексируем элементами множества  $\mathcal{A}$ , которые записаны в определенном порядке.

## 5.0.4 Коды Рида-Соломона.

Мы рассмотрим три вида кодов Рида-Соломона длин  $n = q - 1$ ,  $q$ ,  $q + 1$ , соответственно. Все они имеют в качестве проверочной матрицу вида (5.0.1), но различные множества  $\mathcal{A}$ . Следует сказать, что все рассматриваемые ниже коды Рида-Соломона с кодовым расстоянием  $d$ , очевидно, имеют размерность  $k = n - d + 1$ , ибо размерность пространства строк матрицы  $B_{\mathcal{A}}^{(d)}$  над полем  $\mathbb{F}_q$ , очевидно, равна  $d - 1$ . Все коды лежат на границе Синглтона (оценка (2.0.27)), т.е. они являются MDR-кодами (см. раздел 2.0.6).

Мы рассматриваем следующие три типа кодов Рида-Соломона:

- Тип 1.  $n = q - 1$ . В этом случае множество  $\mathcal{A}$  состоит из всех ненулевых элементов поля  $\mathbb{F}_q$ .
- Тип 2.  $n = q$ . В этом случае множество  $\mathcal{A}$  состоит из всех элементов поля  $\mathbb{F}_q$ . Следует сказать, что столбец  $(\alpha_j^0, \alpha_j, \dots, \alpha_j^{d-2})^T$ , у которого  $\alpha_j = 0$ , имеет по определению вид  $(1, 0, \dots, 0)^T$ .
- Тип 3.  $n = q + 1, d > 3$ . В этом случае множество  $\mathcal{A}$  состоит из всех элементов поля  $\mathbb{F}_q$  и еще одного элемента  $\infty$  (бесконечности), т.е.  $\mathcal{A} = \mathbb{F}_q \cup \{\infty\}$ . Предполагается, что элемент  $\infty$  обладает естественными свойствами этого понятия. Например,  $a\infty = \infty$ ,  $a \neq 0$ ,  $\frac{a}{\infty} = 0$  и т.п. Столбец  $\alpha(\infty) = (\alpha_j^0, \alpha_j, \dots, \alpha_j^{d-2})^T$ , у которого  $\alpha_j = \infty$ , по определению имеет вид  $(0, 0, \dots, 1)^T$ .

Рассмотрим несколько более общую ситуацию. Мы будем считать, что значение многочлена  $f(x) = \sum_{s=0}^{d-2} f_s x^s$  степени не выше  $d-2$  в точке  $\infty$  равно коэффициенту  $f_{d-2}$  при его старшем члене. В частности,  $f(\infty) = 0$ , если степень  $f(x)$  меньше  $d-2$ . В этом случае мы говорим, что  $f(x)$  имеет корень  $\infty$ . Следовательно,  $\alpha(\infty)$  — последовательность значений в точке  $\infty$  многочленов  $1, x, x^2, \dots, x^{d-2}$ .

Более того, соглашение относительно значения  $f(\infty)$  позволяет считать, что каждая строка матрицы  $B_{\mathcal{A}}$  кодов типа 3 также, как и в случае кодов типов 1 и 2, является значением многочлена  $x^j$ ,  $0 \leq j \leq d-2$ , в точках множества  $\mathcal{A}$ .

Заметим, что коды типа 3 можно рассматривать как алгебро-геометрические коды, определенные на кривой рода 0. Более об этом мы распространяться не будем.

Коды Рида-Соломона всех типов будем обозначать одним символом  $RS_q(n, d)$ . Все они лежат на границе Синглтона (см. секцию 2.0.6) и имеют параметры  $[n, n - d + 1, d]_q$ . Эти коды являются, так называемым,  $q$ -значными MDR-кодами (определение см. в секции 2.0.6), а именно кодами, которые имеют максимально возможную размерность  $n - d + 1$  при заданных  $n$  и  $d$ .

Следует сказать, что коды типа 3, в некотором смысле, являются наиболее интересным среди, определенных ранее трех типов кодов Рида-Соломона. В частности, они имеют при заданном кодовом расстоянии  $d$  наибольшее значение скорости передачи (отношение размерности кода к его длине). Группа автоморфизмов (определение — ниже) этих кодов является наиболее мощной в классе кодов  $RS_q(n, d)$  всех типов.

Одна из модификаций кода типа 3 (длины  $n = q + 1$ ) будет далее использована как основа для построения "системы открытого шифрования", которую мы будем подробно изучать. В частности, мы подробно изучим группу автоморфизмов этого кода. Эта группа автоморфизмов имеет наиболее сложное строение по сравнению с группами автоморфизмов кодов типов 1. и 2. Мы сначала изучим группу автоморфизмов кодов типа 2., а затем рассмотрим свойства группы автоморфизмов кода типа 3.

Как будет показано далее, коды типа 1 и 3 при некотором упорядочивании множества  $\mathcal{A}$  являются циклическими (для кода типа 2 это не всегда так). Они могут быть заданы (определены) и многими другими способами. Например, код типа 1 может быть представлен как идеал определенного вида в кольце многочленов по  $\text{mod } x^n - 1, n|q-1$ . Переходим к изучению свойств кодов  $RS_q(n, d)$ .

**Теорема 5.0.4** Кодом, двойственным к коду  $RS_q(n, d)$  типа 2, является код  $RS_q(n, n - d + 2)$ , а кодом, двойственным к коду  $RS_q(n, d)$  типа 3, является код  $RS_q(n, n - d + 3)$ .

**Доказательство.** Как следует из определения двойственного кода (см. секцию 1.1.3), кодом, двойственным к  $RS_q(n, d)$ , является код  $RS_q^\perp(n, d)$ , натянутый на строки матрицы  $B_{\mathcal{A}}$ . Проверим, что код  $RS_q^\perp(n, d)$  типа 2 или 3 совпадает с кодом  $RS_q(n, n - d + 2)$  или  $RS_q(n, n - d + 3)$ , соответственно.

Заметим, что

$$\sum_{x \in \mathbb{F}_q} x^s = \begin{cases} 0, & \text{если } 0 \leq s < q - 1 \\ -1, & \text{если } s = q - 1 \end{cases}. \quad (5.0.3)$$

Из первого равенства в (5.0.3) следует, что строки матриц  $B_{\mathcal{A}}^{(d)}$  и  $B_{\mathcal{A}}^{(n-d+2)}$  (см. (5.0.1)) при  $\mathcal{A} = \mathbb{F}_q$  ортогональны. Кроме того,  $\dim RS_q^\perp(n, d) = \dim RS_q(n, n - d + 2) = n - d + 1$ . Поэтому  $RS_q^\perp(n, d) = RS_q(n, n - d + 2)$ , что доказывает теорему для кода типа 2.

Для кода типа 3, очевидно, что строки матриц  $B_{\mathcal{A}}^{(d)}$  и  $B_{\mathcal{A}}^{(n-d+3)}$  за исключением последних являются ортогональными. Из второго равенства в (5.0.3) следует, что последние строки этих матриц при  $\mathcal{A} = \mathbb{F}_q \cup \{\infty\}$  также ортогональны, что доказывает утверждение теоремы.  $\square$

Следует отметить, что для кодов  $RS_q(n, d)$  типа 1 теорема 5.0.4 не верна: первые строки матриц  $B_{\mathcal{A}}^{(d)}$  и  $B_{\mathcal{A}}^{(d')}$  при  $\mathcal{A} = \mathbb{F}_q \setminus \{0\}$  не ортогональны при любом  $d'$ .

Векторы кода  $RS_q(n, d)$  типа 2 и 3 удобно представлять как вектор

$$\mathbf{a}_f = (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)), \quad \{\alpha_1, \dots, \alpha_n\} = \mathcal{A}, \quad (5.0.4)$$

значений многочлена  $f(x) = f_0 + f_1x + \dots + f_kx^k$  степени не выше  $k = n - d + 1$  в первом случае (тип 2) и  $k = n - d + 2$  во втором случае (тип 3), где  $f(\alpha) = f_k$ , если  $\alpha = \infty$ .

**Следствие 5.0.1** Кодом, двойственным к коду  $RS_q(n, d)$  типа 2, является код образованный всеми последовательностями  $\mathbf{a}_f$ , у которых  $\deg f \leq n - d$ , а кодом, двойственным к коду  $RS_q(n, d)$  типа 3, является код образованный всеми последовательностями  $\mathbf{a}_f$ , у которых  $\deg f \leq n - d + 1$ .

## 5.1 Циклические коды

Пусть  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ . Вектор  $\mathbf{a}^{(1)} = (a_1, \dots, a_{n-1}, a_0)$  называется циклическим сдвигом вектора  $\mathbf{a}$  на один разряд влево. Циклический сдвиг вектора  $\mathbf{a}$  на  $j$  разрядов влево определим индуктивным образом:  $\mathbf{a}^{(j)} = (\mathbf{a}^{(j-1)})^{(1)}$ , где  $\mathbf{a}^{(0)} = \mathbf{a}$ .

Очевидно, циклический сдвиг вектора  $\mathbf{a}$  на  $j$  разрядов влево совпадает с циклическим сдвигом вектора  $\mathbf{a}$  на  $n - j$  разрядов вправо.

**Определение 5.1.1** Код  $\mathfrak{K}$  называется циклическим, если для любого  $\mathbf{a} \in \mathfrak{K}$  вектор  $\mathbf{a}^{(1)}$  также принадлежит  $\mathfrak{K}$ .

Очевидно, циклический код является замкнутым относительно циклических сдвигов на любое число разрядов как влево так и вправо.

Цикличность кода часто бывает полезной при его практическом использовании. Кроме того циклические коды имеют и интересные алгебраические свойства. Поэтому их изучению уделяется достаточно много внимания.

Мы обозначаем через  $\mathbb{F}_q[x]/x^n - 1$  кольцо вычетов многочленов по  $\text{mod } x^n - 1$  с коэффициентами из поля  $\mathbb{F}_q$ . Каждому вектору  $\mathbf{a} = (a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n$  сопоставим многочлен  $\mathbf{a}(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\text{mod } x^n - 1$ . И наоборот, каждому многочлену  $\mathbf{a}(x)$  сопоставим вектор  $\mathbf{a}$ . Таким образом, каждому линейному коду  $\mathfrak{K} \in \mathbb{F}_q^n$  мы сопоставляем линейное подпространство  $\mathfrak{K}(x)$  многочленов из  $\mathbb{F}_q[x]/\text{mod } x^n - 1$  и наоборот.

**Определение 5.1.2** Коды  $\mathfrak{K}$  и  $\mathfrak{K}(x)$  мы называем эквивалентными.

Число  $w(\mathbf{a}(x))$  ненулевых коэффициентов многочлена  $\mathbf{a}(x)$  будем называть весом этого многочлена. Очевидно,  $w(\mathbf{a}) = w(\mathbf{a}(x))$ . Отсюда вытекает, что коды  $\mathfrak{K}$  и  $\mathfrak{K}(x)$  имеют одинаковый весовой спектр. В частности, у эквивалентных кодов  $\mathfrak{K}$  и  $\mathfrak{K}(x)$  совпадают кодовые расстояния:  $d(\mathfrak{K}) = d(\mathfrak{K}(x))$ .

Как хорошо известно, кольцо многочленов  $R_q = R_q^{(n)} = \mathbb{F}_q[x]/\text{mod } x^n - 1$  является кольцом главных идеалов. Другими словами каждый идеал  $I$  кольца  $R_q$  имеет вид

$$I = f(x)R_q = \langle f(x) \rangle, \quad (5.1.1)$$

где  $f(x)$  — многочлен, который делит  $x^n - 1$ .

Совсем нетрудно установить (Упражнение ), что  $f(x)$  в (5.1.1) — это ненулевой многочлен наименьшей степени, который принадлежит идеалу  $I$ .

**Лемма 5.1.1** Линейный код  $\mathfrak{K}$  длины  $n$  является циклическим тогда и только тогда, когда эквивалентный ему код  $\mathfrak{K}(x)$  является идеалом в кольце многочленов  $R_q^{(n)}$ , т.е. тогда и только тогда, когда  $\mathfrak{K}(x) = f(x)R_q^{(n)} = \langle f(x) \rangle$  для некоторого многочлена  $f(x) \in \mathbb{F}_q[x]$ , делящего  $x^n - 1$ .

**Доказательство.** Если  $\mathfrak{K}(x)$  — идеал кольца  $R_q$  и  $\mathbf{a}(x) \in \mathfrak{K}(x)$ , то многочлен  $x\mathbf{a}(x)$  также принадлежит идеалу  $\mathfrak{K}(x)$ . Это следует из определения идеала.

С другой стороны, многочлену  $x\mathbf{a}(x)$  соответствует вектор  $\mathbf{a}^{(1)}$ , который является циклическим сдвигом вектора  $\mathbf{a}$ , т.е.  $\mathbf{a}^{(1)} \in \mathfrak{K}$ .

Следовательно, если  $\mathfrak{K}$  — циклический код, то линейное подпространство  $\mathfrak{K}(x)$ , очевидно, инвариантно относительно умножения его элементов на моном  $x$ . Отсюда следует, что  $\mathfrak{K}(x)$  является идеалом кольца  $R_q$ .  $\square$

Многочлен  $f(x)$  называется порождающим многочленом кода  $\mathfrak{K}(x) = \langle f(x) \rangle$ .

### Теорема 5.1.1

*i. Пусть*

$$x^n - 1 = \prod_{i=0}^s f_i^{\lambda_i}(x), \quad (5.1.2)$$

где  $f_i(x)$  — неприводимый над полем  $\mathbb{F}_q$  многочлен степени  $l_i$ , и пусть  $\theta_i \in \mathbb{F}_{q^{l_i}}$ ,  $i = 0, \dots, s$ , — его корень.

Код  $\mathfrak{K}_f(x)$ , эквивалентный линейному циклическому коду  $\mathfrak{K}_f$  с порождающим многочленом

$$f(x) = f_{i_1}^{\lambda'_{i_1}}(x) \cdots f_{i_m}^{\lambda'_{i_m}}(x), \lambda'_{i_j} \leq \lambda_{i_1}, \quad (5.1.3)$$

образован всеми многочленами  $\mathbf{a}(x)$ , у которых корнями являются элементы  $\theta_{i_1}, \dots, \theta_{i_m}$  с кратностями  $\lambda'_i$ ,  $i = 1, \dots, m$ , соответственно, т.е.  $\mathfrak{K}_f(x) = f(x)R_q^{(n)}$ .

ii. Предположим, что многочлен  $x^n - 1$  не имеет кратных корней и  $\tau_1, \dots, \tau_s$  все корни многочлена  $f(x)$ .

Тогда проверочная матрица  $B_f$  циклического кода  $\mathfrak{K}$  с порождающим многочленом  $f(x)$  имеет вид

$$B_f = \begin{pmatrix} \tau_1^0 & \tau_1^1 & \tau_1^2 & \cdots & \tau_1^{n-1} \\ \tau_2^0 & \tau_2^1 & \tau_2^2 & \cdots & \tau_2^{n-1} \\ \tau_3^0 & \tau_3^1 & \tau_3^2 & \cdots & \tau_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \tau_s^0 & \tau_s^1 & \tau_s^2 & \cdots & \tau_s^{n-1} \end{pmatrix}. \quad (5.1.4)$$

iii. Проверочные матрицы  $B_f$  и

$$B'_f = \begin{pmatrix} \theta_{i_1}^0 & \theta_{i_1}^1 & \theta_{i_1}^2 & \cdots & \theta_{i_1}^{n-1} \\ \theta_{i_2}^0 & \theta_{i_2}^1 & \theta_{i_2}^2 & \cdots & \theta_{i_2}^{n-1} \\ \theta_{i_3}^0 & \theta_{i_3}^1 & \theta_{i_3}^2 & \cdots & \theta_{i_3}^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \theta_{i_m}^0 & \theta_{i_m}^1 & \theta_{i_m}^2 & \cdots & \theta_{i_m}^{n-1} \end{pmatrix}. \quad (5.1.5)$$

определяют один и тот же код  $\mathfrak{K}$ .

**Доказательство.** Пункт i. По лемме 5.1.1 код  $\mathfrak{K}(x)$  является идеалом  $I$  кольца  $R_q^{(n)}$ . Любой идеал  $I$  этого кольца является главным. Следовательно, он может быть задан с помощью порождающего многочлена  $f: I = f(x)R_q^{(n)}, f|x^n - 1$ .

Таким образом,  $I$  состоит из всех многочленов  $\mathbf{a}(x) \in R_q^{(n)}$ , которые имеют в качестве своих корней все корни  $\theta_{i_1}, \dots, \theta_{i_m}$  многочлена  $f(x)$  с теми же кратностями, что и у многочлена  $f(x)$ . Так как  $f(x)|x^n - 1$ , то кратность корней  $f(x)$  не превосходит кратности соответствующих корней многочлена  $x^n - 1$ .

Пункт ii. Очевидно, что  $\mathbf{a}(\tau_j) = 0$ ,  $j = 1, \dots, s$ , тогда и только тогда, когда  $B_f \mathbf{a}^T = 0$ .

Пункт iii. Если  $\mathbf{a}(\theta_j) = 0$ ,  $j = 1, \dots, m$ , то и  $\mathbf{a}(\theta_j^q) = 0$ ,  $j = 1, \dots, s$ . Отсюда следует, что  $\mathbf{a}(\theta_j) = 0$ ,  $j = 1, \dots, s$ , ибо каждый элемент  $\tau_j$  сопряжен над полем  $\mathbb{F}_q$  с одним из элементов  $\theta_{i_1}, \dots, \theta_{i_m}$ .  $\square$

Заметим, что если  $n$  и характеристика  $p$  поля  $\mathbb{F}_q$  — взаимно простые числа ( $(p, n) = 1$ ), то многочлен  $x^n - 1$  не имеет кратных корней. Это следует из того, многочлены  $x^n - 1$  и  $nx^{n-1}$  (производная  $x^n - 1$ ) взаимно просты.

Упражнение. Доказать, что идеалы  $\langle f_i^{\lambda_i}(x) \rangle$  и  $\langle f_i^{\lambda_i+1}(x) \rangle$  совпадают в кольце многочленов  $R_q^{(n)}$ .

### 5.1.1 Циклические коды $RS_q(n, d)$ типа 1

Ниже мы докажем, что при некотором упорядочивании множества  $\mathcal{A}$  коды  $RS_q(n, d)$ ,  $n = q - 1$ , типа 1 имеют эквивалентное представление в виде идеала кольца  $R_q^{(n)}$  вычетов по модулю многочлена  $x^n - 1$ . Вместе с тем далее естественно рассматривать несколько более широкий класс циклических кодов, чем коды  $RS_q(n, d)$ ,  $n = q - 1$ , а именно коды, у которых длина  $n$  является делителем числа  $q - 1$ . Остановимся на этом более подробно.

Пусть  $\theta$  — элемент поля  $\mathbb{F}_q$  порядка  $n$ ,  $n|q-1$ , и  $f_{d,\theta}(x) = (x-1)(x-\theta)\cdots(x-\theta^{d-2})$  — минимальный многочлен над  $\mathbb{F}_q$  элементов  $1, \theta, \dots, \theta^{d-2}$ . Рассмотрим в качестве множества  $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\}$  в определении матрицы  $B_{\mathcal{A}}^{(d)}$  множество  $\mathcal{A}_\theta = \{\theta^j | j = 0, \dots, n-1\}$ , т.е. положим  $\alpha_j = \theta^{j-1}$ ,  $j = 1, \dots, n$ .

**Лемма 5.1.2** *Код  $\mathfrak{K}(x)$ , эквивалентный коду  $\mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)})$ , является идеалом в кольце многочленов  $R_q^{(n)}$ , порожденным многочленом  $f_{d,\theta}(x)$  и состоит из многочленов  $\mathbf{a}(x) \in R_q^{(n)}$  таких, что  $\mathbf{a}(\theta^j) = 0$ ,  $j = 0, \dots, \theta^{d-2}$ .*

**Доказательство.** Если  $\mathbf{a} = (a_0, \dots, a_{n-1})$ , то

$$\mathbf{a} \cdot B_{\mathcal{A}_\theta}^{(d)T} = 0. \quad (5.1.6)$$

Равенство (5.1.6), очевидно, можно записать в виде  $\mathbf{a}(\theta^j) = 0$ ,  $j = 0, \dots, \theta^{d-2}$ . Это показывает, что код  $\mathfrak{K}(x)$  является идеалом, порожденным многочленом  $f_{d,\theta}(x)$ . Отсюда и из леммы 5.1.2 следует доказываемая лемма.  $\square$

**Следствие 5.1.1** *Линейный код  $\mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)}) \subseteq \mathbb{F}_q^n$ ,  $n|q-1$ , является циклическим кодом.*

**Доказательство** следует из лемм 5.1.2 и 5.1.1.  $\square$

### 5.1.2 Представление вектора циклического кода в виде рекуррентной последовательности

**Определение 5.1.3** *Многочлен  $f(x)$ ,  $f(x)|x^n - 1$ ,  $\deg f(x) = n - k$ , называется порождающим многочленом линейного циклического кода  $\mathfrak{K}$ , если эквивалентный ему код  $\mathfrak{K}(x)$  является идеалом  $I = \langle f(x) \rangle$ , порожденным многочленом  $f(x)$  в кольце  $R_q^{(n)}$  многочленов по  $\text{mod } x^n - 1$ .*

*Многочлен  $g(x) = \frac{x^n - 1}{f(x)}$ ,  $\deg g(x) = k$ , называется анулирующим или проверочным многочленом кода  $\mathfrak{K}$ .*

Последнее название объясняется тем, что для любого  $\mathbf{a}(x) \in \mathfrak{K}(x)$

$$\mathbf{a}(x)g(x) = 0 \text{ mod } (x^n - 1). \quad (5.1.7)$$

Это соотношение вытекает из того, что многочлен  $\mathbf{a}(x)$  кратен многочлену  $f(x)$  и, следовательно, многочлен  $\mathbf{a}(x)g(x)$  кратен многочлену  $x^n - 1$ , т.е. является нулевым многочленом в кольце  $R_q^{(n)}$ .

Если  $g(x) = \sum_{i=0}^k g_{k-i}x^i$ ,  $g_0 = 1$ , то равенство (5.1.7) можно записать в виде

$$\text{коэфф}_{x^j} \mathbf{a}(x)g(x) = a_j + a_{j-1}g_1 + \dots + a_{j-k+1}g_{k-1} + a_{j-k}g_k = 0, \quad j = 0, \dots, n-1, \quad (5.1.8)$$

где индексы у элементов  $a_i$  приводятся по  $\text{mod } n$ . Отсюда вытекает

**Лемма 5.1.3** *Каждый вектор  $\mathbf{a}$  линейного циклического кода  $\mathfrak{K}$  с порождающим многочленом  $f(x)$  является линейной рекуррентной последовательностью с законом рекурсии*

$$a_{j+k} = -(a_{j+k-1}g_1 + \dots + a_{j-1}g_{k-1} + a_jg_k), \quad j = 1, \dots, n, \quad (5.1.9)$$

где  $(g_0, g_1, \dots, g_k)$  — коэффициенты многочлена  $g(x) = \frac{x^n-1}{f(x)}$ , занумерованные в обратном порядке. Можно также сказать, что  $(g_0, g_1, \dots, g_k)$  — коэффициенты многочлена  $x^k g(x^{-1}) = g_k x^k + g_{k-1} x^{k-1} + \dots + g_1 x + g_0$ , занумерованные обычным образом.

□

Таким образом, каждый вектор  $\mathbf{a}$  циклического линейного кода  $\mathfrak{K}$  однозначно определяется своими первыми  $k$  координатами. Оставшиеся  $n - k$  его координат могут быть последовательно вычислены с помощью линейных соотношений (5.1.9).

**Лемма 5.1.4** *Пусть  $\mathfrak{K}$  — линейный циклический код с порождающим многочленом  $f(x)$  и  $\mathfrak{K}'$  — линейный циклический код с порождающим многочленом  $x^k g(x^{-1})$ , где многочлен  $g(x)$  является аннулирующим для  $\mathfrak{K}$ .*

*Тогда  $\mathfrak{K}' = \mathfrak{K}^\perp$ .*

**Доказательство.** С одной стороны, по определению многочленов  $f(x)g(x) = 0 \bmod (x^n - 1)$ .

С другой стороны, пусть  $\mathbf{a}(x) = f(x)a(x) \in \mathfrak{K}(x)$  и  $\mathbf{b}(x) = g(x)b(x) \in \mathfrak{K}''(x)$ , где  $\mathfrak{K}''$  — код с порождающим многочленом  $g(x)$ . Тогда

$$\mathbf{a}(x)\mathbf{b}(x) = \sum_{i=0}^{n-1} a_i b_{k-i} x^k = \sum_{i=0}^{n-1} \langle \mathbf{a}, \overleftarrow{\mathbf{b}}^{(k)} \rangle x^k = 0 \bmod (x^n - 1), \quad (5.1.10)$$

где  $\overleftarrow{\mathbf{b}} = (b_n, b_{n-1}, \dots, b_1)$  — последовательность  $\mathbf{b}$  кода  $\mathfrak{K}''$ , занумерованная в обратном порядке. Отсюда следует, что  $\langle \mathbf{a}, \overleftarrow{\mathbf{b}} \rangle = 0$  для всех  $\mathbf{a} \in \mathfrak{K}$ ,  $\mathbf{b} \in \mathfrak{K}''$ .

Как нетрудно увидеть, циклический код, состоящий из всех последовательностей  $\overleftarrow{\mathbf{b}}$ , где  $\mathbf{b} \in \mathfrak{K}''$ , совпадает с кодом  $\mathfrak{K}'$  с порождающим многочленом  $x^k g(x^{-1})$ . □

**Что можно сказать о цикличности кодов  $RS_q(n, d)$  типов 2 и 3?**

Если  $n = q$ ,  $q = p^u$ ,  $u > 1$ , (код  $RS_q(n, d)$  типа 2), то многочлен  $x^n - 1$  имеет кратные корни. Этот случай мы рассматривать не будем.

Если  $n = q + 1$  (код  $RS_q(n, d)$  типа 3), то многочлен  $x^n - 1$  не имеет кратных корней. Его корни, очевидно, образуют подгруппу  $G_{q+1} = \{\tau^j | j = 0, \dots, q\}$  мультипликативной группы  $\mathbb{F}_{q^2}^*$  поля  $\mathbb{F}_{q^2}$ , где  $\tau = \theta^{q-1}$  и  $\theta$  — первообразный (порождающий) элемент группы  $\mathbb{F}_{q^2}^*$ .

Как упорядочить элементы множества  $\mathbb{F}_q \cup \{\infty\}$  так, чтобы код  $RS_q(n, d)$  типа 3 был эквивалентен некоторому идеалу кольца  $R_q^{(n)}$ , т.е. упорядочить так, чтобы код  $RS_q(n, d)$  типа 3 был циклическим? Ответ на этот вопрос неизвестен.

Вместе с тем в разделе 5.3.1 мы рассмотрим, так называемые, обобщенные БЧХ-коды длины  $n = q + 1$ , которые имеют такие же параметры как и коды Рида-Соломона типа 3, но их порождающая матрица не имеет вида (5.0.1).



### 5.1.3 Представление векторов циклического кода в виде значений функции "след"

Имеется еще один естественный и часто весьма полезный способ представления векторов циклических кодов. Этот способ использует свойства функции  $Tr(x)$ , которая носит название "след". Напомним некоторые свойства этой функции.

Пусть  $\mathbb{F}_q$  — расширение степени  $l$  поле поля  $\mathbb{F}_r$  так, что  $q = r^l$ . Рассмотрим функцию  $Tr(x)$ , отображающую поле  $\mathbb{F}_q$  в поле  $\mathbb{F}_r$ , следующего вида

$$Tr(x) = Tr_{q/r}(x) = x + x^r + x^{r^2} + \dots + x^{r^{l-1}}. \quad (5.1.11)$$

Непосредственно из определения  $Tr(x)$  вытекает, что  $Tr^r(x) = Tr(x)$ . Это как раз и означает, что значения функции  $Tr(x)$  при  $x \in \mathbb{F}_q$  принадлежат полю  $\mathbb{F}_r$ .

Кроме того, функция  $Tr(x)$ , как нетрудно установить, является линейной над полем  $\mathbb{F}_r$ , т.е.  $Tr(ax + by) = aTr(x) + bTr(y)$ , если  $a, b \in \mathbb{F}_r$ .

**Теорема 5.1.2** Пусть  $\mathfrak{K} \subseteq \mathbb{F}_r^n$  — циклический код длины  $n$ ,  $n|q-1$ ,  $q = r^l$ , и пусть  $f(x) \in \mathbb{F}_r[x]$ ,  $f(x)|x^n - 1$ ,  $\deg f(x) = n - k$ , — порождающий многочлен идеала  $\mathfrak{K}(x) = f(x)R_r^{(n)}$  в кольце многочленов по mod  $(x^n - 1)$ .

Предположим, что  $\theta_0, \theta_1, \dots, \theta_m$  — все попарно несопряженные корни многочлена  $x^k g(x^{-1})$ , где  $g(x) = \frac{x^n - 1}{f(x)}$ ,  $\mathbb{F}_{r_j}$  — наименьшее расширение поля  $\mathbb{F}_r$ , к которому принадлежит элемент  $\theta_j$ , и  $\theta_j = \theta^{k_j}$ , где  $\theta$  — некоторый первообразный элемент поля  $\mathbb{F}_q$ .

Тогда каждый вектор  $\mathbf{a} = (a_1, a_1, \dots, a_n) \in \mathfrak{K}$  может быть единственным образом представлен в виде

$$\mathbf{a} = (T_{\beta_0, \dots, \beta_m}(\theta), T_{\beta_0, \dots, \beta_m}(\theta^2), \dots, T_{\beta_0, \dots, \beta_m}(\theta^n)), \beta_j \in \mathbb{F}_{r_j}, \quad (5.1.12)$$

где  $T_{\beta_0, \dots, \beta_m}(x) = Tr_{r_0/r}(\beta_0 x^{k_0}) + \dots + Tr_{r_m/r}(\beta_m x^{k_m})$ .

Наоборот, любой вектор  $\mathbf{a}$ , определяемый соотношением (5.1.12), принадлежит коду  $\mathfrak{K}$ .

**Доказательство.** Для доказательства единственности достаточно показать, что если коэффициенты  $\beta_0, \dots, \beta_m$  в определении функций  $T_j(\theta_j)$  — не все нули, то вектор  $\mathbf{a}$  является ненулевым.

Положим  $H_j(x) = \alpha_j x^{k_j}$ . Так как  $\theta_j \in \mathbb{F}_{r_j}$ , то  $\theta_j^{r_j} = \theta_j$ . Поэтому многочлен  $Tr_{q/r}(H_j(x))$  может быть записан в виде

$$Tr(H_j(x)) = Tr_{q/r_j}(\alpha_j) x^{k_j} + Tr_{q/r_j}(\alpha_j^r) x^{k_j r} + \dots + Tr_{q/r_j}(\alpha_j^{r^{l_j-1}}) x^{k_j r^{l_j-1}}, \quad x \in \mathbb{F}_q, \quad (5.1.13)$$

где  $Tr_{q/r_j}(y) = y + y^{r_j} + \dots + y^{r_j^{l_j-1}}$  — функция, отображающая поле  $\mathbb{F}_q$  в поле  $\mathbb{F}_{r_j}$  и  $l_j = \frac{l}{r_j}$ . Отсюда следует, что

$$Tr(H_j(x)) = Tr_{r_j/r}(Tr_{q/r_j}(\alpha_j) x^{k_j}) = Tr_{r_j/r}(\beta_j x^{k_j}) = T_j(x^{k_j}), \quad (5.1.14)$$

где  $\beta_j = Tr_{q/r_j}(\alpha_j)$ .

Если  $\beta_j \neq 0$ , то многочлен  $Tr(H_j(x))$  является ненулевым и имеет степень не выше, чем  $q - 2$ . Заметим, что если  $k_j = q - 1$ , то мы полагаем, что  $\deg T_j(x^{k_j}) = 0$ , ибо мы рассматриваем значения многочлена только при ненулевых значениях  $x$ , а  $x^{q-1} = 1$  и, следовательно,  $T_j(x^{q-1}) = \text{const}$  при всех  $x \in \mathbb{F}_q^*$ .

Ключевое замечание. Пусть  $S_j$  — множество степеней мономов, которые входят в многочлен  $T_j(x^{k_j})$  с ненулевыми коэффициентами. Тогда  $S_j \cap S_{j'} = \emptyset$ , если  $j \neq j'$ . Это происходит из-за того, что по условию теоремы корни  $\theta_j$  многочлена  $f(x)$  попарно не сопряжены и, следовательно,  $r^i k_j \not\equiv k_{j'} \pmod{q-1}$ ,  $j \neq j'$ , при всех  $i = 0, \dots, l-1$ .

Из сказанного выше вытекает, что степень многочлена  $T_{\beta_0, \dots, \beta_m}(x) = T_{\beta_0, \dots, \beta_m}(x^{k_0}) + \dots + T_{\beta_0, \dots, \beta_m}(x^{k_m})$  не выше  $q - 2$ . Следовательно, многочлен  $T(x)$  принимает ненулевые значения при  $x \in \mathbb{F}_q^*$ , т.е. вектор  $\mathbf{a}$  является ненулевым. Таким образом, мы показали, что представление (5.1.12) единственно.

Покажем теперь, что векторы  $\mathbf{a}$  вида (5.1.12) и только они являются векторами, принадлежащим циклическому коду  $\mathfrak{K}$ .

С одной стороны, как нетрудно увидеть, последовательность  $\mathbf{a}$  является рекуррентной последовательностью с законом рекурсии (5.1.9), где  $(g_0, g_1, \dots, g_k)$  — коэффициенты многочлена  $x^k g(x^{-1}) = g_k x^k + g_{k-1} x^{k-1} + \dots + g_1 x + g_0$ . Отсюда и из леммы 5.1.3 вытекает, что  $\mathbf{a} \in \mathfrak{K}$ .

С другой стороны размерность пространства  $L$ , натянутого на последовательности  $\mathbf{a}$ , очевидно, равна  $\deg x^k g(x^{-1}) = k$ , т.е.  $L = \mathfrak{K}$ .  $\square$

Некорым огрублением предыдущей теоремы является следующее утверждение.

**Теорема 5.1.3** Пусть  $\mathfrak{K} \subseteq \mathbb{F}_r^n$  — циклический код длины  $n$ ,  $n|q-1$ ,  $q = r^l$ , и пусть  $f(x) \in \mathbb{F}_r[x]$ , где  $f(x)|x^n - 1$ ,  $\deg f(x) = n - k$ , — порождающий многочлен идеала  $\mathfrak{K}(x) = f(x)R_r^{(n)}$  в кольце многочленов по  $\text{mod}(x^n - 1)$ . Как следует из леммы 5.1.3, код  $\mathfrak{K}$  является также рекуррентной последовательностью с законом рекурсии (5.1.9).

Предположим, что  $\theta_0, \theta_1, \dots, \theta_s \subseteq \mathbb{F}_q$  — все корни многочлена  $x^k g(x^{-1})$ , где  $g(x) = \frac{x^n - 1}{f(x)}$ ,  $\mathbb{F}_{r_j}$  — наименьшее расширение поля  $\mathbb{F}_r$ , к которому принадлежит элемент  $\theta_j$ , и  $\theta_j = \theta^{k_j}$ , где  $\theta$  — некоторый первообразный элемент поля  $\mathbb{F}_q$ .

Тогда каждый вектор  $\mathbf{a} = (a_1, a_1, \dots, a_n) \in \mathfrak{K}$  может быть единственным образом представлен в виде

$$\mathbf{a} = (a_0, a_1, \dots, a_{n-1}), \text{ где } a_t = \sum_{j=1}^s \beta_j \theta_j^t, \beta_j \in \mathbb{F}_{r_j}, t = 0, \dots, n-1. \quad (5.1.15)$$

Наоборот, любой вектор  $\mathbf{a}$ , определяемый соотношением (5.1.15), принадлежит коду  $\mathfrak{K}$ , если  $a_t \in \mathbb{F}_r$  для всех  $t$ .

Теорему 5.1.3 в некоторых случаях удобнее использовать, чем теорему 5.1.2.

#### 5.1.4 Представление элементов циклического кода в виде элементов группового кольца циклической группы над конечным полем

Пусть  $G$  — циклическая группа порядка  $n$ , в которой групповую операцию мы обозначаем символом  $\cdot$ . Таким образом,  $G$  — группа, каждый элемент  $h$  которой имеет вид

$h = g^j$ ,  $0 \leq j < n$ , где  $g$  — некоторый элемент группы  $G$ , который называется порождающим. Заметим, что при  $n > 2$  у группы  $G$  имеется несколько различных порождающих элемента. Обычно циклическую группу отождествляют с аддитивной группой вычетов по  $\text{mod } n$  или мультипликативной группой корней  $n$ -й степени из единицы в том или ином поле.

**Определение 5.1.4** Пусть  $\mathfrak{G}$  — конечная мультипликативная группа порядка  $n$ . Слово мультипликативная означает, что групповая операция группы  $\mathfrak{G}$  записывается с помощью знака умножения  $\cdot$ . Этот знак мы будем часто упускать. Групповое кольцо  $H(\mathfrak{G})$  группы  $G = \{g_0, g_1, \dots, g_{n-1}\}$  над конечным полем  $\mathbb{F}_q$  представляет собой множество формальных сумм элементов из  $\mathfrak{G}$  с коэффициентами из  $\mathbb{F}_q$  следующего вида

$$\mathfrak{k}(a_{g_0}, \dots, a_{g_{n-1}}) := \sum_{g \in \mathfrak{G}} a_g g = a_{g_0} g_0 + a_{g_1} g_1 + \dots + a_{g_{n-1}} g_{n-1}, \quad a_g \in \mathbb{F}_q, \quad (5.1.16)$$

на котором заданы две операции: сложение  $+$  и умножение  $\cdot$ .

Сложение в кольце  $H(\mathfrak{G})$  определяется как покомпонентное сложение в поле  $\mathbb{F}_q$ , т.е.  $\mathfrak{k}(a_{g_0}, \dots, a_{g_{n-1}}) + \mathfrak{k}(a'_{g_0}, \dots, a'_{g_{n-1}}) = \mathfrak{k}(a_{g_0} + a'_{g_0}, \dots, a_{g_{n-1}} + a'_{g_{n-1}})$ .

Что касается умножения, то оно определяется следующим образом

$$\mathfrak{k}(a_{g_0}, \dots, a_{g_{n-1}}) \mathfrak{k}(a'_{g_0}, \dots, a'_{g_{n-1}}) = \sum_{g, g' \in \mathfrak{G}} a_g a_{g'} g g' = \mathfrak{k}(b_{g_0}, \dots, b_{g_{n-1}}), \quad (5.1.17)$$

где  $b_h = \sum_{gg'=h} a_g a_{g'} = \sum_{g \in \mathfrak{G}} a_g a_{g^{-1}h}$  (свертка в группе  $\mathfrak{G}$  последовательностей  $(a_{g_0}, \dots, a_{g_{n-1}})$  и  $(a'_{g_0}, \dots, a'_{g_{n-1}})$ ).

Эквивалентным образом групповое кольцо можно определить как множество всех функций, определенных на элементах группы  $\mathfrak{G}$ , со значениями в поле  $\mathbb{F}_q$ . Операция сложения в кольце функций — обычная, поточечная, а операция умножения — свертка вида (5.1.17).

Если  $\mathfrak{G} = \mathfrak{C}_n$  — циклическая группа порядка  $n$  и  $x$  — ее образующий элемент, то элемент  $\mathfrak{k}$  группового кольца  $H(\mathfrak{C}_n)$  можно представить в виде

$$\mathfrak{k} = \mathfrak{k}(a_0, \dots, a_{n-1}) = \sum_{j=0}^{n-1} a_j x^j, \quad a_j \in \mathbb{F}_q. \quad (5.1.18)$$

В свою очередь равенство (5.1.17) можно, очевидно, записать в виде

$$\mathfrak{k}(a_0, \dots, a_{n-1}) \mathfrak{k}(a'_0, \dots, a'_{n-1}) = \sum_{i,j=0}^{n-1} a_i a'_j x^{i+j}, \quad (5.1.19)$$

где сложение в показателе каждого монома  $x^{i+j}$  является сложением по модулю  $n$  в виду того, что в группе  $\mathfrak{C}_n$  выполнено равенство  $x^n = 1$ , где символ  $1$  в данном случае означает единицу кольца  $\mathfrak{C}_n$ .

Выражение (5.1.19) представляет собой умножение двух многочленов  $\mathfrak{k}(a_0, \dots, a_{n-1})$  и  $\mathfrak{k}(a'_0, \dots, a'_{n-1})$  с коэффициентами из поля  $\mathbb{F}_q$ , в котором показатели у всех мономов  $x^{i+j}$  приводятся по модулю  $n$ . Это условие, как нетрудно увидеть, выполняется тогда и

только тогда, когда умножение многочленов в (5.1.19) проводить по модулю многочлена  $x^n - 1$ , ибо  $x^{i+j \bmod n} \equiv x^{i+j} \bmod x^n - 1$ .

Таким образом, одним из возможных и важнейшим представлением группового кольца  $H(\mathfrak{C}_n)$  является кольцо  $\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  многочленов по модулю многочлена  $x^n - 1$ . Это представление очень удобно и мы его будем далее использовать.

Другим естественным представлением кольца  $H(\mathfrak{C}_n)$  является представление в виде кольца циркулянтных матриц с элементами из поля  $\mathbb{F}_q$ . Поясним, что это такое.

Рассмотрим  $n \times n$ -матрицу

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad (5.1.20)$$

элементы которой принадлежат полю  $\mathbb{F}_q$ . Очевидно,  $C^n = I$ , где  $I$  — единичная матрица. Заметим, что мультипликативная группа матриц  $C^j$ ,  $j = 0, 1, \dots, n-1$  представляет собой, так называемое, регулярное представление циклической группы  $\mathfrak{C}_n$  над полем  $\mathbb{F}_q$ .

Положим  $C_j = C^j$ ,  $j = 0, 1, \dots, n-1$ .

Рассмотрим кольцо  $\mathcal{C}(n, \mathbb{F}_q) = \mathcal{C}(\mathbb{F}_q)$ , образованное всеми матрицами вида  $A = a_0 C_0 + \dots + a_{n-1} C_{n-1}$ ,  $\gamma_j \in \mathbb{F}_q$ , в котором кольцевые операции являются обычные сложение и умножение матриц. Очевидно, что матрицы  $C_j$ ,  $j = 0, 1, \dots, n-1$ , являются линейно-независимыми над полем  $\mathbb{F}_q$ , поэтому  $\mathcal{C}(n, \mathbb{F}_q)$  изоморфно групповому кольцу  $H(\mathfrak{C}_n)$ . Это еще одно точное представление кольца  $H(\mathfrak{C}_n)$ . Отметим, что единичная матрица  $I$  с элементами из  $\mathbb{F}_q$  является единицей кольца  $\mathcal{C}(n, \mathbb{F}_q)$ .

Матрицы  $A$  из кольца  $\mathcal{C}(\mathbb{F}_q)$  будем называть циркулянтами, ибо каждая строка  $A$  является циклическим сдвигом ее первой строки.

Очевидно, что аддитивная группа кольца  $\mathcal{C}(\mathbb{F}_q)$  изоморфна группе  $\mathbb{F}_q \times \dots \times \mathbb{F}_q$  ( $n$  раз). Структуру мультипликативной полугруппы кольца  $H(\mathfrak{C}_n) \cong \mathcal{C}(\mathbb{F}_q)$  мы изучим в следующем разделе.

## Структура мультипликативной полугруппы кольца $H(\mathfrak{C}_n)$

Так как кольцо вычетов  $\mathbb{F}_q[x]/(x^l - 1)\mathbb{F}_q[x]$  и кольцо  $\mathcal{C}(\mathbb{F}_q)$  являются точными представлениями кольца  $H(\mathfrak{C}_n)$ , то кольца  $\mathbb{F}_q[x]/(x^l - 1)\mathbb{F}_q[x]$  и  $\mathcal{C}(\mathbb{F}_q)$  изоморфны. Очевидно, что взаимнооднозначное отображение  $\pi$

$$\pi : \sum_{i=0}^{l-1} \gamma_i C_i \leftrightarrow \sum_{i=0}^{l-1} \gamma_i x^i, \quad \gamma_i \in \mathbb{F}_q, \quad (5.1.21)$$

является изоморфизмом колец  $\mathcal{C}(\mathbb{F}_q)$  и  $\mathbb{F}_q[x]/(x^l - 1)\mathbb{F}_q[x]$ .

Мы будем рассматривать только случай  $(n, q) = 1$ . В этом случае многочлен  $x^n - 1$  не имеет кратных корней. (Упражнение)

Пусть

$$x^n - 1 = \prod_{i=0}^{s-1} f_i(x), \quad (5.1.22)$$

где  $f_i$  — неприводимые над  $\mathbb{F}_q$  многочлены степени  $n_i$ . Так как  $x^l - 1$  не имеет кратных корней, то все  $f_i$  взаимно просты.

**Лемма 5.1.5** *Существует взаимно однозначное соответствие между неприводимыми многочленами  $f_i$  из разложения (5.1.22) и различными циклотомическими классами  $S_r = \{rq^j \bmod n \mid j = 0, \dots, n-1\}$  кольца  $\mathbf{Z}_n$  вычетов по модулю  $n$ .*

*Степень  $n_i$  многочлена  $f_i(x)$  равна числу элементов циклотомического класса  $S_r$ , который соответствует многочлену  $f_i(x)$ .*

**Доказательство.** Элемент  $x$  мы будем рассматривать как корень уравнения  $x^n - 1 = 0$ .

При любом целом  $r$  элемент  $x^r$  также является корнем многочлена  $x^n - 1$ . (Упражнение) Кроме того, все элементы  $x^r$ ,  $r = 0, \dots, n-1$ , попарно не сравнимы по  $\bmod (x^n - 1)$  и потому являются всеми корнями уравнения  $x^n - 1 = 0$  степени  $n$ .

Отсюда следует, что при некотором  $r$  элемент  $x^r$  является корнем многочлена  $f_i(x)$ . Многочлены  $f_i(x)$  при различных  $i$  взаимно простые, поэтому  $x^r$  — корень только одного неприводимого многочлена  $f_i(x)$ .

С другой стороны, если  $x^r$  — корень  $f_i(x)$ , то корнем многочлена  $f_i(x)$  является и элемент  $x^{rq}$ . Легко увидеть, что все корни неприводимого над  $\mathbb{F}_q$  полинома  $f_i(x)$  получаются из одного с помощью суперпозиция нескольких отображений  $x^r \rightarrow x^{rq}$ . Заметим, что число  $rq$  в показателе монома  $x^{rq}$  автоматически приводится по модулю  $n$ , т.е.  $rq \in S_r$ . Это устанавливает взаимно однозначное соответствие между циклотомическими классами и неприводимыми многочленами  $f_i(x)$ .

Степень неприводимого многочлена  $f_i(x)$ , очевидно, равна числу элементов циклотомического класса  $S_r$ , где  $r$  — одно из чисел, для которого  $x^r$  является корнем многочлена  $f_i(x)$ .  $\square$

В частности, если  $n$  простое число (простое число Мерсена) и  $q$  — первообразный элемент по  $\bmod n$ , то многочлен  $x^n - 1 = 0$  является произведением двух неприводимых многочленов:  $x - 1$  и  $\frac{x^n - 1}{x - 1}$ . Если  $q = 2$  и  $n = 2^l - 1$  — простое число, то, как нетрудно установить, в разложении (5.1.22) входит один многочлен степени 1 и  $\frac{2^l - 2}{l}$  многочленов степени  $l$ . (Упражнение)

Предположим, что многочлен  $f(x)$  является делителем многочлена  $x^n - 1$ . Очевидно, идеал  $R_f$  кольца  $R = \mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$ , образованный всеми многочленами кольца  $R$ , которые кратны многочлену  $\frac{x^n - 1}{f(x)}$ , имеет размерность  $\deg f(x)$ . Как нетрудно увидеть, идеал  $R_f$  можно определить и по другому: идеал  $R_f$  образован всеми многочленами  $r(x)$  кольца  $R$ , для которых выполнено сравнение  $f(x)r(x) \equiv 0 \bmod (x^n - 1)$ . (Упражнение)

**Лемма 5.1.6** *Пусть  $R_f$  и  $R_g$  — два идеала, у которых многочлены  $f$  и  $g$  взаимно просты. Тогда*

$$R_{f \cdot g} = R_f \oplus R_g, \quad (5.1.23)$$

где знак  $\oplus$  означает прямую сумму линейных над  $\mathbb{F}_q$  пространств  $R_f$  и  $R_g$ .

**Доказательство.** В условиях леммы идеал  $R_f \oplus R_g$ , очевидно, состоит из многочленов кратных многочлену  $\frac{x^n-1}{f(x)g(x)}$ . Отсюда следует утверждение леммы.  $\square$

(Упражнение. Обобщить лемму на тот случай, когда многочлены  $f$  и  $g$  не взаимно просты.)

Отметим, что если  $f(x)$  является неприводимым многочленом, то кольцо  $R_f$  изоморфно конечному полю  $\mathbb{F}_{q^m}$ , где  $m = \deg f(x)$ , ибо, как нетрудно увидеть, что  $R_f \cong \mathbb{F}_q[x]/f(x)\mathbb{F}_q[x]$ . (Упражнение)

**Следствие 5.1.2** *Кольцо вычетов  $R = \mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  является прямой суммой колец  $R_{f_j}$ ,  $j = 0, \dots, s-1$ :*

$$R = R_{f_0} \oplus \dots \oplus R_{f_{s-1}} \cong \mathbb{F}_{q^{n_0}} \oplus \dots \oplus \mathbb{F}_{q^{n_{s-1}}} \quad (5.1.24)$$

**Доказательство** непосредственно следует из соотношения (5.1.22) и леммы (5.1.6).  $\square$

Компоненты  $R_{f_j}$  в равенстве (5.1.24) являются попарно ортогональными, т.е. если  $f(x) \in R_{f_j}$  и  $g(x) \in R_{f_i}$ , то  $f(x)g(x) = 0$  в кольце  $R$ , в том случае, когда  $i \neq j$ . Это утверждение непосредственно вытекает из определения идеала  $R_f$ .

Рассмотрим эндоморфизм  $\varphi_i$ ,  $i = 0, \dots, s-1$ , отображающий элемент  $f(x) = \sum_{i=0}^{n-1} \gamma_i x^i \in \mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  в элемент  $\varphi_i(f(x))$  вида

$$\varphi_i(f(x)) \equiv F_i(x) \frac{x^l - 1}{f_i(x)} f(x) \pmod{x^l - 1}, \quad (5.1.25)$$

где полином  $F_i(x)$ ,  $\deg F_i(x) < n_i$ , определен с помощью следующего сравнения

$$F_i(x) \frac{x^n - 1}{f_i(x)} \equiv 1 \pmod{f_i(x)}. \quad (5.1.26)$$

Отметим, что полином  $F_i(x)$  определен корректно, ибо полиномы  $\frac{x^n-1}{f_i(x)}$  и  $f_i(x)$  взаимно просты, а  $f_i(x)$  — неприводимый полином.

**Лемма 5.1.7** *Эндоморфизм  $\varphi_i$  гомоморфно отображает кольцо  $\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  в кольцо  $R_{f_i}$ , которое изоморфно конечному полю  $\mathbb{F}_{q^{n_i}}$ , где  $n_i = \deg f_i(x)$ .*

**Доказательство.** Легко видеть, что  $\varphi_i(f(x)g(x)) = \varphi_i(f(x))\varphi_i(g(x))$  и  $\varphi_i(f(x) + g(x)) = \varphi_i(f(x)) + \varphi_i(g(x))$ . (Упражнение)

Поэтому линейное отображение  $\varphi_i$  является эндоморфизмом кольца  $\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  в свое подкольцо  $R_{f_i}$ .  $\square$

**Следствие 5.1.3** *Единицей подкольца  $\varphi_i(\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x])$  (образа кольца  $\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x]$  при отображении его эндоморфизмом  $\varphi_i$ ) является многочлен  $F_i(x) \frac{x^n-1}{f_i(x)} = \varphi_i(1)$ .*

Заметим, что единица 1 кольца  $\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x] = R$  не принадлежит кольцу  $\varphi_i(\mathbb{F}_q[x]/(x^n - 1)\mathbb{F}_q[x])$ .

Таким образом, отображение  $\varphi_i$  является гомоморфной проекцией элементов кольца  $R$  в подкольцо  $R_i$ , изоморфное конечному полю  $\mathbb{F}_{q^{n_i}}$ .

Лемму (5.1.7) можно преформулировать следующим образом.

**Теорема 5.1.4** *Групповое кольцо над полем  $\mathbb{F}_q$  циклической группы порядка  $n$  в случае  $(n, q) = 1$  является прямым произведением попарно ортогональных подколец, каждое из которых изоморфно некоторому конечному полю  $\mathbb{F}_{q^{n_i}}$  — расширению степени  $n_i$  поля  $\mathbb{F}_q$ , где  $n_i$  — степени неприводимых многочленов из разложения (5.1.22).*

Сделаем еще одно замечание, связанное с групповым кольцом  $\mathcal{C}(\mathbb{F}_q)$ . Как нами было установлено, образ эндоморфизма  $\varphi_i$  является одновременно конечным полем и подкольцом кольца  $R$ . Поэтому конечное поле  $\mathbb{F}_{q^{n_i}}$  (расширение степени  $n_i$  поля  $\mathbb{F}_q$ ) можно реализовать как в виде подкольца кольца вычетов многочленов по  $\text{mod}(x^n - 1)$  так и в виде подкольца кольца циркулянтных матриц  $\mathcal{C}(\mathbb{F}_q)$ .

Выгода в последнем представлении поля  $\mathbb{F}_{q^{n_i}}$  состоит в том, что сложность умножения в кольце циркулянтных матриц или сложность умножения многочленов в кольце вычетов многочленов по  $\text{mod}(x^n - 1)$  может оказаться существенно меньше, чем сложность умножения многочленов по модулю неприводимого многочлена  $f_i$  степени  $n_i$ . Поэтому реализация поля в виде кольца циркулянтных матриц может упростить выполнение операции умножения в некоторых конечных полях. Этот вопрос до конца не исследован.

Вместе с тем также следует отметить, что операция сложения в кольце циркулянтных матриц или кольце вычетов многочленов по  $\text{mod}(x^n - 1)$  такая же или почти такая же как и операция сложения элементов поля  $\mathbb{F}_{q^{n_i}}$  в обычном его представлении.

Сделаем еще ряд полезных замечаний, вытекающих из полученных выше результатов о структуре кольца  $R$ .

Рассмотрим  $n \times n$ -матрицу

$$D_i = F_i(C)F'_i(C) \quad (5.1.27)$$

где многочлен  $F_i(C)$  определен соотношением (5.1.26), а  $F'_i(C) = \frac{x^n - 1}{f_i(x)}$ . Очевидно,  $D_i D_j = 0$ , если  $i \neq j$ .

Заметим, что из леммы 5.1.7 непосредственно следует, что  $D_i^2 = D_i$ , т.е.  $D_i$  — идемпотент кольца  $\mathcal{C}(\mathbb{F}_q)$ .

Лемма 5.1.7 может быть на языке кольца  $\mathcal{C}(\mathbb{F}_q)$  может быть сформулирована следующим образом

**Лемма 5.1.8** *i. Пространство  $\mathbb{F}_q$  может быть представлено в виде прямой суммы ортогональных подпространств  $\mathbb{F}_q D_i = \{\mathbf{a} D_i \mid \mathbf{a} \in \mathbb{F}_q\}$  так, что*

$$\mathbb{F}_q^n = \mathbb{F}_q^n D_0 \oplus \mathbb{F}_q^n D_1 \oplus \cdots \oplus \mathbb{F}_q^n D_{s-1} \quad (5.1.28)$$

*ii. Эндоморфизм  $\widehat{\varphi} : A \rightarrow AD_i$ ,  $A \in \mathcal{C}(\mathbb{F}_q)$ , кольца  $\mathcal{C}(\mathbb{F}_q)$  гомоморфно отображает  $\mathcal{C}(\mathbb{F}_q)$  в свое подкольцо  $\mathcal{C}_i(\mathbb{F}_q) = \mathcal{C}(\mathbb{F}_q) D_i$ . Кольцо  $\mathcal{C}_i(\mathbb{F}_q)$  изоморфно конечному полю  $\mathbb{F}_{q^{n_i}}$ . Для матрицы  $D_i$  выполнено соотношение  $D_i^2 = D_i$ .*

*iii. Регулярное представление циклической группы  $\mathfrak{C}_n$  на пространстве  $\mathbb{F}_q^n$  можно представить в виде прямого произведения представлений на подпространствах  $V_i = \mathbb{F}_q^n D_i$  размерности  $n_i$ ,  $i = 0, \dots, s-1$ . Матрицу  $C^i$  (см. (5.1.20)) в неко-*

тором базисе можно записать в блочно-диагональном виде

$$C^i = \begin{pmatrix} A_0^i & 0 & \cdots & 0 \\ 0 & A_1^i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{s-1}^i \end{pmatrix}, \quad (5.1.29)$$

где  $A_j$  —  $n_j \times n_j$  — матрица, действующая на подпространстве  $V_i$ .

### Идемпотенты кольца $\mathfrak{C}(\mathbb{F}_q)$

Элемент  $e \neq 0$  некоторого кольца  $K$  называется идемпотентом, если  $e^2 = e$ . Например, если  $K = \mathbb{F}_q$ , то единица мультипликативной группы  $\mathbb{F}_q^*$  поля  $\mathbb{F}_q$  является единственным идемпотентом кольца  $\mathbb{F}_q$ . Вообще, если  $E$  — единица кольца  $K$ , то  $E$  — идемпотент этого кольца. В общем случае в кольце имеются идемпотенты отличные от единицы. Например, в кольца  $\mathfrak{C}(\mathbb{F}_q)$  в случае  $(n, q) = 1$  имеется еще один идемпотент  $e$ , отличный от единицы:  $e = \frac{1}{n} \sum_{i=0}^{n-1} C_i$ . (Упражнение) В общем случае вопрос о виде и числе идемпотентов в кольце  $K$  весьма непрост.

#### Теорема 5.1.5

- i. Матрицы  $D_i$ ,  $i = 0, \dots, s-1$ , являются ортогональными идемпотентами кольца матриц  $\mathfrak{C}(\mathbb{F}_q)$ .

Множество всех идемпотентов кольца  $\mathfrak{C}(\mathbb{F}_q)$  является линейным пространством размерности  $s$  над полем  $\mathbb{F}_q$ , натянутым на линейно-независимые матрицы  $D_i$ ,  $i = 0, \dots, s-1$ . (см. (5.1.27))

- ii. Многочлены  $F_i(x) \frac{x^n-1}{f_i(x)}$ ,  $i = 0, \dots, s-1$  являются ортогональными идемпотентами кольца вычетов  $\mathbb{F}_q[x]/(x^n-1)\mathbb{F}_q[x]$ .

Множество всех идемпотентов кольца вычетов  $\mathbb{F}_q[x]/(x^n-1)\mathbb{F}_q[x]$  является линейным пространством размерности  $s$ , натянутым на линейно-независимые многочлены  $F_i(x) \frac{x^n-1}{f_i(x)}$ ,  $i = 0, \dots, s-1$ .

**Доказательство** теоремы непосредственно вытекает из леммы 5.1.8 и следствия 5.1.3 и того очевидного факта, что в поле имеется единственный идемпотент равный единице мультипликативной группы этого поля.  $\square$

**Представление циклического кода в виде прямой суммы простых подколец кольца вычетов многочленов по mod  $(x^n-1)$**

Из теоремы 5.1.4 и теоремы 5.1.5 непосредственно вытекает

**Теорема 5.1.6** Циклический код  $\mathfrak{K} \subseteq \mathbb{F}_q^n$  над полем  $\mathbb{F}_q$  длины  $n$  и размерности  $k$  в случае  $(n, q) = 1$  является прямой суммой некоторых простых подколец  $R_i$ , каждое из



которых изоморфно конечному полю  $\mathbb{F}_{q^{n_i}}$  (расширению степени  $n_i$  поля  $\mathbb{F}_q$ ), где  $n_i$  — степень неприводимых многочленов из разложения (5.1.22).

Таким образом,

$$\mathfrak{K}(x) = \mathfrak{K}_{i_1}(x) \oplus \cdots \oplus \mathfrak{K}_{i_t}(x), \quad (5.1.30)$$

где коды  $\mathfrak{K}_{i_s}(x) = R_{i_s}$  определены перед определением 5.1.2 и  $\{i_1, \dots, i_t\} \subseteq \{0, 1, \dots, m-1\}$  (см. (5.1.22)). Каждый код  $\mathfrak{K}_{i_s}(x)$  входит в сумму (5.1.30) однократно.

Размерность  $k$  кода  $\mathfrak{K}(x)$  равна  $k = \sum_{s=1}^t \dim \mathfrak{K}_{i_s} = \sum_{s=1}^t n_{i_s}$ .

**Теорема 5.1.7** Образующими кода  $\mathfrak{K}_i(x)$  являются многочлены  $F_i(x)^{\frac{x^n-1}{f_i(x)}}, xF_i(x)^{\frac{x^n-1}{f_i(x)}}, \dots, x^{n_i}F_i(x)^{\frac{x^n-1}{f_i(x)}}$ , где первый многочлен является идемпотентом, а последующие — его циклическими сдвигами.

## 5.2 Коды Боуза-Чоудхури-Хоквингема (БЧХ-коды)

Предположим, что поле  $\mathbb{F}_r, r = p^{l'}$ , является подполем поля  $\mathbb{F}_q, q = r^l$ . В этом случае мы будем рассматривать  $r$ -значный подкод  $RS_{q,r}(n, d)$   $RS$ -кода Рида-Соломона  $RS_q(n, d)$ ,  $n \leq q+1$ , который состоит из всех векторов  $RS_q(n, d)$ , координаты которых принадлежат полю  $\mathbb{F}_r$ . В качестве кода  $RS_{q,r}(n, d)$  мы будем рассматривать код с проверочной матрицей  $B_{\mathcal{A}_\theta}^{(d)}$  (определение множества  $\mathcal{A}_\theta$  перед леммой 5.1.2), где  $\theta \in \mathbb{F}_q$  — элемент порядка  $n$ .

В том случае, когда  $RS_q(n, d)$  — код Рида-Соломона типа 1 и  $r < q$ , полученный код называют кодом Боуза-Чоудхури-Хоквингема (обозначение:  $BCH_{q,r}(n, d), n|q-1$ ). Таким образом,

$$BCH_{q,r}(n, d) = RS_q(n, d) \cap \mathbb{F}_r^n, \quad n|q-1. \quad (5.2.1)$$

### 5.2.1 Группа автоморфизмов БЧХ-кода

Следующая лемма непосредственно вытекает из соотношения (5.2.1).

**Лемма 5.2.1** Группа автоморфизмов кода  $RS_q(n, d)$ ,  $n|q-1$ , является подгруппой автоморфизмов кода  $BCH_{q,r}(n, d)$ .

Заметим, что обратное утверждение, вообще говоря, не верно.

Как следует из леммы 5.4.2, БЧХ-код  $BCH_{q,r}(n, d)$ ,  $n = q-1$ , при некотором упорядочивании его разрядов является циклическим.

Заметим, что координаты векторов кода  $BCH_{q,r}(n, d)$  мы индексируем элементами мультипликативной группы  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$  поля  $\mathbb{F}_q$ .

Если  $r < q$ , то, как будет показано ниже, группа автоморфизмов кода  $BCH_{q,r}(n, d)$  содержат элементы, которые не являются циклическими сдвигами. Речь идет о перестановках координат векторов кода  $BCH_{q,r}(n, d)$ , порождаемых отображением

$$\tau : x \rightarrow x^r, \quad x \in \mathbb{F}_q, \quad (5.2.2)$$

индексов координат.

### Лемма 5.2.2

- i. Перестановка  $\tau$  координат векторов кода  $BCH_{q,r}(n, d)$  с проверочной матрицей  $B_{\mathcal{A}_\theta}^{(d)}$ , принадлежит группе автоморфизмов БЧХ-кода  $BCH_{q,r}(n, d)$ .
- ii. Подгруппа  $A(BCH_{q,r}(n, d))$  автоморфизмов БЧХ-кода  $BCH_{q,r}(n, d)$ , порожденная перестановками  $\sigma^{(1)}$  (циклический сдвиг) и  $\tau$ , имеет порядок  $ln$ , если  $\theta$  не принадлежит никакому подполю поля  $\mathbb{F}_q$ .

#### Доказательство.

i. Пусть  $B_{\mathcal{A}_\theta}^{(d)}(\theta^{j-1})$  —  $j$ -ый столбец матрицы  $B_{\mathcal{A}_\theta}^{(d)}$  (определение матрицы  $B_{\mathcal{A}}^{(d)}$  в (5.0.1)), индексированный элементом поля  $\theta^j$ , где  $\theta \in \mathbb{F}_q$  — элемент порядка  $n$ . По определению, вектор  $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_r^n$  принадлежит коду  $BCH_{q,r}(n, d)$  тогда и только тогда, когда

$$\sum_{j=1}^n a_j B_{\mathcal{A}_\theta}^{(d)}(\theta^{j-1}) = 0. \quad (5.2.3)$$

Если возвести левую часть (5.2.3) в степень  $r$ , то мы получим

$$\left( \sum_{j=1}^n a_j B_{\mathcal{A}_\theta}^{(d)}(\theta^{j-1}) \right)^r = \sum_{j=1}^n a_j B_{\mathcal{A}_\theta}^{(d)}(\theta^{r(j-1)}) = 0. \quad (5.2.4)$$

Это равенство показывает, что вектор, полученный перестановкой координат вектора  $\mathbf{a}$  в соответствии с перестановкой  $\tau$ , также является вектором кода  $BCH_{q,r}(n, d)$ . Это доказывает п. i. утверждения теоремы.

ii. Очевидно,  $\tau\sigma^{(1)} = (\sigma^{(1)})^r \tau = \sigma^{(r)}\tau$ , где через  $\sigma^{(r)}$  обозначен циклический сдвиг  $(\sigma^{(1)})^r$  на  $r$  разрядов. Отсюда вытекает, что любое слово  $\iota = \tau^{i_1}\sigma^{(r_1)} \dots \tau^{i_k}\sigma^{(r_k)}$  группы  $\langle \tau, \sigma^{(1)} \rangle$  можно записать единственным образом в виде  $\iota = \sigma^{(j)}\tau^i$  с некоторыми  $i, j$ .

Если  $l'$  — наименьшее число, для которого  $\theta^{r^{l'}} = \theta$ , то то порядок группы  $\langle \tau, \sigma^{(1)} \rangle$  равен  $l'n$ . Очевидно, если  $\theta \in \mathbb{F}_q$  и не принадлежит никакому подполю  $\mathbb{F}_q$ , то  $l' = l$ .  $\square$

Упражнение. Доказать, что  $l' < l$ , если  $r$  принадлежит подполю поля  $\mathbb{F}_q$ .

### 5.2.2 Представление БЧХ-кода в виде идеала кольца $R_r^{(n)}$

Код  $BCH_{r,q}(n, d)$  является циклическим. Поэтому по Следствию 5.1.1 эквивалентный ему код  $BCH_{r,q}(n, d)(x)$  является идеалом  $I = f(x)R_r^{(n)}$  в кольце многочленов по  $\text{mod } (x^n - 1)$ . Наша задача — вычислить порождающий многочлен  $f(x)$  кода  $BCH_{r,q}(n, d)$ .

### Лемма 5.2.3

- a. Порождающий многочлен  $f(x)$  кода  $BCH_{r,q}(n, d)$  с проверочной матрицей  $B_{\mathcal{A}_\theta}^{(d)}$  является минимальным многочленом над  $\mathbb{F}_r$  элементов  $\theta^s$ ,  $s = 0, 1, \dots, d-2$ .
- b. Пусть  $t = d-2 - \left\lfloor \frac{d-2}{r} \right\rfloor$  и  $\{s_1, \dots, s_m\}$  — подмножество множества  $\{1, \dots, d-2\}$ , состоящее из всех чисел не делящихся на  $r$ . Тогда многочлен  $f(x)$  можно представить в виде

$$f(x) = f_0(x)f_1(x) \cdots f_m(x), \quad (5.2.5)$$

где  $f_0(x) = x - 1$  и  $f_j(x)$ ,  $j = 1, \dots, t$ , — неприводимый над  $\mathbb{F}_r$  многочлен степени  $n_j$ ,  $n_j | l$ ,  $q = r^l$ , который является минимальным многочленом элемента  $\theta^{s_j}$ .

**Доказательство.** Очевидно, множество  $\{\theta^{s_1}, \dots, \theta^{s_m}\}$  образуют все попарно несопряженные над полем  $\mathbb{F}_r$  элементы поля  $\mathbb{F}_q$ , которые принадлежат множеству  $\theta^s$ ,  $s = 0, 1, \dots, d - 2$ . Поэтому многочлен  $f(x)$  является минимальным над полем  $\mathbb{F}_r$  многочленом элементов  $\theta^s$ ,  $s = 0, 1, \dots, d - 2$ . Отсюда и из Теоремы 5.1.1 (п. iii.) вытекает утверждение леммы.  $\square$

### 5.2.3 Параметры БЧХ-кода

Размерность БЧХ-кода может быть вычислена с помощью Леммы 5.2.3 или Теоремы 5.1.1. Вместе с тем для доказательства одной из следующих теорем мы предпочитаем использовать другой математический аппарат, который представляется автору более естественным.

**Теорема 5.2.1** Обозначим через  $d'$  — кодовое расстояние и через  $k'$  — размерность на поле  $\mathbb{F}_r$  кода  $BCH_{r,q}(n, d)$  длины  $n \leq q - 1$ ,  $q = r^l$ .

Для параметров кода  $BCH_r(n, d)$ ,  $n | q - 1$ , с проверочной матрицей  $B_{A_\theta}^{(d)}$  справедливы следующие оценки

$$d' \geq d, \quad k' \geq n - 1 - \left( d - 2 - \left\lfloor \frac{d-2}{r} \right\rfloor \right) l, \quad (5.2.6)$$

где  $[x]$  — целая часть числа  $x$ .

**Доказательство.** Очевидно, что  $d' \geq d$ , так как код  $BCH_{r,q}(n, d)$  является подкодом кода  $RS_q(n, d)$ .

Основная идея для доказательства оценки для размерности  $k'$  состоит в следующем. Векторы линейного кода  $BCH_{r,q}(n, d)$  принадлежат пространству  $\mathbb{F}_r^n$ , поэтому проверочную матрицу  $B_A^{(d)}$  кода  $BCH_{r,q}(n, d)$  можно представить в виде проверочной матрицы  $B_{A,r}^{(d)}$  с элементами поля  $\mathbb{F}_r^n$ . Если это сделано, то  $k' = n - t$ , где  $t$  — число линейно-независимых строк матрицы  $B_{A,r}^{(d)}$ . Поэтому далее для доказательства оценки для  $k'$  нам достаточно показать, что матрицу  $B_A^{(d)}$  можно представить как матрицу  $B_{A,r}^{(d)}$  с  $(d - 1 - \lfloor \frac{d-1}{r} \rfloor) l$  строками. Заметим, что строки проверочной матрицы  $B_{A,r}^{(d)}$ , вообще говоря, не являются линейно-независимыми.

Пусть  $\omega = \{\omega_1, \dots, \omega_l\}$  — какой-либо базис поля  $\mathbb{F}_q$  над полем  $\mathbb{F}_r$ . В этом случае элемент  $\alpha \in \mathbb{F}_q$  можно представить в виде  $\alpha = \sum_{j=1}^l a_j \omega_j$ . Вектор  $\bar{\alpha} = (a_1, \dots, a_l)$  представляет элемент  $\alpha$  поля  $\mathbb{F}_q$  в базисе  $\omega$ .

Заменим каждый элемент  $\alpha_i^j$  матрицы  $B_A^{(d)}$  (см. (5.0.1)) соответствующим вектор-столбцом  $\bar{\alpha}_i^j$ . В результате мы получим матрицу  $B_{A,r}^{(d)}$  над  $\mathbb{F}_r$  с  $l(d - 1)$  строками и  $n$  столбцами. Вообще говоря, не все строки  $B_{A,r}^{(d)}$  являются линейно-независимыми по следующей причине.

Вектор  $\bar{\alpha}^r$  линейно выражается через координаты вектора  $\bar{\alpha}$  в виду того, что отображение  $x \rightarrow x^r$  является линейным отображением над полем  $\mathbb{F}_r$ . Поэтому отображение  $\bar{\alpha} \rightarrow \bar{\alpha}^r$  векторного пространства  $\mathbb{F}_r^l$  можно представить как  $\bar{\alpha}^r = \bar{\alpha}U$  с некоторой невырожденной матрицы  $U \in M_l(\mathbb{F}_r)$ .

Обозначим через  $B_{\mathcal{A}}^{(d),i}$   $i$ -ую строку матрицы  $B_{\mathcal{A}}^{(d)}$  и через подматрицу  $B_{\mathcal{A},r}^{(d),i}$  размера  $l \times n$ , которая соответствует строке  $B_{\mathcal{A}}^{(d),i}$  после замены ее элементов на соответствующие вектор-столбцы. Как следует из утверждения предыдущего абзаца, справедливо соотношение

$$B_{\mathcal{A},r}^{(d),ri} = B_{\mathcal{A},r}^{(d),i} \cdot U. \quad (5.2.7)$$

Это означает, что все строки матрицы  $B_{\mathcal{A},r}^{(d),ri}$  линейно зависят от строк матрицы  $B_{\mathcal{A},r}^{(d),i}$ . Таким образом, если  $ri \leq d-2$ , то строки матрицы  $B_{\mathcal{A},r}^{(d),ri}$  можно удалить, не изменяя пространства строк матрицы  $B_{\mathcal{A},r}^{(d)}$ , т.е. не изменяя кода  $BCH_r(n, d)$ .

Число строк  $B_{\mathcal{A}}^{(d),j}$ ,  $j > 0$ , матрицы  $B_{\mathcal{A}}^{(d)}$ , у которых  $j$  кратно  $r$  равно, очевидно,  $\left\lfloor \frac{d-2}{r} \right\rfloor$ . Кроме того, нулевая строка  $B_{\mathcal{A}}^{(d),0}$  порождает подпространство размерности над  $\mathbb{F}_r$  равной 1. Таким образом, размерность над  $\mathbb{F}_r$  строк матрицы  $B_{\mathcal{A},r}^{(d),0}$  не превосходит  $l(d-2 - \left\lfloor \frac{d-2}{r} \right\rfloor) + 1$ . Отсюда следует утверждение теоремы.  $\square$

В некоторых случаях при построении БЧХ-кода  $\widehat{BCH}_{r,q}(n, d)$  вместо матрицы  $B_{\mathcal{A}}^{(d)}$  используют матрицу

$$\widehat{B} = \widehat{B}_{\mathcal{A}}^{(d)} = \begin{pmatrix} \alpha_1^{1+s} & \alpha_2^{1+s} & \dots & \alpha_n^{1+s} \\ \alpha_1^{2+s} & \alpha_2^{2+s} & \dots & \alpha_n^{2+s} \\ \alpha_1^{3+s} & \alpha_2^{3+s} & \dots & \alpha_n^{3+s} \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{d-1+s} & \alpha_2^{d-1+s} & \dots & \alpha_n^{d-1+s} \end{pmatrix}, \quad d > 2, \quad n \leq q, \quad -n \leq s \leq n. \quad (5.2.8)$$

Также как и ранее, в этом случае  $r$ -значный код  $\widehat{BCH}_{r,q}(n, d)$  состоит из всех векторов кода с проверочной матрицей  $\widehat{B}_{\mathcal{A}}^{(d)}$ , координаты которых принадлежат полю  $\mathbb{F}_r$ .

Совершенно также как это делается для кода Рида-Соломона  $RS_q(n, d)$  с проверочной матрицей  $B_{\mathcal{A}}^{(d)}$  доказывается, что кодовое расстояние кода с проверочной матрицей  $\widehat{B}_{\mathcal{A}}^{(d)}$  равно  $d$ .

Особенно полезным бывает использование кода  $\widehat{BCH}_{r,q}(n, d)$  с  $s = 0$  вместо кода  $BCH_{r,q}(n, d)$  в двоичном случае ( $r = 2$ ), когда требуется построить код с нечетным значением  $d$ . В этом случае код  $\widehat{BCH}_{2,q}(n, d)$  имеет размерность большую на 1 по сравнению с размерностью кода  $BCH_{2,q}(n, d)$ . (см. Теоремы 5.2.1 и 5.2.2 ниже)

**Теорема 5.2.2** *Обозначим через  $d'$  — кодовое расстояние и через  $k'$  — размерность на поле  $\mathbb{F}_r$  кода  $\widehat{BCH}_{r,q}(n, d)$  длины  $n \leq q-1$ .*

*Код  $BCH_r(n, d)$  имеет параметры*

$$d' \geq d, \quad k' \geq n - \left( d - 1 - \left\lfloor \frac{d-1}{r} \right\rfloor \right) \frac{l}{l'}, \quad (5.2.9)$$

где  $[x]$  — целая часть числа  $x$ .

**Доказательство** практически не отличается от доказательства теоремы 5.2.1.  $\square$

Следует обратить внимание на то, что размерности кода  $RS_r(n, d)$  и кода  $BCH_{r,q}(n, d)$  или  $\widehat{BCH}_{r,q}(n, d)$  (при  $r < q$ ) в теоремах 5.2.1 и 5.2.2 вычисляются над разными полями: размерность первого — над  $\mathbb{F}_q$ , а размерности второго и третьего — над его подполем  $\mathbb{F}_r$ .

Интересно сравнить результаты этого раздела теоремой 5.1.6.

## 5.2.4 Циклические коды Боуза-Чоудхури-Хоквингема

Как следует из леммы 5.1.1 код  $\mathfrak{K}(x) \in \mathbb{F}_r[x]/x^n - 1$ , эквивалентный БЧХ-коду  $\mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)})$ , является идеалом  $I$  в кольце  $R_q^{(n)} = F_r[x]/\text{mod } x^n - 1$ . Для того, чтобы определить многочлен  $f(x) \in F_r[x]$ ,  $f(x)|x^n - 1$ , который порождает идеал  $I$ , воспользуемся следствием 5.1.1.

Очевидно,  $\mathbf{a} \in \mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)})$ , тогда и только тогда, когда  $\mathbf{a}(\theta^j) = 0$ ,  $j = 0, \dots, d-2$ . Поэтому  $f(x)$  — минимальный многочлен над полем  $\mathbb{F}_r$  элементов  $\theta^j \in \mathbb{F}_q$ ,  $j = 0, \dots, d-2$ , т.е.  $f(x) \in F_r[x]$  — многочлен минимальной степени такой, что  $f(\theta^j) = 0$ ,  $j = 0, \dots, d-2$ .

Если  $\theta^j$  — корень многочлена  $f(x)$ , то  $\theta^{jr}$  также корень  $f(x)$ , ибо  $f^r(x) = f(x^r)$ . Поэтому  $f(x)$  делится на минимальный над полем  $\mathbb{F}_r$  многочлен  $f_j(x)$  элемента  $\theta^j$ . Заметим, что  $f_j(x)$  является неприводимым многочленом.

Обозначим через  $S_d = \{\theta^{j_0}, \dots, \theta^{j_m}\}$  множество, состоящие из всех попарно несопряженных над полем  $\mathbb{F}_r$  элементов множества  $\{\theta^0, \dots, \theta^{d-2}\}$ .

**Лемма 5.2.4** *Порождающим многочленом  $r$ -значного БЧХ-кода  $\mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)})$  (БЧХ-кода над полем  $\mathbb{F}_r$ ) является многочлен*

$$f(x) = f_0(x) \cdots f_m(x), \quad (5.2.10)$$

где  $f_i(x)$  — минимальный над полем  $\mathbb{F}_r$  многочлен элемента  $\theta^{j_i}$ .

**Доказательство.** Очевидно,  $f(x)$  совпадает с минимальным многочлен над полем  $\mathbb{F}_r$  элементов  $\theta^j \in \mathbb{F}_q$ ,  $j = 0, \dots, d-2$ , т.е. является порождающим многочленом  $r$ -значного БЧХ-кода  $\mathfrak{K}(B_{\mathcal{A}_\theta}^{(d)})$ .  $\square$

Пусть  $r_i$  — минимальная степень расширения поля  $\mathbb{F}_r$ , к которому принадлежит элемент  $\theta^{j_i}$ . Очевидно,  $r_i = \deg f_i(x)$ . Следовательно,

$$\deg f(x) = r_0 + \cdots + r_m, \quad (5.2.11)$$

где  $r_i \leq l$ , если  $\theta^{j_i} \notin \mathbb{F}_r$  и  $r_i = 1$ , если  $\theta^{j_i} \in \mathbb{F}_r$ . Отсюда следует оценка

$$\deg f(x) \leq 1 + \left\lceil \frac{d-2}{r} \right\rceil l. \quad (5.2.12)$$

Из этой оценки вытекает оценка  $\dim BCH_{r,q}(n, d) = \deg \frac{x^n - 1}{f(x)} \geq n - 1 - \left\lceil \frac{d-2}{r} \right\rceil l$ . Последняя оценка является оценкой для размерности  $k'$  кода БЧХ-кода  $BCH_{r,q}(n, d)$  из теоремы 5.2.1, доказанная другим способом по сравнению с доказательством этой теоремы.

Свершенно аналогичным образом строится порождающий многочлен  $f(x)$  для БЧХ-кода  $\widehat{BCH}_{r,q}(n, d)$ . Для степени  $f(x)$  справедлива оценка  $\deg f(x) \leq \left\lceil \frac{d-1}{r} \right\rceil l$ .

## 5.2.5 Точное значение размерности БЧХ-кода при не слишком больших значениях $d$

Пусть  $r$  — примарное число (степень простого),  $q = r^l$  и  $h$ ,  $0 \leq h \leq q-1$ , — целое число. Будем обозначать через  $\lfloor v \rfloor$  неотрицательный вычет числа  $v$  по  $\text{mod } r^l - 1 = q-1$ .

Множество  $C_h = \{\lfloor vr^j \rfloor | j = 0, \dots, l-1\}$  мы называем циклотомическим классом, порожденным числом  $h$ . Наименьшее число в циклотомическом классе  $C_h$  обозначим через  $h_{\min}$ .

Обозначим через  $\bar{h} = (h_0, \dots, h_{l-1})$   $l$ -мерный вектор с координатами принадлежащими интервалу  $[0, r-1]$ , который представляет собой  $r$ -ичную запись числа  $h$ , т.е.  $h = h_0 + h_1r + \dots + h_{l-1}r^{l-1}$ .

Очевидно, вектор  $\overline{\lfloor vr \rfloor}$  представляет собой циклический сдвиг вектора  $\overline{\lfloor v \rfloor}$  на один разряд вправо, т.е.

$$\overline{\lfloor vr \rfloor} = \overline{\lfloor v \rfloor}^{(1)}. \quad (5.2.13)$$

**Лемма 5.2.5** Если  $0 < h < q^{\frac{1}{2}} = r^{\frac{l}{2}}$ , то  $|C_h| = l$ .

**Доказательство.** Как нетрудно увидеть, достаточно показать, что для любого  $j, 0 < j < l$  векторы  $h$  и  $hr^j$  являются различными по  $\text{mod } r^l - 1 = q - 1$ .

Рассмотрим множество векторов

$$\overline{C_h} = \{\bar{h}' | h' \in C_h\} = \{\bar{h}'^{(j)} | j = 0, \dots, l-1\}, \quad (5.2.14)$$

где  $\bar{h}'^{(j)}$  — циклический сдвиг вектора  $\bar{h}'$  на  $j$  разрядов вправо. Пусть  $\bar{h} = (h_0, \dots, h_{l-1}) \in \overline{C_h}$  и  $h_{j_0}$  — ненулевая координата вектора  $\bar{h}$  с наименьшим номером  $j_0$ . Без ограничения общности, полагаем, что  $j_0 = 0$ , т.е.  $h_0 \neq 0$ . Если это не так, то сдвинем вектор  $\bar{h}$  на  $l - j_0$  разрядов вправо. В результате получим вектор  $\bar{h}' = \bar{h}^{(l-j_0)}$ , который также принадлежит множеству  $\overline{C_h}$ . Для числа  $h' \in C_h$ , очевидно, выполнено  $h' \leq h < r^{\frac{l}{2}}$ . Так как,  $\overline{C_h} = \overline{C_{h'}}$ , то в качестве  $h$  можно взять вектор  $h'$ .

Заметим, что последние  $l - \frac{l}{2}$  координат вектора  $\bar{h}$  равны нулю.

Если  $j < \frac{l}{2}$ , то вектор  $\bar{h}^{(j)}$  отличен от вектора  $\bar{h}$  в виду того, что у второго координата с номером 0 равна нулю в то время как у первого она отлична от нуля.

Если же  $j \geq \frac{l}{2}$ , то вектор  $\bar{h}^{(j)}$  отличен от вектора  $\bar{h}$  в виду того, что у первого имеется координата с номером  $j \geq \frac{l}{2}$ , которая отлична от нуля в то время как у второго все координаты с номерами  $j \geq \frac{l}{2}$  равны нулю.  $\square$

**Следствие 5.2.1** Пусть  $\theta$  — некоторый первообразный корень поля  $\mathbb{F}_q$  и  $\tau = \theta^s$ ,  $s|q-1$ , — элемент поля  $\mathbb{F}_q$  порядка  $n = \frac{q-1}{s}$ .

Тогда

$$\deg f_j(x) = l \quad (5.2.15)$$

если  $0 < js < r^{\frac{l}{2}}$ , где  $f_j(x)$  — минимальный над полем  $\mathbb{F}_r$  многочлен элемента  $\tau^j$ .

**Доказательство.** Очевидно,  $\deg f_j(x) = |C_{sj}|$ . Их последней леммы следует доказываемое равенство (5.2.15).

**Теорема 5.2.3** Пусть  $\theta$  — некоторый первообразный элемент поля  $\mathbb{F}_q$  и  $\tau = \theta^s$ ,  $s|q-1$ , — элемент поля  $\mathbb{F}_q$  порядка  $\frac{q-1}{s}$ . Предположим, что  $(d-2)s < r^{\frac{l}{2}}$ , если мы рассматриваем код  $BCH_{r,q}(n, d)$ , и  $(d-1)s < r^{\frac{l}{2}}$ , если мы рассматриваем код  $\overline{BCH}_{r,q}(n, d)$ .

Тогда

$$\begin{aligned} \dim BCH_{r,q}(n, d) &= n - 1 - l \cdot \left( d - 2 - \left\lfloor \frac{d-2}{r} \right\rfloor \right) \\ \dim \widehat{BCH}_{r,q}(n, d) &= n - l \cdot \left( d - 1 - \left\lfloor \frac{d-1}{r} \right\rfloor \right). \end{aligned} \quad (5.2.16)$$

**Доказательство.** Сначала рассмотрим код  $BCH_{r,q}(n, d)$ . Из леммы 5.2.4, следствия 5.2.1 вместе с соотношением (5.2.11) вытекает соотношение

$$\deg f(x) = 1 + ml. \quad (5.2.17)$$

Таким образом, для доказательства теоремы в рассматриваемом случае достаточно показать, что  $m = d - 2 - \left\lfloor \frac{d-2}{r} \right\rfloor$ , где  $m$  — число попарно несопряженных элементов в множестве  $\{\tau, \tau^2, \dots, \tau^{d-2}\}$ .

Число  $\left\lfloor \frac{d-2}{r} \right\rfloor$  равно числу различных  $j$  в интервале  $[1, d-2]$ , которые кратны числу  $r$ . Если исключить из интервала  $[1, d-2]$  эти числа (числа кратные  $r$ ), то в оставшемся множестве чисел будет  $d - 2 - \left\lfloor \frac{d-2}{r} \right\rfloor$  элементов. Эти числа в виду леммы 5.2.4 входят в различные циклотомические классы  $C_j$ , каждый из которых содержит  $l$  элементов. Это доказывает, что  $m = d - 2 - \left\lfloor \frac{d-2}{r} \right\rfloor$  и, следовательно, доказывает первое равенство в (5.2.16).

Доказательство второго равенства в (5.2.16) почти не отличается от вывода первого равенства.  $\square$

Естественным расширением класса кодов Рида-Соломона являются, так называемые, обобщенные коды Рида-Соломона, которые также носят название альтернантных кодов. Следует сказать, что альтернантные коды используются при построении и анализе одной кодовой системы открытого шифрования, подробно рассматриваемой в главе 12. Переходим к их определению.

### 5.3 Обобщенные коды Рида-Соломона $RS_q(n, d)$ .

Рассмотрим матрицу

$$C_{\mathcal{A}}^{(d)} = \begin{pmatrix} z_1 \alpha_1^0 & z_2 \alpha_2^0 & \cdots & z_n \alpha_n^0 \\ z_1 \alpha_1 & z_2 \alpha_2 & \cdots & z_n \alpha_n \\ z_1 \alpha_1^2 & z_2 \alpha_2^2 & \cdots & z_n \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1 \alpha_1^{d-2} & z_2 \alpha_2^{d-2} & \cdots & z_n \alpha_n^{d-2} \end{pmatrix}, \quad d > 3, n \leq q+1, \quad (5.3.1)$$

где  $z_j \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ ,  $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_{q,\infty}$ ,  $\alpha_j \neq \alpha_i$  при  $j \neq i$  и при  $\alpha_j = \infty$  соответствующий столбец матрицы  $C_{\mathcal{A}}^{(d)}$  имеет вид  $(0, \dots, 0, z_j)^T$ .

Также как для обычного код Рида-Соломона, обобщенный код длины  $n \leq q+1$  имеет кодовое расстояние равное  $d$  и размерность  $n - d + 1$ . Это доказывается точно также как и для обычного кода. Обобщенный код Рида-Соломона будем обозначать также как и обычный код Рида-Соломона, т.е. символами  $RS_q(n, d)$ .

Матрица  $C_{\mathcal{A}}^{(d)}$ , очевидно, может быть представлена в виде  $C_{\mathcal{A}}^{(d)} = B_{\mathcal{A}}^{(d)} \cdot D$ , где  $D = \text{diag}(z_1, z_2, \dots, z_n)$ ,  $z_j \in \mathbb{F}_q \setminus \{0\}$ , — диагональная матрица и  $B_{\mathcal{A}}^{(d)}$  — проверочная матрица кода Рида-Соломона (см. (5.0.1)). Заметим, что матрица  $C_{\mathcal{A}}^{(d)}$  после некоторого преобразования далее будет выступать как проверочная матрица системы открытого шифрования. В этой связи значительный интерес представляет строение группы обобщенных автоморфизмов кода Рида-Соломона с проверочной матрицей  $B_{\mathcal{A}}^{(d)}$ , к изучению которой мы переходим.

### 5.3.1 Обобщенные БЧХ-коды

Обобщенный код  $BCH_r(n, d)$  определяется аналогично тому, как это было сделано в разделе 5.2:  $BCH_r(n, d) = RS_q(n, d) \cap \mathbb{F}_r^n$ , т.е. коду  $BCH_r(n, d)$  принадлежат все векторы кода  $RS_q(n, d)$ , координаты которых принадлежат подполю  $\mathbb{F}_r$  поля  $\mathbb{F}_q$ . Класс всех обобщенных БЧХ-кодов значительно шире класса просто БЧХ-кодов в виду того, что обобщенный БЧХ-код помимо упорядоченного множества  $\mathcal{A} \subseteq \mathbb{F}_{q,\infty}$  определяется вектором коэффициентов  $\mathbf{z} = (z_1, z_2, \dots, z_n) \in \mathbb{F}_q^{*n}$ , которые можно задавать произвольным образом. В связи с этим естественно ожидать, что в классе обобщенных БЧХ-кодов найдутся коды с лучшими параметрами, чем у просто БЧХ-кода. Эти ожидания оправданы. Далее мы, в качестве заслуживающих внимания примеров обобщенных БЧХ-кодов, построим один класс циклических кодов, и рассмотрим некоторые двоичные коды Гоппы. Эти коды не являются БЧХ-кодами.

В общем случае оценок размерности  $k'$  обобщенных БЧХ-кодов над полем  $\mathbb{F}_r$ , подобных приведенным в теоремах 5.2.1 и 5.2.2, не известно. Задача их вычисления даже для частных значений вектора  $\mathbf{z}$  часто является нетривиальной.

### 5.3.2 Циклический обобщенный БЧХ-код длины $n = q + 1$

Мы рассматриваем обобщенный циклический БЧХ-код длины  $q + 1$  над полем  $\mathbb{F}_q$ . Как следует из теоремы 5.1.6, код  $\mathfrak{K}(x)$ , эквивалентный линейному циклическому коду  $\mathfrak{K}$ , является подкольцом  $\langle f(x)R_q^{(q+1)} \rangle$  в кольце  $R_q^{(q+1)}$  многочленов по многочлену  $\text{mod } x^{q+1} - 1$ . Таким образом, чтобы построить "хороший" циклический код достаточно выбрать подходящий многочлен  $f(x)$ .

Пусть  $G$  — множество всех корней многочлена  $x^{q+1} - 1$ . Так как  $x^{q+1} - 1$  не имеет кратных корней, то  $|G| = q+1$ . Очевидно,  $G \subset \mathbb{F}_{q^2}$  и  $G$  — циклическая группа. Обозначим через  $\theta$  порождающий элемент группы  $G$ .

Как следует из леммы 5.1.1, для построения порождающего многочлена  $f(x)$  достаточно указать его корни, которые, как сказано выше, принадлежат полю  $\mathbb{F}_{q^2}$ , если они не равны  $\pm 1$ .

Заметим, что при  $t < \frac{q+1}{2}$  множество  $\Theta_t = \{\theta, \dots, \theta^t\}$  состоит из попарно не сопряженных над полем  $\mathbb{F}_q$  элементов из поля  $\mathbb{F}_{q^2}$ . Это происходит из-за того, что  $(\theta^j)^q = \theta^{-j} = \theta^{q+1-j}$ , т.е. элемент  $\theta^j$  сопряжен с элементом  $\theta^{q+1-j}$ , который при  $j \leq t < \frac{q+1}{2}$  не входит в множество  $\Theta_t$ .

Пусть  $f(x)$  — минимальный многочлен элементов из множества  $\Theta_t$ , т.е.

$$f(x) = f_1(x) \cdots f_t(x), \quad (5.3.2)$$

где  $f_j(x)$  — минимальный многочлен элемента  $\theta^j \in \mathbb{F}_{q^2}$  над полем  $\mathbb{F}_q$ . Очевидно,  $\deg f_j(x) = 2$ , поэтому степень многочлена  $f(x)$  равна  $2t$ .

**Теорема 5.3.1** Код  $\mathfrak{K}_f$  с порождающим многочленом  $f(x)$  имеет размерность  $q+1-2t$  и его кодовое расстояние  $d$  не меньше, чем  $2t+1$ .

**Доказательство.** Заметим, что корнями многочлена  $f(x)$  являются элементы  $\theta^1, \dots, \theta^t, \theta^{-1}, \dots, \theta^{-t}$ . Из теоремы 5.1.1 вытекает, что проверочная матрица кода  $\mathfrak{K}_f$  имеет вид



$$B_f = \begin{pmatrix} \theta^{1 \cdot 0} & \theta^{1 \cdot 1} & \theta^{1 \cdot 2} & \dots & \theta^{1 \cdot (n-1)} \\ \theta^{2 \cdot 0} & \theta^{2 \cdot 1} & \theta^{2 \cdot 2} & \dots & \theta^{2 \cdot (n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \theta^{t \cdot 0} & \theta^{t \cdot 1} & \theta^{t \cdot 2} & \dots & \theta^{t \cdot (n-1)} \\ \theta^{-1 \cdot 0} & \theta^{-1 \cdot 1} & \theta^{-1 \cdot 2} & \dots & \theta^{-1 \cdot (n-1)} \\ \theta^{-2 \cdot 0} & \theta^{-2 \cdot 1} & \theta^{-2 \cdot 2} & \dots & \theta^{-2 \cdot (n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \theta^{-t \cdot 0} & \theta^{-t \cdot 1} & \theta^{-t \cdot 2} & \dots & \theta^{-t \cdot (n-1)} \end{pmatrix}. \quad (5.3.3)$$

Докажем, что любые  $2t$  столбца матрицы  $B_f$  являются линейно-независимыми над полем  $\mathbb{F}_{q^2}$ .

Действительно, пусть

$$\Delta = \begin{vmatrix} \beta_1 & \beta_2 & \beta_3 & \dots & \beta_{2t} \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \dots & \beta_{2t}^2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \beta_1^t & \beta_2^t & \beta_3^t & \dots & \beta_{2t}^t \\ \beta_1^{-1} & \beta_2^{-1} & \beta_3^{-1} & \dots & \beta_{2t}^{-1} \\ \beta_1^{-2} & \beta_2^{-2} & \beta_3^{-2} & \dots & \beta_{2t}^{-2} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \beta_1^{-t} & \beta_2^{-t} & \beta_3^{-t} & \dots & \beta_{2t}^{-t} \end{vmatrix} \quad (5.3.4)$$

— определитель, образованный  $2t$  столбцами матрицы  $B_f$ .

Умножим  $j$ -ый столбец  $\Delta$  на элемент  $\beta_j^t$ . В результате получим определитель  $\Delta'$  Вандермонда, который отличен от нуля в силу того, что  $\beta_j, j = 1, \dots, 2t$  — различные ненулевые элементы поля  $\mathbb{F}_{q^2}$ . Так как  $\Delta' = \beta_1^t \dots \beta_{2t}^t \Delta$ , то  $\Delta \neq 0$ . Это доказывает линейную независимость любых  $2t$  столбцов матрицы  $B_f$  и, следовательно, оценку теоремы для кодового расстояния.

Утверждение теоремы о размерности кода  $\mathfrak{K}$  вытекает из того, что степень  $f(x)$  равна  $2t$ .  $\square$

Заметим, что если к множеству  $\Theta_t$  добавить еще один элемент, равный 1, то код  $\mathfrak{K}'$  с порождающим многочленом  $(x-1)f(x)$  имеет размерность на единицу меньшую, чем код  $\mathfrak{K}$ , а оценку кодового расстояния на единицу большую, чем код  $\mathfrak{K}$ .

Проверочная матрица (5.3.3) не является проверочной матрицей вида (5.0.1) или вида (5.1.5), т.е. не является проверочной матрицей БЧХ-кода. Вместе с тем, если умножить  $j$ -ый столбец  $B_f$  на элемент  $\theta_j^t$ , то полученная матрица уже будет проверочной матрицей БЧХ-кода, т.е. код  $\mathfrak{K}_f$  является обобщенным БЧХ-кодом.

### 5.3.3 Коды Гоппы

Содержание этого раздела в основном повторяет содержание соответствующего раздела книги [7].

$r$ -значные коды Гоппы имеют длину  $n = q, q = r^l$ . Они являются обобщенными БЧХ-коды типа 2. Интересно отметить, что определение кода Гоппы совсем не похоже на определение обобщенного БЧХ-кода. И только потом выяснится, что они могут быть

также представлены как коды с проверочной матрицей вида (5.3.1) с достаточно нетривиальным значением коэффициентов  $z_j$ .

### Определение кода Гоппы $\mathfrak{K}_G$ .

Свяжем с каждым вектором  $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_r^n$  рациональную функцию

$$R_{\mathbf{a}}(x) = \frac{a_1}{x - \alpha_1} + \dots + \frac{a_n}{x - \alpha_n}, \quad (5.3.5)$$

где  $\alpha_j \in \mathbb{F}_q$  и  $\alpha_i \neq \alpha_j$ , если  $i \neq j$ . И наоборот с каждой рациональной функцией, которая может быть представлена в виде (5.3.5), сопоставим вектор  $\mathbf{a}$ .

Пусть  $G(x)$  — многочлен степени  $m$  над полем  $\mathbb{F}_q$ , который не имеет корней в  $\mathbb{F}_q$ . Код Гоппы  $\mathfrak{G}_G$  состоит из всех векторов  $\mathbf{a}$ , для которых справедливо

$$R_{\mathbf{a}}(x) \equiv 0 \pmod{G(x)}. \quad (5.3.6)$$

### Кодовое расстояние кода Гоппы.

Сравнение (5.3.6) означает, что если мы запишем рациональную функцию  $R_{\mathbf{a}}(x)$  как

$$R_{\mathbf{a}}(x) = \frac{F_1(x)}{F_2(x)}, \quad (5.3.7)$$

где  $F_1(x), F_2(x)$  — взаимно простые многочлены, то  $F_1(x) \equiv 0 \pmod{G(x)}$ , т.е. многочлен  $F_1(x)$  делится на многочлен  $G(x)$ .

Отображение вектора  $\mathbf{a}$  в рациональную функцию  $R_{\mathbf{a}}(x)$  обладает тем свойством, что  $w(\mathbf{a}) = \deg F_2(x)$ . Это позволяет утверждать, что

$$d(\mathfrak{K}_G) = \min_{\mathbf{a} \in \mathfrak{K}_G, \mathbf{a} \neq 0} \deg F_2(x) \geq F_1(x) + 1. \quad (5.3.8)$$

Так как для ненулевого вектора  $\mathbf{a} \in \mathfrak{K}_G$   $G(x) | F_1(x)$ , то из оценки (5.3.8) вытекает, что

$$d(\mathfrak{G}_G) \geq \deg G(x) + 1 = m + 1. \quad (5.3.9)$$

### Проверочная матрица кода Гоппы.

Пусть  $\vartheta_1, \dots, \vartheta_u$  — попарно не сопряженные корни многочлена  $G(x)$ . Очевидно, соотношение (5.3.6) выполнено тогда и только тогда, когда  $R_{\mathbf{a}}(\vartheta_j) = 0$ ,  $j = 1, \dots, u$ . Отсюда непосредственно вытекает, что матриц

$$B(\mathfrak{K}_G) = \begin{pmatrix} \frac{1}{\vartheta_1 - \alpha_1} & \frac{1}{\vartheta_1 - \alpha_2} & \dots & \frac{1}{\vartheta_1 - \alpha_n} \\ \frac{1}{\vartheta_2 - \alpha_1} & \frac{1}{\vartheta_2 - \alpha_2} & \dots & \frac{1}{\vartheta_2 - \alpha_n} \\ \vdots & \vdots & \dots & \vdots \\ \frac{1}{\vartheta_u - \alpha_1} & \frac{1}{\vartheta_u - \alpha_2} & \dots & \frac{1}{\vartheta_u - \alpha_n} \end{pmatrix} \quad (5.3.10)$$

является проверочной матрицей кода  $\mathfrak{K}_G$ .

## Размерность кода Гоппы над полем $\mathbb{F}_r$ .

Матрицу  $B(\mathfrak{K}_G)$  мы запишем как матрицу с элементами из поля  $\mathbb{F}_q$  с помощью следующего стандартного приема.

Пусть  $\mathbb{F}_{q^{m_i}}$  — наименьшее расширение поля  $\mathbb{F}_q$ , к которому принадлежит корень  $\vartheta_j$  многочлена  $G(x) \in \mathbb{F}_q[x]$ . Очевидно,  $m_1 + \dots + m_u = m$ . Представим элемент  $\frac{1}{\vartheta_i - \alpha_j} \in \mathbb{F}_{q^{m_i}}$  как вектор-столбец высоты  $m_i$ , который представляет этот элемент в некотором базисе поля  $\mathbb{F}_{m_i}$  над полем  $\mathbb{F}_q$ . В результате мы получим матрицу  $B'(\mathfrak{K}_G)$  с элементами из поля  $\mathbb{F}_q$  с  $m$  строками.

Точно также с помощью того же приема из матрицы  $B'(\mathfrak{G}_G)$  мы получим матрицу  $B''(\mathfrak{G}_G)$  с элементами из поля  $\mathbb{F}_r$ , которая имеет  $l \cdot m$  строк. Отсюда вытекает, что для размерности  $k$  кода справедлива оценка

$$k = n - \text{число линейно-независимых строк } B''(\mathfrak{G}_G) \geq n - l \cdot m. \quad (5.3.11)$$

## Код Гоппы как обобщенный БЧХ-код

Наша задача — выписать проверочную матрицу  $B(\mathfrak{K}_G)$  кода Гоппы  $\mathfrak{K}_G \subset \mathbb{F}_r^n$  в виде матрицы вида

$$B(\mathfrak{K}_G) = H \cdot C_{\mathcal{A}}^{(m-1)}, \quad \mathcal{A} = \mathbb{F}_q \quad (5.3.12)$$

над полем  $\mathbb{F}_q$ , где матрица  $C_{\mathcal{A}}^{(d)}$  определена соотношением (5.3.1) и  $H$  невырожденная матрица.

Так как элемент  $\alpha_j$  не является корнем многочлена  $G(x)$ , то в кольце вычетов по  $\text{mod } G(x)$  многочлен  $x - \alpha_j$  имеет обратный, т.е. существует многочлен  $f_j(x)$  степени не выше  $m - 1$  такой, что  $(x - \alpha_j)f_j(x) \equiv 1 \pmod{G(x)}$  или  $(x - \alpha_j)f_j(x) \equiv \frac{1}{x - \alpha_j} \pmod{G(x)}$ . Нетрудно вычислить многочлен  $f_j(x)$  в явном виде:

$$f_j(x) \equiv \frac{1}{x - \alpha_j} \equiv A_j \frac{G(x) - G(\alpha_j)}{x - \alpha_j} \pmod{G(x)}, \quad (5.3.13)$$

где коэффициент  $A_j$ , как легко установить, равен  $A_j = -G^{-1}(\alpha_j)$ .

Пусть  $G(x) = \sum_i 0^m g_i x^i$ . Так как  $\frac{x^i - \alpha_j^i}{x - \alpha_j} = x^{i-1} + x^{i-2}\alpha_j + \dots + x\alpha_j^{i-2} + \alpha_j^{i-1}$ , то

$$\text{коэфф}_{x^{i-1}} f_j(x) = g_i + g_{i+1}\alpha_j + \dots + g_m \alpha_j^{m-i}. \quad (5.3.14)$$

Вектор  $\mathbf{a}$  принадлежит коду  $\mathfrak{K}_G$  тогда и только тогда, когда  $F(x) = a_1 f_1(x) + \dots + a_n f_n(x) \equiv 0 \pmod{G(x)}$ . Так как степень многочлена  $F(x)$  меньше  $m$ , то вектор  $\mathbf{a}$  принадлежит коду  $\mathfrak{K}_G$  тогда и только тогда, когда все коэффициенты  $F(x)$  равны нулю, т.е. с учетом (7.0.3) и (5.3.13) когда

$$\sum_{j=1}^n a_j G^{-1}(\alpha_j) (g_i + g_{i+1}\alpha_j + \dots + g_m \alpha_j^{m-i}) = 0, \quad i = 0, \dots, m-1. \quad (5.3.15)$$

Соотношение (5.3.15), очевидно, можно записать в виде

$$H \cdot B_{\mathcal{A}}^{(m-1)} \cdot D \mathbf{a}^T = 0, \quad (5.3.16)$$

где ниже диагональная невырожденная матрица, которую в явном виде мы выписывать не будем, матрица  $B_A^{(m-1)}$  определена в (5.0.1) и  $D = \text{diag}(G^{-1}(\alpha_1), \dots, G^{-1}(\alpha_n))$ . Это показывает, что  $H \cdot B_A^{(m-1)} \cdot D$  — проверочная матрица кода  $\mathfrak{K}_G$ , которую можно представить в виде (5.3.12).

Упражнение: выписать в явном виде матрицу  $H$  и установить, что она невырождена.

### Двоичные коды Гоппы.

Заметим, что для кодового расстояния кода Гоппы в общем случае известна только оценка  $d \geq \deg G(x) + 1$ . Она повторяет соответствующую оценку для альтернантного кода с той же оценкой размерности. Вместе с тем в двоичном случае можно получить оценку снизу кодового расстояния кода  $\mathfrak{K}_G$ , лучшую, чем приведенная выше оценка.

**Теорема 5.3.2** *Для кодового расстояния  $d(\mathfrak{K}_G)$  двоичного кода Гоппы  $\mathfrak{K}_G$  справедлива оценка*

$$d(\mathfrak{K}_G) \geq 2m + 1, \quad (5.3.17)$$

где  $m = \deg G(x)$ .

**Доказательство.** В двоичном случае (и только в этом случае) в представлении рациональной функции  $R_a$  в виде (5.3.7) знаменатель является производной числителя, т.е.

$$R_a(x) = \frac{F'(x)}{F(x)}. \quad (5.3.18)$$

Это легко проверить. Упражнение.

В поле характеристики 2 в многочлен, который является производной другого многочлена, входят с ненулевыми коэффициентами только мономы, у которых степень является четным числом. Поэтому производную  $F'(x)$  можно записать в виде  $F'(x) = \widehat{F}^2(x)$  с некоторым многочленом  $\widehat{F}(x)$ .

Ненулевой вектор  $a$  принадлежит коду  $\mathfrak{K}_G$  тогда и только тогда, когда  $F'(x) = \widehat{F}^2(x) \equiv 0 \pmod{G(x)}$ . Поэтому  $\deg F'(x) \geq 2m$  и, следовательно,  $w(a) = \deg F(x) \geq 2m + 1$ .  $\square$

Как показывает несложный анализ, двоичный код  $\mathfrak{K}_G$  имеет те же оценки для параметров, что и двоичный БЧХ-код с проверочной матрицей  $B_A^{(d)}$ ,  $A = \mathbb{F}_q$ , (см. (5.1.5)), где  $d = 2m$ . Вместе с тем максимальная длина кода двоичного Гоппы на единицу больше, чем максимальная длина БЧХ-кода с той же оценкой для размерности.

## 5.4 Автоморфизмы кода

Многие коды обладают замечательными свойствами, связанными с наличием у них той или иной симметрии. Цикличность кода является простейшим примером таких симметрий. Одним из естественных свойств симметрии кода  $\mathfrak{K} \subseteq \mathbb{F}_q$  является сохранение некоторых функций, определенных на этом коде. Самой естественной и важной из таких функций является расстояние  $d(a, b)$  между различными элементами  $a, b \in \mathfrak{K}$ .

**Определение 5.4.1** Симметрией  $\varphi$  кода  $\mathfrak{K}$  называется взаимно однозначное отображение

$$\varphi : \mathfrak{K} \rightarrow \mathfrak{K}, \quad (5.4.1)$$

кода в себя, сохраняющее метрику Хемминга  $d(\mathbf{a}, \mathbf{b})$ , т.е.  $\varphi$  — отображение, для которого справедливо

$$d(\mathbf{a}, \mathbf{b}) = d(\varphi(\mathbf{a}), \varphi(\mathbf{b})) \text{ для всех пар } \mathbf{a}, \mathbf{b} \in \mathfrak{K}. \quad (5.4.2)$$

Заметим, что некоторых случаях кроме сохранения кодового расстояния симметрия  $\varphi$  дополнительно может быть линейной функцией, т.е. для нее выполняется

$$\varphi(\mathbf{a}) + \varphi(\mathbf{b}) = \varphi(\mathbf{a} + \mathbf{b}) \text{ для всех } \mathbf{a}, \mathbf{b} \in \mathfrak{K}. \quad (5.4.3)$$

В этом случае симметрия называется линейной.

Если  $\varphi, \varphi'$  — две симметрии кода  $\mathfrak{K}$ , то произведение этих симметрий  $\varphi \cdot \varphi'$  (последовательное применение одной, а затем другой) также является симметрией кода  $\mathfrak{K}$ . Поэтому все симметрии кода  $\mathfrak{K}$  образуют группу  $\Sigma_{\mathfrak{K}}$ , в которой групповой операцией является суперпозиция отображений.

Следует сказать, что о строении группы  $\Sigma_{\mathfrak{K}}$  для почти всех нетривиальных кодов  $\mathfrak{K}$  известно очень мало.

Мы далее будем изучать только линейные симметрии кодов.

Не надо думать, что во всех случаях симметрии являются линейными. Существуют коды, например код Хемминга, для которого существуют симметрии, не являющимися линейными функциями на  $\mathfrak{K}$ .

### 5.4.1 Группа автоморфизмов кода

Если переставить координаты кодового вектора  $\mathbf{a}$  некоторого кода  $\mathfrak{K}$ , то полученный вектор  $\mathbf{a}'$  может как принадлежать так и не принадлежать коду  $\mathfrak{K}$ .

**Определение 5.4.2** Перестановка  $\delta$  координат векторов пространства  $\mathbb{F}_q^n$  называется автоморфизмом кода  $\mathfrak{K}$ , если

$$\delta(\mathbf{a}) \in \mathfrak{K} \text{ для всех } \mathbf{a} \in \mathfrak{K}. \quad (5.4.4)$$

Аutomорфизм кода, очевидно, является линейной симметрией.

Заметим, что на множестве перестановок координат векторов пространства  $\mathbb{F}_q^n$  можно естественным и очевидным образом определить операцию умножения  $\cdot$ , по отношению к которой это множество перестановок становится группой  $S_n$  порядка  $n!$ . Эта некоммутативная (при  $n > 2$ ) группа носит название симметрической группы.

Очевидно, что если  $\delta'$  — другой автоморфизм кода  $\mathfrak{K}$ , то произведение перестановок  $\delta \cdot \delta'$  также является автоморфизмом этого кода. Поэтому все автоморфизмы кода  $\mathfrak{K}$  образуют группу  $\Delta_{\mathfrak{K}}$ . Эта группа называется группой автоморфизмов кода  $\mathfrak{K}$ .

Перестановку координат  $\delta$  удобно представлять себе в виде перестановочной матрицы  $\Gamma_{\delta} = \Gamma = \|\gamma_{i,j}\|$ , которая реализует эту перестановку в виде умножения вектора на матрицу. А именно, элемент  $\gamma_{i,j}$  матрицы  $\Gamma_{\delta}$  равен 1 тогда и только тогда, когда координата с номером  $i$  переходит посредством действия  $\delta$  в координату с номером  $j$ . Во всех

остальных случаях  $\gamma_{i,j} = 0$ . Таким образом, матрица  $\Gamma$  представляет из себя матрицу, у которой в любой строке и в любом столбце имеется ровно одна 1.

Перестановочная матрица  $\Gamma$  реализует перестановку  $\delta$  координат вектора  $\mathbf{a} \in \mathbb{F}_q^n$  в виде матричного умножения следующим образом:

$$\delta(\mathbf{a}) = \mathbf{a}\Gamma. \quad (5.4.5)$$

Матричная группа автоморфизмов  $G = G_{\mathfrak{K}}$  образована всеми матрицами  $\Gamma_\delta$ , у которых  $\delta \in \Sigma_{\mathfrak{K}}$ .

Отметим, что автоморфизмы кода  $\mathfrak{K}$ , очевидно, сохраняют расстояние Хемминга между парами векторов не только кода  $\mathfrak{K}$ , но и всего пространства  $\mathbb{F}_q^n$ , т.е. автоморфизмы являются симметриями. Более того, они являются линейными симметриями.

Как следует из определения, если  $\mathfrak{K}$  — циклический код, то подстановка

$$\delta^{(1)} = \begin{pmatrix} 1, 2, \dots, n-1, n \\ 2, 3, \dots, n, 1 \end{pmatrix} \quad (5.4.6)$$

(циклический сдвиг координат вектора  $\mathbf{a} \in \mathbb{F}_q^n$  на один разряд вправо)

является автоморфизмом, принадлежащим группе  $\Sigma_{\mathfrak{K}}$ . Порядок циклической группы  $\langle \delta^{(1)} \rangle$  (группы, порожденной подстановкой  $\delta^{(1)}$ ) равен  $n$ . Поэтому группа автоморфизмов циклического кода содержит в качестве подгруппы циклическую группу. Верно и обратное: если  $\Sigma_{\mathfrak{K}}$  содержит циклическую подгруппу порядка  $n$ , то код после некоторой перестановки его координат становится циклическим. (Упражнение)

Пусть  $\Gamma \in G_{\mathfrak{K}}$  и  $B$  ( $A$ ) — проверочная (соответственно порождающая) матрица кода  $\mathfrak{K}$ . Тогда  $B' = B \cdot \Gamma$  ( $A' = A \cdot \Gamma$ ), очевидно, также является проверочной (соответственно порождающей) матрицей кода  $\mathfrak{K}$ .

Строки матрицы  $B$  являются базисом некоторого пространства  $L_{\mathfrak{K}}$ , натянутого на строки матрицы  $B$ . Это пространство, очевидно, совпадает с кодом  $\mathfrak{K}^\perp$ , двойственным к коду  $\mathfrak{K}$ . Пусть  $B'$  — другой базис  $L_{\mathfrak{K}}$ . Обозначим через  $h_{n-k} = h$   $n-k \times n-k$  — матрицу перехода от базиса  $B$  к базису  $B'$ :  $B' = h \cdot B$ . Совершенно также определяется  $k \times k$  — матрица перехода  $h$  для матрицы  $A$ :  $A' = h \cdot A$ . Таким образом,  $C' = h \cdot C$ , где через  $C$  мы обозначаем одну из матриц  $A$  или  $B$ . Это утверждение удобно представить в виде

**Лемма 5.4.1** *Перестановочная матрица  $\Gamma$  является элементом группы матричных автоморфизмов кода  $\mathfrak{K}$ , если существует невырожденная матрица  $h \in M_{n-k}(\mathbb{F}_q)$  (если  $C = B$ ) и  $h \in M_k(\mathbb{F}_q)$  (если  $C = A$ ) такая, что*

$$C \cdot \Gamma = h \cdot C. \quad (5.4.7)$$

Интересно отметить, что отображение  $\Gamma \rightarrow h$ , определяемое соотношением (5.4.7), реализует гомоморфизм матричной группы  $G_{\mathfrak{K}}$  автоморфизмов кода  $\mathfrak{K}$  (матрицы размера  $n \times n$ ) в матричную группу, образованную матрицами  $h$  размера  $n-k \times n-k$  ( $C = B$ ) или  $k \times k$  ( $C = A$ ).

Ядро  $J(\mathfrak{K})$  этого гомоморфизма образуют элементы  $\Gamma$ , которые оставляют на месте все векторы кода  $\mathfrak{K}$ . Поэтому матрицы  $h$ , на которые отображается группа  $G_{\mathfrak{K}}$  посредством соответствия  $B \cdot \Gamma = h \cdot B$ , изоморфна факторгруппе  $G_{\mathfrak{K}}/J(\mathfrak{K})$ . Так как далее мы ограничимся рассмотрением только кодов, у которых ядро  $J(\mathfrak{K})$  тривиально (состоит из одного единичного элемента), то мы всегда будем полагать, группа образованная

матрицами  $h$ , изоморфна группе  $G_{\mathfrak{R}}$ . К кодам, у которых ядро тривиально, относятся коды  $RS_q(n, d)$ . Доказательство этого утверждения в более общей форме см. ниже (Лемма 5.4.2).

### 5.4.2 Подгруппы группы автоморфизмов кодов Рида-Соломона $RS_q(n, d)$

Как и прежде, мы нумеруем координаты векторов кода  $RS_q(n, d)$  элементами одного из подмножеств множества  $\mathbb{F}_{q,\infty} = \mathbb{F}_q \cup \{\infty\}$ . Так код  $RS_q(n, d)$  типа 1 нумеруется элементами множества  $\mathbb{F}_{q,\infty} \setminus \{0, \infty\}$ , код типа 2 — элементами множества  $\mathbb{F}_{q,\infty} \setminus \{0\}$  и код типа 3 — элементами множества  $\mathbb{F}_{q,\infty}$ . Следовательно, любую перестановку координат кода  $RS_q(n, d)$  можно рассматривать как взаимно-однозначным отображением одного из указанных подмножеств множества  $\mathbb{F}_{q,\infty}$  в себя.

#### Лемма 5.4.2

- i. Подгруппой группы автоморфизмов кода  $\mathfrak{R}(B_{\mathcal{A}_0}^{(d)})$  (который при  $n = q - 1$  является кодом  $RS_q(n, d)$  типа 1) является циклическая группа порядка  $n$ , порожденная отображением

$$x \rightarrow \theta x. \quad (5.4.8)$$

- ii. Подгруппой группы автоморфизмов кода  $RS_q(n, d)$  типа 2 является метаабелева группа порядка  $(q - 1)q$ , образованная всеми аффинными отображениями

$$x \rightarrow ax + b, \quad a \in \mathbb{F}_q \setminus \{0\}, b \in \mathbb{F}_q \quad (5.4.9)$$

поля  $\mathbb{F}_q$  в себя.

Если поле  $\mathbb{F}_q$  — простое, т.е.  $q$  — простое число  $p$ , и множество  $\mathcal{A}$  имеет вид  $\mathcal{A}_0 = \{0, 1, \dots, p - 1\}$ , то код  $RS_q(n, d)$  с порождающей матрицей  $B_{\mathcal{A}_0}^{(d)}$  является циклическим.

#### Доказательство.

- i. Утверждение этого пункта является очевидным.
- ii.  $j$ -ая строка  $B_j^{(d)}$  матрицы  $B_{\mathcal{A}}^{(d)}$  представляет собой вектор значений многочлена  $x^j$  во всех точках множества  $\mathcal{A}$ . В данном случае множество  $\mathcal{A}$  совпадает с полем  $\mathbb{F}_q$ . Очевидно, отображение  $\delta : x \rightarrow ax + b$  переводит строку  $B_j^{(d)}$  в строку значений многочлена  $(ax + b)^j$ . Эту строку, очевидно, можно представить как линейную комбинацию строк  $B_s^{(d)}$ ,  $s = 0, \dots, j$ . Поэтому для перестановочной матрицы  $\Gamma_\delta$  справедливо равенство (5.4.7) в лемме 5.4.1. При этом матрица  $h$  в (5.4.7) является верхней треугольной матрицей.

Если  $\mathbb{F}_q$  — простое поле и множество  $\mathcal{A}$  упорядочено указанным в условии теоремы способом, то перестановка координат  $\delta^{(1)}$ , соответствующая отображению  $x \rightarrow x + 1$ , с одной стороны, циклически сдвигает координаты  $j$ -ой строки  $B_j^{(d)}$  матрицы  $B_{\mathcal{A}_0}^{(d)}$  на один разряд вправо. С другой стороны, многочлен  $(x + 1)^j$  линейно выражается через многочлены  $x^s$ ,  $0 \leq s \leq j$ . Поэтому циклически сдвинутая строка  $B_j^{(d)}$  линейно выражается через строки  $B_s^{(d)}$ ,  $0 \leq s \leq j$ , т.е. для матрицы  $B_{\mathcal{A}_0}^{(d)}$  справедлива лемма 5.4.1.  $\square$

Заметим, что в п.ii теоремы мы упорядочивали элементы множества  $\mathcal{A}$  с помощью аддитивной группы поля  $\mathbb{F}_q$ , которая только при  $q = p$  является циклической группой. В тоже же время в п.i теоремы мы упорядочивали элементы множества  $\mathcal{A}$  с помощью мультипликативной группы поля  $\mathbb{F}_q$ , которая всегда является циклической группой.

## 5.5 Группа обобщенных автоморфизмов кода

Если в качестве обычных автоморфизмов кода  $\mathfrak{K}$  выступали перестановки координат, реализуемые перестановочными матрицами  $\Gamma$ , то в качестве обобщенных автоморфизмов выступают перестановки вместе с умножением переставляемых координат на ненулевые элементы поля  $\mathbb{F}_q$ . А именно, мы рассматриваем линейные преобразования пространства  $\mathbb{F}_q^n$ , реализуемые невырожденными матрицами вида  $\Lambda = \Gamma \cdot D$ , где  $\Gamma$  — перестановочная матрица и  $D$  — диагональная матрица. Матрицы вида  $\Lambda$  носят название мономиальных. Другими словами,  $\Lambda$  — перестановочная матрица, у которых ненулевыми элементами являются ненулевые элементы поля  $\mathbb{F}_q$ .

Также, как перестановочные матрицы, мономиальные матрицы, очевидно, сохраняют расстояние Хемминга в пространстве  $\mathbb{F}_q^n$ . А именно,  $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a}\Lambda, \mathbf{b}\Lambda)$ . Более того, любая мономиальная матрица реализует линейную симметрию пространства  $\mathbb{F}_q^n$ .

Произведение  $\Lambda \cdot \Lambda'$  мономиальных матриц  $\Lambda$  и  $\Lambda'$  является мономиальной матрицей. Отсюда вытекает, что множество всех мономиальных матриц является конечной группой  $M_n$ . Порядок  $M_n$ , как нетрудно увидеть, равен  $n!(q-1)^n$ .

Теперь переформулируем для обобщенных автоморфизмов некоторые из определений раздела 5.4.1.

Если мономиальная матрица  $\Lambda$  такова, что  $\mathbf{a}\Lambda \in \mathfrak{K}$  для всех  $\mathbf{a} \in \mathfrak{K}$ , то она называется обобщенным автоморфизмом кода  $\mathfrak{K}$ . Очевидно, что если  $\Lambda'$  — другой автоморфизм, то произведение  $\Lambda \cdot \Lambda'$  также является обобщенным автоморфизмом. Поэтому все обобщенные автоморфизмы кода  $\mathfrak{K}$  образуют группу  $\Xi_{\mathfrak{K}}$ , которая называется *группой обобщенных автоморфизмов кода  $\mathfrak{K}$* . Элементами группы  $\Xi_{\mathfrak{K}}$  являются мономиальные матрицы размера  $n \times n$ .

Также как в разделе 5.4.1 (представление группы автоморфизмов  $\Delta_{\mathfrak{K}}$ ) можно рассмотреть представление группы обобщенных автоморфизмов  $\Xi_{\mathfrak{K}}$  для линейного кода  $\mathfrak{K}$  в виде невырожденных матриц над  $\mathbb{F}_q$  размера  $k \times k$  или  $n-k \times n-k$ . А именно, элементу  $\Lambda$  из  $\Xi_{\mathfrak{K}}$  сопоставим матрицу  $h = h_{\Lambda}$ , которая определяется соотношением

$$C \cdot \Lambda = h_{\Lambda} \cdot C, \quad (5.5.1)$$

где  $C$  — одна из матриц порождающая или проверочная линейного кода  $\mathfrak{K}$ .

Произведению  $\Lambda \cdot \Lambda'$  двух элементов из  $\Xi_{\mathfrak{K}}$  соответствует произведение  $g(\Lambda \cdot \Lambda') = h_{\Lambda'} \cdot h_{\Lambda}$  двух элементов из  $H_{\mathfrak{K}}$ . Поэтому множество всех матриц  $h_{\Lambda}$  является конечной группой. Заметим, что порядок следования сомножителей в  $H_{\mathfrak{K}}$  обратный по сравнению с  $\Xi_{\mathfrak{K}}$ .

Таким образом рассматриваемое отображение  $g : \Lambda \rightarrow h_{\Lambda}$  является антигомоморфизмом группы  $\Xi_{\mathfrak{K}}$  в группу матриц размера  $k \times k$  или  $n-k \times n-k$  над полем  $\mathbb{F}_q$ .

**Лемма 5.5.1** *При  $d > 3$  для кода  $\mathfrak{K} = RS_q(n, d)$  антигомоморфизм  $g$  является антиизоморфизмом, т.е.  $|\Xi_{\mathfrak{K}}| = |H_{\mathfrak{K}}|$ .*



**Доказательство.** Нам надо доказать, что ядро гомоморфизма  $g$  тривиально. Это следует из-за того, что матрица  $B$  не содержит пропорциональных столбцов и поэтому  $B \neq B \cdot \Lambda$  для любой неединичной мономимальной матрицы  $\Lambda$ . Поэтому среди неединичных мономимальных матриц  $\Lambda$  не существует такой, что  $\mathbf{a} = \mathbf{a}\Lambda$  для всех  $\mathbf{a} \in RS_q(n, d)$ , т.е.  $g$  — антиизоморфизм.  $\square$

**Теорема 5.5.1** *Подгруппой группы обобщенных автоморфизмов кода  $RS_q(n, d)$  типа 3 является группа  $\Phi_q$  порядка  $(q^2 - 1)q$ , образованная дробно-линейными отображениями (см. раздел 5.5.1) множества  $\mathbb{F}_q \cup \{\infty\}$  в себя.*

**Доказательство.** Пусть  $\varphi(x) = \frac{ax+b}{cx+e}$  дробно-линейная функция,  $\mathcal{A} = \{\alpha_0, \dots, \alpha_q\} = \mathbb{F}_{q,\infty} = \mathbb{F}_q \cup \{\infty\}$ ,  $D_\varphi = \text{diag}((c\alpha_0 + e)^{d-2}, \dots, (c\alpha_q + e)^{d-2})$  — диагональная матрица и  $\Gamma_\varphi$  — подстановочная матрица, реализующая подстановку  $\sigma : x \rightarrow \varphi(x)$ . Отметим, что  $(c\alpha_i + e)^{d-2} = \text{коэфф}_{x^{d-2}}(cx + e)^{d-2}$ , если  $\alpha_i = \infty$ .

Мы докажем, что матрица  $\Lambda_\varphi = \Gamma_\varphi \cdot D_\varphi$  является обобщенным автоморфизмом кода  $RS_q(n, d)$  типа 3.

$j$ -ая строка матрицы  $B_{\mathcal{A}}^{(d)}$  (определение см. в разделе (1.2.9)) представляет собой значения функции  $x^j$  на элементах множества  $\mathcal{A} = \mathbb{F}_{q,\infty}$ . Очевидно, мономимальная матрица  $\Lambda_\varphi$  преобразуют эту строку в строку значений функции  $(ax + b)^j(cx + e)^{d-2-j}$ .

Многочлен  $(ax + b)^j(cx + e)^{d-2-j}$  степени не выше  $d-2$ , очевидно, линейно выражается через многочлены  $1, x, \dots, x^{d-2}$ , т.е. каждая строка матрицы  $B_{\mathcal{A}}^{(d)}\Lambda_\varphi$  линейно выражается через строки матрицы  $B_{\mathcal{A}}^{(d)}$ . Отсюда следует утверждение теоремы.  $\square$

Этот результат будет использован при анализе стойкости системы открытого шифрования, построенной с помощью кода Рида-Соломона (см. §4).

Следует сказать несколько слов о строении и свойствах группы дробно-линейных преобразований, которые интересны сами по себе и поносятся в разделе ?.

### 5.5.1 Группа дробно-линейных преобразований.

Элементами группы дробно-линейных преобразований  $\Phi_q$  множества  $\mathbb{F}_{q,\infty}$  в себя являются дробно-линейные функции  $\phi(x) = \frac{ax+b}{cx+e}$ , отличные от постоянной. Очевидно, каждое дробно-линейное преобразование  $\phi(x)$  взаимно однозначно отображает множество  $\mathbb{F}_{q,\infty}$  в себя. (Упражнение 1.)

Множество  $\Phi_q$  действительно является некоммутативной группой. "Умножением"  $\circ$  в ней служит суперпозиция функций, т.е.  $\phi \circ \phi' = \phi(\phi'(x))$ .

Группа  $\Phi_q = PGL(2, q)$  имеет порядок  $(q+1)q(q-1)$  (Упражнение 2.).

Очень интересным и существенным свойством группы  $\Phi_q$ , является то, что она — трижды транзитивная группа. Это означает, что для любых двух пар троек  $(a_1, a_2, a_3)$  и  $(b_1, b_2, b_3)$ ,  $a_i, b_i \in \mathbb{F}'_q$ , с попарно различными координатами в группе  $\Phi_q$  найдется элемент  $\phi$  (всегда один), для которого выполнено  $\phi(a_i) = b_i, i = 1, 2, 3$ . Доказательство этих свойств несложно и предоставляется читателю (см. упражнения 3, а также

[23] и [3], стр. 344-345).

Группа  $\Xi_{\mathcal{A}}$  обобщенных автоморфизмов кода Рида-Соломона также является трижды транзитивной в следующем смысле. Для любой пары упорядоченных троек из попарно различных элементов  $(\beta_1, \beta_2, \beta_3)$  и  $(\gamma_1, \gamma_2, \gamma_3)$ , где  $(\beta_1, \beta_2, \beta_3), (\gamma_1, \gamma_2, \gamma_3) \in \mathcal{A} =$

$\{\alpha_0, \alpha_2, \dots, \alpha_q\} = \mathbb{F}'_q$  существует такая мономиальная матрица  $\Lambda_\phi \in \Xi_{\mathfrak{K}}$ , которая переводит координаты  $x_{\beta_1}, x_{\beta_2}, x_{\beta_3}$  вектора  $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$  в координаты  $x_{\gamma_1}, x_{\gamma_2}, x_{\gamma_3}$  вектора  $\mathbf{x}\Lambda_\phi$  с умножением их на соответствующие постоянные, определяемые диагональной матрицей  $D_\phi = \text{diag}(d_{\alpha_1}, d_{\alpha_2}, \dots, d_{\alpha_n}) = ((c\alpha_0 + e)^{d-2}, \dots, (c\alpha_q + e)^{d-2})$ .

Чтобы построить такую матрицу  $\Lambda_\phi$  достаточно в качестве функции  $\phi$  взять функцию, переводящую тройку  $(\beta_1, \beta_2, \beta_3)$  в тройку  $(\gamma_1, \gamma_2, \gamma_3)$ .

Например, с помощью подходящей матрицы  $\Lambda_\phi$  можно передвинуть на первые три места координаты вектора  $\mathbf{x}$  с номерами  $(\beta_1, \beta_2, \beta_3)$ . В частности, пусть  $\beta_1 = 1, \beta_2 = 0, \beta_3 = \infty$  и  $\gamma_1 = \alpha_1, \gamma_2 = \alpha_2, \gamma_3 = \alpha_3$ , тогда  $\mathbf{x}\Lambda_\phi = (d_{\alpha_1}x_1, d_{\alpha_2}x_0, d_{\alpha_3}x_\infty, d_{\alpha_4}x_{\phi(\alpha_4)}, \dots, d_{\alpha_n}x_{\phi(\alpha_n)})$  для некоторой подходящей функции  $\phi(x)$ .

## 5.6 Число обобщенных кодов Рида-Соломона

### 5.6.1 Число проверочных матриц кода $RS_q(n, d)$

Если  $h$  — невырожденная матрица размера  $d - 1 \times d - 1$ , то, как нетрудно видеть, проверочные матрицы  $B$  и  $hB$  определяют один и тот же код  $RS_q(n, d)$ . В качестве задачи для самостоятельного доказательства приведем следующее утверждение. *Матрицы  $B$  и  $hB$  различны, если  $h \neq E$  (единичная матрица).* Отсюда следует, что число различных проверочных матриц, которые определяют один и тот же код  $RS_q(n, d)$ , равно  $N_{q,d-1}$ , где  $N_{q,s}$  — число невырожденных квадратных матриц  $h$  размера  $s \times s$ .

**Лемма 1.** *Число  $N_{q,s}$  равно*

$$N_{q,s} = (q^s - 1)(q^s - q) \cdots (q^s - q^{s-1}). \quad (5.6.1)$$

**Доказательство.** Первую строку невырожденной матрицы  $h$  над полем  $\mathbb{F}_q$  размера  $s \times s$  можно выбрать  $q^s - 1$  способами — все векторы длины  $s$ , исключая нулевой. Вторую строку —  $q^s - q$  способами — все векторы, которые не пропорциональны первой строке. Третью строку —  $q^s - q^2$  способами — все векторы, которые не входят в подпространство размерности 2 пространства  $\mathbb{F}_q^s$ , натянутое на первые две строки. И так далее. Наконец, последнюю строку  $h$  можно выбрать  $q^s - q^{s-1}$  способами — все векторы, которые не принадлежат  $s - 1$ -мерному пространству, натянутому на первые  $s - 1$  строк  $h$ . Отсюда вытекает лемма 1.

Заметим, что вычислить число различных матриц достаточно просто; вместе с тем вычислить число различных кодов  $RS_q(n, d)$  значительно сложнее.

### 5.6.2 Число обобщенных кодов Рида-Соломона

Результатами этого раздела мы воспользуемся в следующих разделах при изучении и анализе кодовых систем открытого шифрования.

**Лемма 5.6.1** *Порядок группы  $\Xi_{\mathfrak{K}}$  автоморфизмов кода Рида-Соломона  $\mathfrak{K} = RS_q(n, d)$  не превосходит  $\min\{N_{q,d-1}, N_{q,n-d+1}\}$ , где  $N_{q,s}$  — число невырожденных квадратных матриц  $h$  размера  $s \times s$  над полем  $\mathbb{F}_q$ .*

**Доказательство.** Как следует из леммы 5.5.1  $|\Xi_{\mathfrak{K}}| = |H_{\mathfrak{K}}|$ , где  $H_{\mathfrak{K}}$  — образ группы автоморфизмов  $\Xi_{\mathfrak{K}}$  кода  $\mathfrak{K} = RS_q(n, d)$  размерности  $k = n - d - 2$  в группу невырожденных  $r \times r$  матриц над  $\mathbb{F}_q$  и  $r$  — одно из чисел  $k$  или  $n - k$  (см. раздел 5.5). Поэтому  $|\Xi_{\mathfrak{K}}| \leq \max(N_{q,k}, N_{q,n-k})$ , где  $k = n - d + 1$  — размерность  $RS_q(n, d)$ . Теорема доказана.  $\square$

Хотя оценка для числа  $|\Xi_{\mathfrak{K}}|$  во многих случаях, по-видимому, весьма грубая, ничего лучшего не известно.

Рассмотрим ансамбль (множество)  $\mathfrak{A}_{\mathfrak{K}}$ ,  $\mathfrak{K} = RS_q(n, d)$ , кодов, определяемых проверочными матрицами из множества  $\mathfrak{B} = \{B\Lambda \mid \Lambda \in U_{q,n}\}$ , где  $B$  — одна, не важно какая, матрица вида (1.2.2), а  $U_{q,n}$  — множество (группа) всех мономиальных матриц над полем  $\mathbb{F}_q$ . Заметим, что ансамбль  $\mathfrak{A}_{\mathfrak{K}}$  совпадает с множеством всех линейных над полем  $\mathbb{F}_q$  кодов, проверочные матрицы которых имеют вид (1.1.5). Кроме того, нетрудно установить, что  $|U_{q,n}| = n!(q-1)^n$ . Нас будет интересовать число различных кодов в ансамбле  $\mathfrak{A}_{\mathfrak{K}}$ .

Следует отметить, что различные матрицы  $B\Lambda$  не обязательно определяют различные коды ансамбля  $\mathfrak{A}_{\mathfrak{K}}$ . Например, если  $\mathfrak{K}$  — один из кодов ансамбля  $\mathfrak{A}_{\mathfrak{K}}$  с проверочной матрицей  $B$  и  $D$  — нетривиальный обобщенный автоморфизм кода  $\mathfrak{K}$ , то матрицы  $B \cdot D$  и  $B$ , где  $B \cdot D \neq B$ , являются различными проверочными матрицами одного и того же кода.

**Лемма 5.6.2** Пусть  $A_q(n, d)$  — число различных кодов в ансамбле  $\mathfrak{A}_{\mathfrak{K}}$ , где  $\mathfrak{K} = RS_q(n, d)$ . Имеет место равенство

$$A_q(n, d) = \frac{n!(q-1)^n}{|\Xi_{\mathfrak{K}}|}, \quad (5.6.2)$$

где  $\Xi_{\mathfrak{K}}$  — группа автоморфизмов одного из кодов не важно какого из ансамбля  $\mathfrak{A}_{\mathfrak{K}}$ .

**Доказательство.** Пусть  $B$  — проверочная матрица кода  $\mathfrak{K} = RS_q(n, d)$  и  $\Lambda$  — мономиальная матрица. Очевидно, группа обобщенных автоморфизмов  $\Xi_{\mathfrak{K}}$  и  $\Xi_{\mathfrak{K}'}$ , где  $\mathfrak{K}'$  — код с проверочной матрицей  $B' = B\Lambda$ , сопряжены:  $\Xi_{\mathfrak{K}} = \Lambda^{-1}\Xi_{\mathfrak{K}'}\Lambda$ . Поэтому для доказательства леммы в качестве  $\mathfrak{K}$  можно выбрать любой код из ансамбля  $\mathfrak{A}_{\mathfrak{K}}$ .

Коды с проверочными матрицами  $B \cdot D \cdot \Lambda$  и  $B \cdot \Lambda$  совпадают, если  $D \in \Xi_{\mathfrak{K}}$  (группа обобщенных автоморфизмов  $\mathfrak{K}$ ), и различны, если  $\Lambda \notin \Xi_{\mathfrak{K}}$ .

Представим мономиальную группу  $M_n$  как объединение левых смежных классов  $\gamma_j \Xi_{\mathfrak{K}}$  по ее подгруппе  $\Xi_{\mathfrak{K}}$ :

$$M_n = \bigcup_{j=1}^T \gamma_j \Xi_{\mathfrak{K}} \quad (5.6.3)$$

Из вышесказанного следует, что коды с проверочными матрицами  $B \cdot \Lambda$  и  $B \cdot \Lambda'$  совпадают или различны, в зависимости от того элементы  $\Lambda$  и  $\Lambda'$  лежат в одном или разных смежных классах. Таким образом, число  $A_q(n, d)$  совпадает с числом  $T$  в равенстве (5.6.3).

Все смежные классы содержат по  $|\Xi_{\mathfrak{K}}|$  элементов. Поэтому в (5.6.3)  $T = \frac{|M_n|}{|\Xi_{\mathfrak{K}}|}$ , что доказывает теорему.  $\square$

К сожалению, как уже было отмечено, порядок группы  $\Xi_{\mathfrak{K}}$  обобщенных автоморфизмов кода Риды-Соломона не известен. Поэтому мы не можем воспользоваться равенством (5.6.2) для вычисления числа  $A_q(n, d)$ .

Вместе с тем из леммы 5.6.1 и соотношений (5.6.1) и (5.6.2) следует

**Следствие 5.6.1** Для числа  $A_q(n, d)$  различных обобщенных Рунда-Соломона  $\mathfrak{R} = RS_q(n, d)$  в ансамбле  $\mathfrak{A}_{\mathfrak{R}}$  имеет место оценка

$$A_q(n, d) \geq \frac{n!(q-1)^n}{N_{q,s}} = \frac{n!(q-1)^n}{(q^s-1)(q^s-q) \cdots (q^s-q^{s-2})}, \quad (5.6.4)$$

где  $s = \min\{n-d+1, d-1\}$ ,  $n!(q-1)^n$  — порядок мономиальной группы  $M_n$  и  $N_{q,s}$  — число различных невырожденных матриц размера  $s \times s$ .

## Глава 6

# Декодирование кодов Рида-Соломона

### 6.1 Что такое алгоритм декодирования?

Алгоритм декодирования оперирует с искаженным вариантом  $\mathbf{a}'$  некоторого (неизвестного) кодового вектора  $\mathbf{a}$ . Его задача — найти одно или несколько наиболее вероятных значений этого исходного кодового вектора  $\mathbf{a}$ .

Алгоритмы декодирования относятся к важнейшим алгоритмам теории кодирования: их сложность в значительной мере определяет возможность использования кодов, корректирующих ошибки, на практике.

Пусть  $A^n$  — метрическое пространство с метрикой  $\lambda(\cdot, \cdot)$ ,  $\mathcal{K} \subset A^n$  — блочный код длины  $n$  над  $A$  и  $\mathbf{a}$  — кодовый вектор из  $\mathcal{K}$ . Обычно полагают, что  $A$  — конечное поле  $\mathbb{F}_q$  или  $A^n$  — единичная сфера  $S^{n-1}$  или  $U^{n-1}$  в  $n$ -мерном евклидовом или унитарном пространстве.

Если "пропустить" вектор  $\mathbf{a} \in A^n$  через канал связи с ошибками, то на его выходе появится вектор  $\mathbf{a}' \in A^n$ , который, вообще говоря, отличается от  $\mathbf{a}$ . Следует отметить, что метрика  $\lambda(\cdot, \cdot)$ , с помощью которой измеряется отличие  $\mathbf{a}'$  от  $\mathbf{a}$ , так или иначе определяется свойствами дискретного канала связи. В данном разделе в качестве метрики  $\lambda$  для дискретного канала мы будем рассматривать только метрику Хемминга. Для непрерывного канала (случай  $A^n = S^{n-1}$  или  $A^n = U^{n-1}$ ) обычно в качестве метрики  $\lambda$  берут евклидову метрику соответствующего пространства.

В теории информации дискретный канал связи описывается переходными вероятностями  $p(\mathbf{a}'|\mathbf{a})$  (вероятность того, что на выходе канала появиться вектор  $\mathbf{a}'$ , если на его вход подать вектор  $\mathbf{a}$ ). Метрика  $\lambda(\cdot, \cdot)$  подбирается так, чтобы наиболее вероятный вектор  $\mathbf{a}$ , т.е. вектор, для которого вероятность  $p(\mathbf{a}'|\mathbf{a})$  принимает максимальное значение, был наиболее близким к вектору  $\mathbf{a}'$ .

Метрика Хемминга отвечает, так называемому дискретному симметричному каналу (ДСК) связи, который определяется следующим образом.

Пусть  $A$  — конечное  $q$ -элементное множество. Дискретный канал определяется переходными вероятностями  $p(a'|a)$ ,  $a', a \in A$ , каждая из которых есть вероятность того, что на выходе канала появиться элемент  $a'$ , если на его вход подать элемент  $a$ . Дискретный канал называется симметричным (ДСК), если

- i.

$$p(a'|a) = \begin{cases} 1-p, & \text{если } a' = a, \\ \frac{p}{q-1}, & \text{если } a' \neq a. \end{cases} \quad (6.1.1)$$

Таким образом, любой символ  $a$  не меняется в канале связи с вероятностью  $1-p$  и замещается другим (происходит ошибка) с вероятностью  $p$ . При этом переход символа  $a$  в другой  $a'$ , если он произошел, не зависит от  $a'$ , т.е. вероятность  $p(a'|a)$  не зависит от  $a$  и  $a'$ , если  $a \neq a'$ .

- ii. Переход в канале связи  $n$ -мерного вектора  $\mathbf{a} = (a_1, \dots, a_n)$  в вектор  $\mathbf{a}' = (a'_1, \dots, a'_n)$ , т.е. вероятность  $p(\mathbf{a}'|\mathbf{a})$ , по определению, равна

$$p(\mathbf{a}'|\mathbf{a}) = p(a'_1|a_1) \cdot \dots \cdot p(a'_n|a_n) = (1-p)^{n-d(\mathbf{a},\mathbf{a}')} p^{d(\mathbf{a},\mathbf{a}')}, \quad (6.1.2)$$

где  $d$  — метрика Хемминга.

Как видно из (6.1.2), ДСК по определению преобразует символы, поступившие на его вход в различные моменты времени, независимо один от другого. Если  $p \leq \frac{1}{2}$ , то, как видно из последнего равенства в (6.1.2), минимальное значение определяется расстоянием Хемминга между векторами  $\mathbf{a}$  и  $\mathbf{a}'$ , т.е. метрика Хемминга "согласована" с дискретным симметрическим каналом связи. Если матрица переходных вероятностей не имеет вида (6.1.1), т.е. канал не является симметрическим, то метрика "согласованная" с таким каналом будет, вообще говоря, неХемминговой. Некоторые из подобного рода неХемминговых метрик будут рассмотрены в разделе 10.4.

Вероятность  $P_t$  того, что в кодовом векторе длины  $n$ , прошедшем через ДСК с вероятностью ошибок  $p$ , произошло  $t$  ошибок равно

$$P_t = (q-1)^t \binom{n}{t} p^t (1-p)^{n-t}. \quad (6.1.3)$$

Среднее число ошибок  $E_{p,n} = \sum_{t=0}^n t P_t$ , произошедшее в векторе  $\mathbf{a} \in A^n$ , как нетрудно вычислить, равно  $E_p = np$ . (Упражнение. Вычислить  $D_{p,n} = \sum_{t=0}^n (E_{p,n} - t P_t)^2$  — дисперсию числа ошибок в векторе  $\mathbf{a}$ ).

Матрица  $P = \|p(a'|a)\|_{a',a \in A}$  называется матрицей переходных вероятностей канала.

В теории кодирования используется модифицированный дискретный симметрический канал связи, который носит название комбинаторного канала связи. В модели комбинаторного канала, которую мы и будем далее использовать, полагают, что искаженный кодовый вектор  $\mathbf{a}' \in A^n$  на выходе комбинаторного канала связи, принадлежит некоторой окрестности кодового вектора  $\mathbf{a}$ , а именно принадлежит шару  $V_{n,t}(\mathbf{a})$  в метрике  $\lambda$  радиуса  $t$  с центром в точке  $\mathbf{a}$ . Таким образом, если  $\lambda$  — метрика Хемминга, то в данной модели канала полагают, что  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$  и вес  $w(\mathbf{e})$  вектора ошибок  $\mathbf{e}$  не выше  $t$ , т.е. кодовый вектор  $\mathbf{a}$  искажен не более, чем в  $t$  разрядах (в канале происходит не более, чем  $t$  ошибок типа замещения символов). Имеются и другие модели комбинаторных каналов, которые отличаются от рассмотренного типами ошибок. Например, известен комбинаторный канал с выпадениями и вставками символов в кодовом векторе.

Формально алгоритм декодирования кода  $\mathcal{K}$  можно рассматривать как алгоритм, который вычисляет решения уравнения

$$\mathbf{x} + \mathbf{e} = \mathbf{a}', \quad \mathbf{x} \in \mathcal{K}, \quad w(\mathbf{e}) \leq t \quad (6.1.4)$$

с неизвестными  $\mathbf{x}$  и  $\mathbf{e}$  и известным вектором  $\mathbf{a}'$ .

Как легко видеть, декодирование всегда однозначно (уравнение (6.1.4) имеет единственное решение), если  $d = d(\mathcal{K}) \geq 2t + 1$ , где  $d(\mathcal{K})$  — кодовое расстояние кода  $\mathcal{K}$ . Если  $d(\mathcal{K}) < 2t + 1$ , то говорят о декодировании за пределами кодового расстояния. В этом случае часто рассматривают списочные алгоритмы декодирования (алгоритмы, которые вычисляют не единственное решение, а список ограниченного размера, в который входит одно или несколько решений уравнения (6.1.4)). Кроме того часто рассматривают алгоритмы декодирования, которые вычисляют правильно одно из решений (6.1.4) почти для всех  $\mathbf{e}$ .

Наиболее сильным алгоритмом декодирования является, так называемый алгоритм декодирования по максимуму правдоподобия. Этот алгоритм для любого  $\mathbf{a}'$  вычисляет один из ближайших к  $\mathbf{a}'$  кодовый вектор  $\mathbf{a}$ . Термин "максимальное правдоподобие" используется из-за того, что метрика Хемминга полностью согласована с ДСК, т.е. ближайший к  $\mathbf{a}'$  кодовый вектор одновременно является наиболее вероятным кодовым вектором  $\mathbf{a}$ , из которого возник  $\mathbf{a}'$ .

Следует сказать, для многих классов линейных кодов уравнение (6.1.4) имеет почти всегда (почти для всех векторов-ошибок  $\mathbf{e}$ ) только одно решение даже, если  $t$  несколько больше, чем  $(d - 1)/2$ .

Основным параметром, который характеризует алгоритм декодирования кода  $\mathcal{K}$ , является его сложность  $T(\mathcal{K})$ . Значительное число работ в области теории кодирования посвящено проблеме разработки эффективных алгоритмов декодирования для тех или иных классов кодов. В этом разделе мы будем рассматривать только декодирование  $q$ -значных кодов Рида-Соломона.

Заметим, что сложность  $T(n, k, t)$  декодирования по максимуму правдоподобия  $q$ -значного кода "общего положения" не выше  $O(\min(nq^k, n|V_{n,t}|))$ , где  $|V_{n,t}|$  — объём шара радиуса  $t$  в метрическом пространстве Хемминга  $\mathbb{F}_q^n$ . Действительно, решение (6.1.4) можно найти, последовательно перебирая либо векторы  $\mathbf{x} \in \mathcal{K}$ , проверяя при этом выполнение условия  $wt(\mathbf{a}' - \mathbf{x}) \leq t$ , либо можно перебирать векторы ошибок  $\mathbf{e}$ , вес которых ограничен числом  $t$ , проверяя выполнимость условия  $\mathbf{a}' - \mathbf{e} \in \mathcal{K}$ . Подобные алгоритмы декодирования принято называть переборными.

Также следует сказать, что не известно никаких бесконечных нетривиальных семейств кодов, для которых алгоритм декодирования по максимуму правдоподобию имеет полиномиальную сложность.

При  $n \rightarrow \infty$ ,  $\frac{k}{n} \rightarrow \kappa$ ,  $\frac{t}{n} \rightarrow \tau$ ,  $0 < \kappa < 1$ ,  $0 < \tau < \frac{1}{2}$ , по современным представлениям сложность  $T(n, k, t)$  декодирования по максимуму правдоподобия кода "общего положения" является предположительно экспоненциальной от длины кода  $n$ . Более того, задача декодирования по максимуму правдоподобия некоторого подкласса кодов "общего положения" даже в несколько ослабленной постановке является NP-полной. Вместе с тем сложность декодирования, рассматриваемых ниже алгоритмов декодирования алгебраических кодов, является полиномиальной по  $n$  (как правило не выше, чем  $O(n^3)$ ). Эти алгоритмы не являются алгоритмами декодирования по максимуму правдоподобия.

### 6.1.1 Вводные понятия

Мы рассматриваем  $q$ -значный код Рида-Соломона  $RS_s(\mathcal{A})$  длины  $N \leq q$  с проверочной матрицей  $B = B_{\mathcal{A}}^{(d)}$  (см. (5.0.1)), где  $\mathcal{A} = \{\alpha_1, \dots, \alpha_N\} \subseteq \mathbb{F}_q$  и кодовым расстоянием  $d = s + 2 \geq 3$ . По определению коду принадлежат все векторы  $\mathbf{a} \in \mathbb{F}_q^N$ , для которых  $\mathbf{a}B^T = 0$ , где  $B^T$  — транспонированная матрица  $B$ .

Мы говорим, что  $\mathbf{a}'$  является кодовым вектором, искаженным  $t$  ошибками, если существуют вектор  $\mathbf{a} \in RS_s(\mathcal{A})$  и вектор  $\mathbf{e}$  веса не более, чем  $t$  такие, что  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$ .

Таким образом, все векторы пространства  $\mathbb{F}_q^N$  разбивается на две подмножества:  $\mathbb{F}^{(t)}$  — кодовые векторы, искаженные  $t$  ошибками, и  $\mathbb{F}_q^N \setminus \mathbb{F}^{(t)}$  — все остальные векторы пространства  $\mathbb{F}_q^N$ . Очевидно,  $\mathbb{F}^{(t)}$  состоит из всех векторов  $\mathbb{F}_q^N$ , расстояние которых до кода  $RS_s(\mathcal{A})$  не более, чем  $t$ .

Алгоритм, который для каждого кодового  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$ , искаженного  $t$  ошибками, находит какой-либо вектор  $\mathbf{a}^*$  из  $RS_s(\mathcal{A})$ , для которого  $\mathbf{a}' = \mathbf{a}^* + \mathbf{e}^*$ ,  $wt(\mathbf{e}^*) \leq wt(\mathbf{e})$ , назовем алгоритмом декодирования кода  $RS_s(\mathcal{A})$  глубины  $t$ . Мы не требуем, чтобы  $\mathbf{a}^* = \mathbf{a}$ .

Таким образом, алгоритм декодирования глубины  $t$  не обязан находить вектор  $\mathbf{a}$ , из которого "образовался" вектор  $\mathbf{a}'$ . Он находит только один из векторов  $\mathbf{a}^*$  кода  $RS_s(\mathcal{A})$ , расстояние которого до  $\mathbf{a}'$  не более, чем  $wt(\mathbf{e})$ .

Если  $\mathbf{a}' \notin \mathbb{F}^{(t)}$ , т.е.  $\mathbf{a}'$  не является кодовым вектором, искаженным  $t$  ошибками, то работа алгоритма декодирования глубины  $t$  никак не регламентирована: он может выдавать произвольный кодовый вектор или не выдавать ничего.

В этой связи в качестве важного класса алгоритмов декодирования следует упомянуть алгоритмы, которые для произвольного вектора  $\mathbf{a}'$  выдают вектор кода  $\hat{\mathbf{a}}$ , наиболее близкий к  $\mathbf{a}'$ . Если таких векторов несколько, то алгоритм выдает один из них. Заметим, что в разделе 6.1 они выступали под именем алгоритм декодирования по максимуму правдоподобия. Эти алгоритмы являются наиболее сильными из всех алгоритмов декодирования и могут быть, очевидно, реализованы переборными средствами.

К настоящему времени не известно никаких полиномиальных алгоритмов этого типа ни для каких нетривиальных бесконечных классов кодов. Вместе с тем более слабый алгоритм, например, алгоритм декодирования кода Рида-Соломона глубины  $t$ , естественно, только для ограниченных значений  $t$ , является полиномиальным, т.е. он является алгоритмом, сложность которого является полиномиальной от длины кода  $n$ . К полиномиальным алгоритмам декодирования также относится, рассматриваемый ниже, алгоритм декодирования кода Рида-Соломона в пределах его кодового расстояния.

Вектор

$$\mathbf{b} = (b_0, \dots, b_s) = \mathbf{a}'B^T = \mathbf{e}B^T = \sum_{i=1}^t k_{j_i} B(\alpha_{j_i}), \quad wt(\mathbf{e}) \leq t \quad (6.1.5)$$

где  $k_{j_i} \in \mathbb{F}_q$  — значения ненулевой координаты с номером  $j_i$  вектора  $\mathbf{e}$  и  $B(\alpha_j)$  —  $j$ -ый столбец матрицы  $B = B_{\mathcal{A}}^{(d)}$  (см. (5.0.1)), называется синдромом вектора  $\mathbf{a}'$ . Вектор  $\mathbf{e}$ , для которого справедливо равенство (6.1.5), называется вектором ошибок, соответствующим синдрому  $\mathbf{b}$ .

Алгоритм, который по синдрому  $\mathbf{b}$  кодового вектора  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$ , искаженного  $t$  ошибками ( $wt(\mathbf{e}) \leq t$ ), находит вектор  $\mathbf{a}^* \in RS_s(\mathcal{A})$ , расстояние которого от  $\mathbf{a}'$  не более, чем  $t$ , назовем синдромным алгоритмом декодирования кода  $RS_s(\mathcal{A})$  глубины  $t$ . По существу, синдромный алгоритм глубины  $t$  — это алгоритм декодирования глубины  $t$ , который работает только с синдромом кодового вектора, искаженного  $t$  ошибками.



Обычно синдромный алгоритм глубины  $t$  сначала находит вектор  $\mathbf{e}$ ,  $wt(\mathbf{e}) \leq t$ , который удовлетворяет соотношению  $\mathbf{b} = \mathbf{e}B^T$ , а затем вычисляет кодовый вектор  $\mathbf{a} = \mathbf{a}' - \mathbf{e}$ . Задача нахождения указанного вектора ошибок  $\mathbf{e}$  является основной и наиболее сложной задачей синдромного алгоритма декодирования. Часто только решением этой задачи и ограничивается синдромный алгоритм.

## 6.2 Синдромный метод декодирования РМ-кодов

### 6.2.1 Предварительные замечания

Основной нашей задачей, которую мы будем решать в этом параграфе, является задача нахождения решений  $\mathbf{x}_0 = \mathbf{e}$  уравнения

$$\mathbf{x}B^T = \mathbf{b}, \mathbf{x} \in \mathbb{F}_q^N, \mathbf{b} \in \mathbb{F}_q^{N-k}, \quad (6.2.1)$$

которые имеют вес  $wt(\mathbf{e})$ , не превосходящий  $t$ . Решение этой задачи, как вытекает из соотношения (6.1.5), является одним из возможных способов декодирования кода Рида-Соломона глубины  $t$ .

Пусть  $L(B) \subset \mathbb{F}_q^N$  — линейное пространство, образованное решениями однородной системы уравнений  $\mathbf{x}B^T = 0$ . Как известно, множество решений  $L(B, \mathbf{b})$  системы (6.2.1) является смежным классом пространства  $L(B)$ , т.е. имеет вид  $L(B, \mathbf{b}) = \{\mathbf{e} + \mathbf{y} | \mathbf{y} \in L(B)\}$ , где  $\mathbf{e}$  — одно из решений (6.2.1).

Отсюда вытекает, что очевидным алгоритмом решения этой задачи является перебор всех векторов множества решений  $M(B, \mathbf{b})$  системы (6.2.1) и выделения среди них тех, вес которых не превосходит  $t$ . Трудоемкость этого алгоритма не меньше, чем  $O(q^k)$ .

Заметим, что можно перебирать и векторы  $\mathbf{e}$ , вес которых не превосходит  $t$ , и которые удовлетворяют уравнению (6.2.1). Трудоемкость этого алгоритма не меньше, чем  $O((q-1)^t \binom{N}{t})$ .

Эти два алгоритма при  $\frac{k}{\log n} \rightarrow \infty$  и  $t \rightarrow \infty$  не являются полиномиальными.

Далее мы будем рассматривать один из возможных полиномиальных алгоритмов решения системы (6.2.1). В основе этого алгоритма лежат классические работы ученых Петербургской школы математиков П.Л. Чебышева, А.А. Маркова и голландского математика Т. Стилтеса, живших в XIX веке. Весьма неожиданным является то, что их идеи, связанные с механическими квадратурами, нашли непосредственное приложения для декодирования кодов Рида-Соломона.

Вид матрицы  $B$  позволяет при условии  $wt(\mathbf{x}) = u \leq t$  записать систему уравнений (6.2.1) в виде

$$b_i = \sum_{j=1}^u e_j \delta_j^i, \quad i = 0, \dots, s, \quad (6.2.2)$$

где неизвестными являются  $u$ -элементное множество  $\Delta = \{\delta_1, \dots, \delta_u\} \subset \mathcal{A} = \{\alpha_1, \dots, \alpha_N\}$  (индексы ненулевых координат вектора ошибок) и набор коэффициентов  $E = \{e_1, \dots, e_u\}$ ,  $e_u \in \mathbb{F}_q \setminus \{0\}$  (значения ненулевых координат вектора ошибок). Мы будем строить алгоритм декодирования как алгоритм решения системы (6.2.2), в которой значение параметра  $u$  известно.

Мы также всегда будем предполагать, что вектор  $\mathbf{b}$  (левая часть в (6.2.2)) выбрана так, что система (6.2.2) имеет решение.

## 6.2.2 Вспомогательные утверждения

Сделаем несколько предварительных замечаний, которые будут использованы далее. Пусть  $\mathfrak{B} = \{\beta_1, \dots, \beta_u\}$  —  $u$ -элементное подмножество элементов поля  $\mathbb{F}_q$ ,

$$m_i = \sum_{j=1}^u k_j \beta_j^i, \quad k_j \in \mathbb{F}_q \setminus \{0\}, \quad u \geq 1, \quad i = 0, \dots, s, \dots \quad (6.2.3)$$

и

$$\Delta_{r-1} = \begin{pmatrix} m_0 & m_1 & \cdots & m_{r-1} \\ m_1 & m_2 & \cdots & m_r \\ \vdots & \vdots & \cdots & \vdots \\ m_{r-1} & m_r & \cdots & m_{2r-2} \end{pmatrix} \quad (6.2.4)$$

— матрица порядка  $r$ .

Обычно величины  $m_i$  называют моментами, элементы множества  $\mathfrak{B}$  — точками сосредоточения масс и  $k_j$  — массой точки  $\beta_j$ . Эти классические термины, введенные в XIX веке, происходят из механической трактовки величин  $k_j$  и  $\beta_j$ .

### Лемма 6.2.1

Если  $r = u$ , то  $\Delta_{r-1} \neq 0$ .

Если  $r > u$ , то  $\Delta_{r-1} = 0$ .

**Доказательство.** Рассмотрим  $u \times u$ -матрицу Вандермонда

$$W_{u-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_u \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^{u-1} & \beta_2^{u-1} & \cdots & \beta_u^{u-1} \end{pmatrix}. \quad (6.2.5)$$

Как хорошо известно, для любого  $u$ -элементного множества  $\mathfrak{B}$  определитель Вандермонда  $|W_{u-1}|$  отличен от нуля.

Нетрудно установить (Упражнение), что

$$\Delta_{u-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_u \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^{u-1} & \beta_2^{u-1} & \cdots & \beta_u^{u-1} \end{pmatrix} \cdot \begin{pmatrix} k_1 & k_1 \beta_1 & \cdots & k_1 \beta_1^{u-1} \\ k_2 & k_2 \beta_2 & \cdots & k_2 \beta_2^{u-1} \\ \vdots & \vdots & \cdots & \vdots \\ k_u & k_u \beta_u & \cdots & k_u \beta_u^{u-1} \end{pmatrix}. \quad (6.2.6)$$

Отсюда вытекает, что определитель

$$|\Delta_{u-1}| = |W_{u-1}|^2 \prod_{i=1}^u k_i \quad (6.2.7)$$

матрицы  $\Delta_{u-1}$  отличен от нуля.

Пусть теперь  $r > u$ . Очевидно,  $\Delta_{r-1} = \prod_{i=1}^u k_i W_{r-1}^2$ , где  $W_{r-1}$  —  $r \times r$ -матрица Вандермонда  $W_{u-1}$ , дополненная  $r - u > 0$  нулевыми столбцами и строками. Очевидно,  $W_{r-1} = 0$  при  $r > u$ , что доказывает лемму.  $\square$

Рассмотрим многочлен

$$T_u(x, y) = T_u(x, y, \mathfrak{B}) = |\Delta_{u-1}|^{-1} \begin{vmatrix} 0 & 1 & x & \cdots & x^{u-1} \\ 1 & m_0 & m_1 & \cdots & m_{u-1} \\ y & m_1 & m_2 & \cdots & m_u \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ y^{u-1} & m_{u-1} & m_u & \cdots & m_{2u-2} \end{vmatrix}. \quad (6.2.8)$$

от двух переменных  $x$  и  $y$ . Многочлен  $T_u(x, y)$  является симметрическим. (Упражнение)

**Лемма 6.2.2** *Имеет место соотношение*

$$T_u(\beta_i, \beta_j, \mathfrak{B}) = \begin{cases} 0, & \text{если } j \neq i, \\ -\frac{1}{k_j}, & \text{если } j = i \end{cases}. \quad (6.2.9)$$

**Доказательство.** Без ограничения общности положим  $j$  равным 1. Легко проверить, что

$$\begin{pmatrix} 0 & 1 & \beta_i & \cdots & \beta_i^{u-1} \\ 1 & m_0 & m_1 & \cdots & m_{u-1} \\ \beta_1 & m_1 & m_2 & \cdots & m_u \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \beta_1^{u-1} & m_{u-1} & m_u & \cdots & m_{2u-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & \beta_1 & \beta_2 & \cdots & \beta_u \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \beta_1^{u-1} & \beta_2^{u-1} & \cdots & \beta_u^{u-1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & \beta_i & \cdots & \beta_i^{u-1} \\ 1 & k_1 & k_1 \beta_1 & \cdots & k_1 \beta_1^{u-1} \\ 0 & k_2 & k_2 \beta_2 & \cdots & k_2 \beta_2^{u-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & k_u & k_u \beta_u & \cdots & k_u \beta_u^{u-1} \end{pmatrix}. \quad (6.2.10)$$

Определитель матрицы, стоящий в левой части равенства (6.2.10), по определению функции  $T_u(\beta_i, \beta_j, \mathfrak{B})$ , равен  $\Delta_{u-1} T_u(\beta_i, \beta_1, \mathfrak{B})$ . Определитель матрицы, стоящий в правой части равенства (6.2.10), равен  $W_{u-1} \cdot \widehat{W}_{u-1, i}$ , где  $\widehat{W}_{u-1, i}$  — определитель последней матрицы в (6.2.10). Этот определитель равен 0, если  $i \neq 1$ , так как он содержит в этом случае две пропорциональных строки, и, очевидно, равен  $-W_{u-1} \prod_{i=2}^u k_i$ , если  $i = 1$ . Отсюда и из равенства (6.2.7) следует утверждение леммы.  $\square$

### 6.2.3 Многочлен локаторов ошибок

Рассмотрим многочлен

$$O_r(x, m_0, m_1, \dots, m_{2u-1}) = O_r(x) = \begin{vmatrix} m_0 & m_1 & \cdots & m_{r-1} & 1 \\ m_1 & m_2 & \cdots & m_r & x \\ m_2 & m_3 & \cdots & m_{r+1} & x^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m_r & m_{r+1} & \cdots & m_{2r-1} & x^r \end{vmatrix}, \quad (6.2.11)$$

степени не выше  $r$ , где моменты  $m_i$  определены в разделе 6.2.2, равенство (6.2.3).

**Лемма 6.2.3** *Множество корней ненулевого многочлена  $O_u(x, m_0, m_1, \dots, m_{2u-1})$  степени  $u$  совпадает с множеством  $\mathfrak{B}$ .*

**Доказательство.** Многочлен  $O_u(x, m_0, m_1, \dots, m_{2u-1})$  отличен от нуля, ибо его коэффициент при  $x^u$ , равный  $|\Delta_{u-1}|$ , согласно лемме 6.2.1 отличен от нуля.

Пусть

$$F_{\mathfrak{B}}(x) = \prod_{i=1}^u (x - \beta_i) = \sum_{j=0}^u a_j x^j \quad (6.2.12)$$

— многочлен, корни которого образуют множество  $\mathfrak{B}$ .

Если прибавить к последней строке определителя в (6.2.11) остальные строки с коэффициентами  $a_j$ , то с учетом определения моментов  $m_j$  получим строку, у которой первая координата равна  $F_{\mathfrak{B}}(x)$ , а остальные — нулю. Отсюда получаем, что  $O_u(x) = |\Delta_{u-1}| F_{\mathfrak{B}}(x)$  и, следовательно,  $O_u(\beta) = 0$  тогда и только тогда, когда  $\beta \in \mathfrak{B}$ .  $\square$

Многочлен  $F_{\mathfrak{B}}(x)$  в теории кодирования называют многочленом локаторов ошибок. Таким образом, лемма 6.2.3 явно указывает способ построения многочлена локатора ошибок:

$$F_{\mathfrak{B}}(x) = |\Delta_u|^{-1} O_u(x, b_0, b_1, \dots, b_{2u-1}), \quad (6.2.13)$$

в том случае, когда известен синдром  $\mathbf{b} = (b_0, \dots, b_s) = \mathbf{a}' B^T$  кодового вектора  $\mathbf{a}'$ , искаженного  $u$  ошибками, и  $d - 2 = s \geq 2u - 1$ . Очевидно, максимальное число ошибок  $u$ , для которых можно построить многочлен локаторов ошибок, ограничено сверху числом  $u \leq \frac{d-1}{2}$ .

Для того, чтобы вычислить множество  $\mathfrak{B}$  локаторов ошибок, которые поразили принятый вектор  $\mathbf{a}'$ , нужно найти корни многочлена  $O_u(x, b_0, b_1, \dots, b_{2u-1})$ , которые всегда принадлежат множеству  $\mathcal{A} \subseteq \mathbb{F}_q$ . Вычисление корней последнего многочлена обычно производят с помощью вычисления его значений во всех точках множества  $\mathcal{A}$ , т.е., по существу, полным перебором элементов множества  $\mathcal{A}$ .

Трудоёмкость рассмотренного алгоритма вычисления множества  $\mathfrak{B}$  индексов ошибок складывается из трудоёмкости двух алгоритмов: вычисления синдрома  $\mathbf{b}$  (умножения вектора  $\mathbf{a}'$  на матрицу  $B$ ) и вычисления корней многочлена  $O_u(x, b_0, b_1, \dots, b_{2u-1})$ .

Трудоёмкость первого, очевидно, не превосходит  $O(u \cdot n)$ ,  $n = |\mathcal{A}|$ , операций в поле  $\mathbb{F}_q$ . Трудоёмкость второго оценить несколько сложнее в виду того, что можно предложить несколько различных алгоритмов для вычисления коэффициентов многочлена  $O_t(x, b_0, b_1, \dots, b_{2u-1})$ .

Самым простым, но не самым эффективным алгоритмом вычисления коэффициентов многочлена  $O_u(x, b_0, b_1, \dots, b_{2u-1})$ , является алгоритм, который вычисляет его коэффициенты, исходя из его представления в виде (6.2.12).

Число операций  $T_0(u, n)$  в поле  $\mathbb{F}_q$ , требуемых для этого не превосходит  $O(u^4)$  в виду того, что каждый коэффициент  $a_j$  при  $x^j$  равен  $\frac{\Delta_{u,j}}{\Delta_u}$ , где  $\Delta_{u,j}$  — минор при элементе  $x^j$  определителя (6.2.11). При этом мы полагаем, что определитель размера  $u \times u$  можно вычислить с помощью  $O(u^3)$  операций в поле  $\mathbb{F}_q$ .

Затем, для вычисления корней  $O_u(x, b_0, b_1, \dots, b_{2u-1})$  мы вычисляем значения многочлена  $F_{\mathfrak{B}}(x)$  в различных точках множества  $\mathcal{A}$ . Если использовать алгоритм Горнера для вычисления значения указанного многочлена в точке, то число операций  $T_1(u, n)$  в поле  $\mathbb{F}_q$ , требуемых для этого, окажется равным  $un$ ,  $n = |\mathcal{A}|$ . В итоге число операций  $T(u, n)$ , требуемых для вычисления корней многочлена  $F_{\mathfrak{B}}(x)$  или, что одно и тоже для нахождения множества локаторов ошибок  $\mathfrak{B}$ , рассмотренным алгоритмом будет равным

$$T(u, n) = T_0(u, n) + T_1(u, n) = O(u^4) + O(un). \quad (6.2.14)$$

Между прочим, в случае  $n \rightarrow \infty$ ,  $u = \text{const}$ , из (6.2.14) следует, что число операций, необходимых для вычисления множества локаторов ошибок  $\mathfrak{B}$ , равно  $O(n)$ .

Дальнейшие исследования по уменьшению трудоемкости  $T(u, n)$  связаны с построением более эффективных алгоритмов вычисления коэффициентов  $a_j$  многочлена  $F_{\mathfrak{B}}(x) = |\Delta_{u-1}|^{-1} O_u(x, b_0, b_1, \dots, b_{2u-1})$ . Для их изложения необходимы некоторые дополнительные сведения, к изложению которых мы и переходим.

## 6.2.4 Алгоритм Берлекэмпа

Как легко установить (Упражнение), последовательность  $\mathbf{m} = (m_0, m_1, \dots, m_s)$ ,  $s \geq 2u$ , координаты  $m_j$  которой определены соотношениями (6.2.3), является рекуррентной последовательностью, т.е. ее координаты связаны линейными соотношениями

$$m_{l+u} = -(a_{u-1}m_{l+u-1} + a_{u-2}m_{l+u-2} + \dots + a_0m_l), \text{ для любого } l \geq 0, \quad (6.2.15)$$

где  $F_{\mathfrak{B}}(x) = x^u + \sum_{i=1}^{u-1} a_i x^i$  — многочлен, корнями которого являются все элементы множества  $\mathfrak{B}$  (см. начало §6.2.2).

Многочлен для которого выполнены соотношения 6.2.15 называется проверочным или аннулирующим последовательности  $\mathbf{m}$ . Из леммы 6.2.3 непосредственно вытекает, что аннулирующим многочленом последовательности  $\mathbf{m}$  является многочлен  $\frac{1}{\Delta_{u-1}} O_u(x, m_0, m_1, \dots, m_{2u-1})$ .

Таким образом, последовательность  $\mathbf{m}$  при  $s > u$  является рекуррентной последовательностью глубины  $u$ . Очевидно, коэффициенты  $a_j$  ее аннулирующего многочлена  $F_{\mathfrak{B}}(x) = \prod_{i=1}^u (x - \beta_i)$  с одной стороны определяются элементами  $\beta_j$ , а с другой — являются решением системы линейных уравнений

$$m_{l+u} + (x_{u-1}m_{l+u-1} + x_{u-2}m_{l+u-2} + \dots + x_0m_l = 0, \quad l = 0, \dots, u-1, \quad (6.2.16)$$

с  $u$  неизвестными.

Предположим теперь, что нам задана только последовательность  $\mathbf{m}$  и мы хотим вычислить ее аннулирующий многочлен  $F(x)$ . Алгоритм Берлекэмпа как раз и предназначен для того, чтобы экономно вычислить коэффициенты  $a_j$  аннулирующего многочлена  $F(x)$  минимальной степени последовательности  $\mathbf{m}$ .

Далее мы предполагаем, что число  $u$  является известным. Как его вычислить в том случае, если оно неизвестно, будет объяснено ниже.

Заметим, что соотношения (6.2.15) можно рассматривать как систему из  $u$  линейных уравнений, в которой неизвестными являются коэффициенты  $a_j$ ,  $j = 0, \dots, u-1$ . Если длина последовательности  $\mathbf{m}$  равна  $2u-1$  ( $s = 2u-2$ ), то число уравнений в (6.2.15) совпадает с числом неизвестных. В этом случае матрицей системы является матрица  $\Delta_{u-1}$ , определитель которой согласно лемме 6.2.1 отличен от нуля. Следовательно, система (6.2.15) при  $s = 2u-2$  всегда имеет единственное решение, которое определяет коэффициенты многочлена локаторов ошибок  $F_{\mathfrak{Z}}(x)$ .

Как хорошо известно, сложность решения линейной системы уравнений методом исключения Гаусса равна  $O(u^3)$ . Таким образом, число операций, требуемых для вычисления многочлена локаторов ошибок снижается с  $O(u^4)$  (число операций, требуемых для вычисления коэффициентов многочлена  $O_u(x)$ , исходя из его определения (6.2.11)) до  $O(u^3)$  (см. (6.2.14)). Дальнейшее снижение трудозатрат до  $O(u^2)$  можно получить, используя хорошо известные рекуррентное соотношение между ортогональными многочленами и, так называемую, формулу Кристофеля-Дарбу.

Далее мы, в конечном итоге, изложим некоторые алгоритмы решения линейной системы (6.2.15), которые имеют небольшую вычислительную сложность.

Матрица коэффициентов системы (6.2.15) имеет вид  $(m_{i+j})$ ,  $i, j = 0, \dots, u-1$ . Матрицы подобного вида хорошо известны и носят название матрицы Ганкеля или ганкелевой матрицей [22]. Эти матрицы на протяжении последних полутора столетий служили предметом исследования многих разделов математического анализа (положительно определенные квадратичные формы, проблемы моментов и т.п.). Эти результаты получены на протяжении последних более, чем полтора столетий несколькими замечательными как отечественными (Чебышев П.Л., Марков А.А. и др.) так и некоторыми зарубежными математиками.

В настоящей книге мы воспользуемся этими классическими результатами. Вместе с тем отметим, что классические результаты известны только для случая, в котором основным полем является поле действительных чисел. Если основным полем является конечное поле характеристики  $p$ , то возникают некоторые дополнительные сложности, которые отсутствуют в классическом случае.

Мы обозначаем через  $O_r(x) = O_r(x, m_0, m_1, \dots, m_{2r-1})$ ,  $1 \leq r \leq u$ , многочлен (см. (6.2.11)), определенный первыми  $2r$  моментами  $m_j$ . Мы полагаем, что  $O_0(x) = 1$  и  $O_{-1}(x) = 0$ .

Мы будем предполагать, что степень многочленов  $O_r(x)$ ,  $r = 1, \dots, u$ , равна  $r$ , т.е., что все определители  $\Delta_{r-1}$ ,  $r = 2, \dots, u$  отличны от нуля. Это является достаточно существенным ограничением на область использования алгоритма Берлекэмпа. Как поступать в случае, когда это предположение не выполнено, мы рассмотрим ниже в разделе 6.2.5.

Пусть  $\mathfrak{Z}$  —  $u$ -элементное подмножество множества  $\mathbb{F}_q$  и  $k_j$ ,  $j = 1, \dots, u$  — ненулевые элементы этого поля. Мы определяем функционал  $\mathfrak{S}_{\mathfrak{Z}}$ , определенный на линейном пространстве многочленов над  $\mathbb{F}_q$  степени не выше  $2u-1$ , с помощью соотношения

$$\mathfrak{S}_{\mathfrak{B}} \left( \sum_{i=0}^{2u-1} a_i x^i \right) = \sum_{i=0}^{2u-1} a_i m_i, \quad a_i \in \mathbb{F}_q, \quad (6.2.17)$$

где элементы  $m_i$  определены соотношением (6.2.3).

**Лемма 6.2.4** *Многочлены*

$$P_r(x) = \frac{1}{\sqrt{|\Delta_r| \cdot |\Delta_{r+1}|}} O_r(x), \quad r = 0, \dots, u, \quad (6.2.18)$$

являются ортонормированными многочленами относительно функционала  $\mathfrak{S}_{\mathfrak{B}}$ , т.е.

$$\mathfrak{S}_{\mathfrak{B}}(P_r(x)P_{r'}(x)) = \begin{cases} 0, & \text{если } r \neq r', \\ 1, & \text{если } r = r' \text{ и } r < u. \end{cases} \quad (6.2.19)$$

**Доказательство.** Для доказательства первого равенства в (6.2.19), очевидно, достаточно показать, что  $\mathfrak{S}_{\mathfrak{B}}(x^r O_{r'}(x)) = 0$ , если  $r < r'$ . Действительно, при  $r < r' \leq u$

$$\begin{aligned} \mathfrak{S}_{\mathfrak{B}}(x^r O_{r'}(x)) &= \mathfrak{S}_{\mathfrak{B}} \left( \begin{vmatrix} m_0 & m_1 & \cdots & m_{r'-1} & x^r \\ m_1 & m_2 & \cdots & m_{r'} & x^{r+1} \\ m_2 & m_3 & \cdots & m_{r'+1} & x^{r+2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m_{r'} & m_{r'+1} & \cdots & m_{2r'-1} & x^{r+r'} \end{vmatrix} \right) = \\ &= \begin{vmatrix} m_0 & m_1 & \cdots & m_{r'-1} & m_r \\ m_1 & m_2 & \cdots & m_{r'} & m_{r+1} \\ m_2 & m_3 & \cdots & m_{r'+1} & m_{r+2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m_{r'} & m_{r'+1} & \cdots & m_{2r'-1} & m_{r+r'} \end{vmatrix} = 0, \end{aligned} \quad (6.2.20)$$

ибо последний столбец последнего определителя совпадает с одним из его предыдущих столбцов.

Если  $r = r' < u$ , то из предпоследнего равенства в (6.2.20) вытекает, что  $\mathfrak{S}_{\mathfrak{B}}(O_r^2(x)) = \mathfrak{S}_{\mathfrak{B}}(|\Delta_r| x^r O_r(x)) = |\Delta_r| |\Delta_{r+1}| \neq 0$ . Поэтому  $\mathfrak{S}_{\mathfrak{B}}(P_r^2(x)) = \frac{1}{|\Delta_r| |\Delta_{r+1}|} \mathfrak{S}_{\mathfrak{B}}(O_r^2(x)) = 1$ .  $\square$

**Лемма 6.2.5** *Имеет место соотношение*

$$xP_r(x) = c_{r,r+1}P_{r+1}(x) + c_{r,r}P_r(x) + c_{r,r-1}P_{r-1}(x), \quad r = 0, \dots, u-1 \quad (6.2.21)$$

где

$$c_{r,r-1} = \frac{\sqrt{|\Delta_{r-1}| |\Delta_{r+1}|}}{|\Delta_r|}, \quad c_{r,r} = \mathfrak{S}_{\mathfrak{B}}(x \cdot P_r^2(x)), \quad c_{r,r+1} = \frac{\sqrt{|\Delta_{r+2}| |\Delta_r|}}{|\Delta_{r+1}|}. \quad (6.2.22)$$

**Доказательство.** Многочлен  $xP_r(x)$  степени  $r+1$  представим в виде суммы ортогональных многочленов  $P_j(x)$ ,  $j = 0, \dots, r+1$ ,

$$xP_r(x) = \sum_{j=0}^{r+1} c_{r,j} P_j(x). \quad (6.2.23)$$

Умножим левую и правую части равенства (6.2.23) на многочлен  $P_k(x)$  и вычислим от обеих частей полученного равенства, используя соотношение (6.2.19), значение функционала  $\mathfrak{S}_{\mathfrak{B}}$ . В результате получим, что  $c_{r,k} = 0$ ,  $k = 0, \dots, r-2$ . Для вычисления коэффициента  $c_{r,r+1}$  достаточно сравнить коэффициенты при  $x^{r+1}$  левой и правой частях равенства (6.2.21). Остальные коэффициенты в (6.2.23), как нетрудно установить, определяются соотношениями (6.2.22).  $\square$

Непосредственно из соотношений (6.2.22) следует

**Следствие 6.2.1** *Равенство (9.2.2) можно представить в виде*

$$xP_r(x) = a_r P_{r+1}(x) + b_r P_r(x) + a_{r-1} P_{r-1}(x), \quad (6.2.24)$$

где

$$a_r = \frac{\sqrt{|\Delta_{r+2}||\Delta_r|}}{|\Delta_{r+1}|}, \quad r = 0, \dots, u-1, \quad b_r = c_{r,r} = \mathfrak{S}_{\mathfrak{B}}(x \cdot P_r^2(x)). \quad (6.2.25)$$

Отметим, что утверждение следствия (6.2.1) является нетривиальным: коэффициенты  $c_{r,r+1}$  и  $c_{r,r-1}$  в (6.2.21) связаны следующим соотношением  $c_{r,r-1} = c_{r-1,r+1}$ .

**Оценка сверху числа операций, требуемых для вычисления многочлена  $P_{r+1}(x)$**

Соотношение (6.2.24) удобно записать в следующем виде

$$O_{r+1}(x) = \frac{|\Delta_{r+1}|}{|\Delta_r|} (b_r - x) O_r(x) - \sqrt{\frac{|\Delta_{r+1}|^3 |\Delta_{r-2}|}{|\Delta_{r-1}|^3 |\Delta_r|}} O_{r-1}(x). \quad (6.2.26)$$

Если в равенстве (6.2.26) известны многочлены  $O_r(x)$ ,  $O_{r-1}(x)$  и коэффициенты  $\alpha_r = \frac{|\Delta_{r+1}|}{|\Delta_r|}$ ,  $b_r$  и  $\beta_r = \sqrt{\frac{|\Delta_{r+1}|^3 |\Delta_{r-2}|}{|\Delta_{r-1}|^3 |\Delta_r|}}$  при  $O_r(x)$  и  $O_{r-1}(x)$ , то число операций, требуемых для вычисления многочлена  $O_{r+1}(x)$ , очевидно, равно  $O(r)$  операций в поле  $\mathbb{F}_q$ .

Коэффициенты  $\alpha_r$ ,  $b_r$ ,  $\beta_r$  можно экономно вычислить следующим образом.

Сначала вычислим определитель  $|\Delta_{r+1}|$ , используя для этого известный многочлен  $O_r(x)$ . Из леммы 6.2.4 (соотношение (6.2.19)) следует

$$\mathfrak{S}_{\mathfrak{B}}(O_r^2(x)) = |\Delta_{r+1}| |\Delta_r|. \quad (6.2.27)$$

Пусть  $O_r(x) = \sum_{j=0}^r o_{r,j} x^j$ . Из определения функционала  $\mathfrak{S}_{\mathfrak{B}}$  вытекает

$$\mathfrak{S}_{\mathfrak{B}}(O_r^2(x)) = |\Delta_r| \mathfrak{S}_{\mathfrak{B}}(x^r \sum_{j=0}^r o_{r,j} x^{j+r}) = |\Delta_r| \sum_{j=0}^r o_{r,j} m_{j+r}. \quad (6.2.28)$$

Таким образом,

$$|\Delta_{r+1}| = \sum_{j=0}^r o_{r,j} m_{j+r}. \quad (6.2.29)$$

Отсюда следует, что для вычисления определителя  $|\Delta_{r+1}|$ , если известны коэффициенты  $o_{r,j}$  многочлена  $O_r(x)$ , требуется  $O(r)$  операций в поле  $\mathbb{F}_q$ .



Похожим образом вычисляется и коэффициент  $b_r = \frac{1}{|\Delta_{r+1}||\Delta_r|} \mathfrak{S}_{\mathfrak{B}}(x \cdot O_r^2(x))$ . Очевидно,

$$\mathfrak{S}_{\mathfrak{B}}(x \cdot O_r^2(x)) = \mathfrak{S}_{\mathfrak{B}}(o_{r,r}x^{r+1}O_r(x) + o_{r,r-1}x^rO_r(x)) = o_{r,r} \sum_{j=0}^r o_{r,j}m_{j+r+1} + o_{r,r-1} \sum_{j=0}^r o_{r,j}m_{j+r}. \quad (6.2.30)$$

Отсюда также следует, что коэффициент  $b_r$  вычисляется за  $O(r)$  операций в поле  $\mathbb{F}_q$ , если известен многочлен  $O_r(x)$ .

Коэффициент  $\beta_r$  вычисляется очевидным образом.

Таким образом, рекуррентная формула (6.2.26) позволяет вычислить многочлен  $O_{r+1}(x)$ , если известны многочлены  $O_r(x)$ ,  $O_{r-1}(x)$ , за  $O(r)$  операций в поле  $\mathbb{F}_q$ .

Переходя от многочлена  $O_{r+1}(x)$  к многочлену  $O_{r+2}(x)$  и так далее, мы в конечном итоге вычислим ненулевой многочлен  $O_u(x)$ , решив тем самым линейную систему уравнений (6.2.16). Ее решением являются коэффициенты многочлены  $O_u(x)$ . Таким образом, общее число операций в поле  $\mathbb{F}_q$ , требуемых для вычисления многочлена локаторов ошибок  $O_u(x)$  равно  $O(u^2)$ .

Напомним, что рассмотренный алгоритм работает только в случае  $|\Delta_j| \neq 0$ ,  $j = 0, \dots, r+1$ .

### 6.2.5 Как вычислить многочлен $O_u(x)$ , если $|\Delta_r| = 0$ для некоторого $r \leq u-1$ ?

Сначала отметим, что для целей декодирования нам необходим только многочлен  $O_u(x)$ . Поэтому только его мы и будем вычислять. Многочлены  $O_r(x)$ ,  $r < u$ , используются только в промежуточных вычислениях  $O_u(x)$ .

Лемму 6.2.4 мы перепишем в ледующем виде

**Лемма 6.2.6** *Многочлены  $O_r(x)$ ,  $r = 0, \dots, u-1$ , являются ортогональными многочленами, т.е.  $\mathfrak{S}_{\mathfrak{B}}(O_r(x)O_{r'}(x)) = 0$ , если  $r \neq r'$ .*

*Более того,  $\mathfrak{S}_{\mathfrak{B}}(O_r(x)f(x)) = 0$ , если  $\deg f(x) < r$ .*

**Доказательство** непосредственно вытекает из равенства (6.2.20).  $\square$

Лемма 6.2.5 отличается от аналогичной леммы 6.2.4 тем, что многочлены  $O_r(x)$  не обязательно имеют степень равную  $r$ . В частности,  $\mathfrak{S}_{\mathfrak{B}}(O_r^2(x)) = 0$ , если  $\deg O_r(x) < r$ .

Вместо равенства 6.2.23, которое, вообще говоря, не выполнено для многочленов  $O_r(x)$ , мы рассмотрим его аналог. А именно, положим  $O'_{u-1}(x) = O_{u-1}(x)$  и

$$O'_r(x) = \begin{cases} x^r + O_r(x), & \text{если } \deg O_r(x) < r \\ O_r(x), & \text{если } \deg O_r(x) = r \end{cases}, \quad r = 0, \dots, u-2. \quad (6.2.31)$$

Таким образом,  $\deg O'_r(x) = r$ . Заметим, что  $\mathfrak{S}_{\mathfrak{B}}(O_r(x))O'_s(x) = 0$ , если  $r > s$ .

Предположим, что  $O_r(x) \neq 0$ . Очевидно,

$$xO_r(x) = \sum_{k=0}^{r'+1} c_{r,k}O'_k(x) = c_{r,r+1}O'_{r+1}(x) + c_{r,r}O'_r(x) + c_{r,r-1}O'_{r-1}(x), \quad r = 0, \dots, u-2, \quad (6.2.32)$$

где  $r'$  — степень многочлена  $O_r(x)$ . Вычислим постоянные  $c_{r,k}$ .

Умножим левую и правую части равенства (6.2.32) на  $O'_k(x)$  и применим к обеим частям оператор  $\mathfrak{S}_{\mathfrak{B}}$ . В результате получим

$$xO_r(x) = \sum_{k=0}^{r'+1} c_{r,k} O'_k(x) = c_{r,r+1} O'_{r+1}(x) + c_{r,r} O'_r(x) + c_{r,r-1} O'_{r-1}(x), \quad r = 0, \dots, u-2, \quad (6.2.33)$$

Основная идея состоит в том, чтобы преобразовать особым образом моменты  $m_j$  в "новые" моменты  $m'_j$  так, чтобы с одной стороны выполнялись соотношения  $|\Delta'_r| \neq 0$ ,  $j = 0, \dots, u$ , а с другой — так, чтобы многочлен  $O_u(x) = O_u(x, m_0, m_1, \dots, m_{2u-1})$  просто выражались через многочлен  $O'_u(x) = O_u(x, m'_0, m'_1, \dots, m'_{2u-1})$ . Отметим, что связь промежуточных многочленов  $O_r(x)$  и  $O'_r(x)$ ,  $r < u$ , между собой может быть достаточно сложной.

Указанное преобразование моментов можно реализовать различными способами. Один из них изложен ниже.

Если в соотношении (6.2.3) положить  $\beta'_j = \beta_j + \gamma$ , то, моменты  $m_j$ , очевидно, заменятся на моменты

$$m'_j = \sum_{i=0}^j m_i \binom{j}{i} \gamma^{j-i}. \quad (6.2.34)$$

Для многочлена  $O'_u(x) = O_u(x, m'_0, m'_1, \dots, m'_{2u-1})$ , в виду леммы 6.2.3 (равенства (6.2.12) и (6.2.13)), будет справедливо соотношение

$$O'_u(x - \gamma, m'_0, m'_1, \dots, m'_{2u-1}) = C_u O_u(x, m_0, m_1, \dots, m_{2u-1}), \quad C_u \neq 0. \quad (6.2.35)$$

В свою очередь определитель  $|\Delta'_r(\gamma)|$ , где

$$\Delta_r(\gamma) = \begin{pmatrix} m'_0 & m'_1 & \cdots & m'_{r-1} \\ m'_1 & m'_2 & \cdots & m'_r \\ \vdots & \vdots & \cdots & \vdots \\ m'_{r-1} & m'_r & \cdots & m'_{2r-2} \end{pmatrix}, \quad (6.2.36)$$

является, в виду (6.2.35), ненулевым многочленом от переменного  $\gamma$  и поэтому принимает ненулевые значения. Также очевидно, что многочлен  $\prod_{r=1}^{u-1} \Delta_r(\gamma)$  также принимает ненулевые значения.

Это доказывает, что всегда существует элемент  $\gamma$ , принадлежащий некоторому расширению поля  $\mathbb{F}_q$ , такой, что  $|\Delta_r| \neq 0$ ,  $r = 1, \dots, u$ .

Используя соотношение (6.2.24), мы получим соотношение

$$a'_r O'_{r+1}(x) = \quad (6.2.37)$$

## 6.2.6 Формула Кристофеля-Дарбу

Используя формулу Кристоффеля-Дарбу можно понизить число операций, необходимых для вычисления значений ошибок  $k_j$  (см. равенство (6.2.3)) аналогично тому, как это делается с помощью алгоритма Берлекемпа, вычисляющего многочлен локаторов ошибок.

Отметим, что из леммы 6.2.2 следует

$$k_j = -\frac{1}{T_u(\beta_j, \beta_j, \mathfrak{B})}. \quad (6.2.38)$$

Несколько иной путь вычисления значения  $k_j$  ошибок состоит в следующем. Величины  $k_j$  являются решением невырожденной линейной системы уравнений (6.2.3), коэффициенты которой определяются множеством  $\mathfrak{B}$ , а правая часть — значениями моментов  $m_i$ ,  $i = 1, \dots, u$ . Таким образом, решая систему (6.2.3), мы вычислим значений ошибок  $k_j$ , если множество локаторов ошибок  $\mathfrak{B}$  уже вычислено.

Первый из этих путей (соотношение (6.2.38)) требует  $O(u^4)$  операций, а второй (решение системы (6.2.3)) —  $O(u^3)$  операций в поле  $\mathbb{F}_q$ . Формула Кристофеля-Дарбу позволяет понизить эти оценки за счет того, что многочлен  $T_u(x, y, \mathfrak{B})$  можно представить в ином, более удобном для вычисления виде.

**Лемма 6.2.7 (Формула Кристофеля-Дарбу)** *Имеет место соотношение*

$$a_{u-1}(P_u(x)P_{u-1}(y) - P_u(y)P_{u-1}(x)) = (y - x) \sum_{r=0}^{u-1} P_r(x)P_r(y), \quad (6.2.39)$$

где коэффициент  $a_{u-1}$  определяется соотношением (6.2.25).

**Доказательство.** Вместе с соотношением (6.2.24) с неизвестным  $x$  рассмотрим такое же соотношение с неизвестным  $y$ :

$$yP_r(y) = a_r P_{r+1}(y) + b_r P_r(y) + a_{r-1} P_{r-1}(y). \quad (6.2.40)$$

Умножим соотношение (6.2.24) на  $P_r(y)$ , а соотношение (6.2.40) — на  $P_r(x)$  и вычтем одно из другого. В результате получим

$$(y - x)P_r(x)P_r(y) = a_r(P_{r+1}(x)P_r(y) - P_{r+1}(y)P_r(x)) + a_{r-1}(P_{r-1}(x)P_r(y) - P_{r-1}(y)P_r(x)) \quad (6.2.41)$$

Теперь просуммируем соотношение (8.6.13) от  $r = 0$  до  $r = u - 1$ . в результате получим соотношение (6.2.39).  $\square$

Сумму

$$h_u(x, y) = \sum_{r=0}^u P_r(x)P_r(y) \quad (6.2.42)$$

называют полиномиальным ядром степени  $u$ . Она обладает следующим замечательным свойством воспроизведения

$$\mathfrak{S}_{\mathfrak{B}}(h_u(x, y)f(x)) = f(y), \quad \deg f(x) \leq u. \quad (6.2.43)$$

Подобным же свойством обладает, как следует из ее определения, и функция  $T_u(x, y, \mathfrak{B})$ :

$$\mathfrak{S}_{\mathfrak{B}}(T_u(x, y, \mathfrak{B})x^r) = -y^r, \quad r = 0, \dots, u. \quad (6.2.44)$$

(Упражнение) Отсюда следует

**Следствие 6.2.2** *Имеет место соотношение*

$$-T_u(x, y, \mathfrak{B}) = \sum_{r=0}^u P_r(x)P_r(y), \quad x, y \in \mathbb{F}_q, \quad (6.2.45)$$

так, что

$$-T_u(\beta_j, \beta_j, \mathfrak{B}) = \sum_{r=0}^u P_r^2(\beta_j) = \frac{1}{k_j}. \quad (6.2.46)$$

**Доказательство.** Соотношение (6.2.45) вытекает из того, что соотношение (6.2.42) полностью определяет полиномиальное ядро  $h_u(x, y)$ , а соотношение (6.2.44) — многочлен  $T_u(x, y, \mathfrak{B})$ . Поэтому значения функций  $-T_u(x, y, \mathfrak{B})$  и  $h_u(x, y)$  совпадают на  $\mathbb{F}_q \times \mathbb{F}_q$ .

Соотношение (6.2.46) следует из (6.2.38).  $\square$

Соотношение (6.2.46), если считать известными коэффициенты  $a_r, b_r$  в равенстве (6.2.24), позволяет вычислить значение  $h_u(\beta_j, \beta_j)$ , равное  $\frac{1}{k_j}$ , за  $O(u)$  операций в поле  $\mathbb{F}_q$ . Для этого с помощью соотношения (6.2.25) последовательно вычисляем значения  $P_r(\beta_j)$ ,  $r = 1, \dots, u$ , а затем — сумму в правой части (6.2.46). Таким образом, общее число операций, требуемых для вычисления всех значений ошибок  $k_j$ , равно  $O(u^2)$ .

### 6.2.7 Как вычислить число $u$ ошибок, поразивших кодовый вектор?

В настоящем разделе решается следующая задача. Предположим, что нам известна ненулевая рекуррентная последовательность

$$\mathbf{a} = (a_0, a_1, \dots, a_N), \quad a_j \in \mathbb{F}_q, \quad (6.2.47)$$

закон рекурсии у которой неизвестен. Необходимо найти этот закон, т.е. найти многочлен  $g(x) = g_u + g_{u-1}x + \dots + g_1x^{u-1} + x^u \in \mathbb{F}_q[x]$ ,  $g_u \neq 0$ , минимальной степени  $u < N$ , для которого выполнено

$$a_{j+u} = -(a_{j+u-1}g_1 + \dots + a_{j-1}g_{u-1} + a_jg_u), \quad j = 1, \dots, N - u. \quad (6.2.48)$$

Число  $u$  мы называем рекуррентным рангом последовательности  $\mathbf{a}$ . Мы всегда будем предполагать, что числа  $u$  и  $q$  являются взаимно простыми. Из этого предположения, в частности, вытекает, что многочлен  $g(x)$  не имеет кратных корней.

Пусть  $\widehat{g}(x) = x^u g(x^{-1})$  и  $n$  минимальное число, для которого многочлен  $\widehat{g}(x)$  делит многочлен  $x^n - 1$ . Очевидно, такое число  $n$  всегда существует в виду того, что  $g_u \neq 0$ .

В разделе 5.1.2 были рассмотрен циклический код  $\mathfrak{K} \subseteq \mathbb{F}_q^n$  длины  $n$  с порождающим многочленом  $f(x) = \frac{x^n - 1}{\widehat{g}(x)}$ . Как следует из леммы 5.1.3, каждый вектор  $\mathbf{a}$  линейного циклического кода  $\mathfrak{K}$  с порождающим многочленом  $f(x)$  является линейной рекуррентной последовательностью с законом рекурсии (6.2.48).

Поэтому, без ограничения общности, мы будем полагать, что  $N \leq n$ . Из теоремы 5.1.3 вытекает, что последовательность  $\mathbf{a} \in \mathfrak{K}$  быть представлена в виде

$$a_j = \sum_{i=1}^u \alpha_i \theta_i^j, \quad \alpha_i \in \mathbb{F}_{q^n} \setminus \{0\}, \quad j = 0, \dots, n - 1, \quad (6.2.49)$$

где  $\theta_i$  — корни многочлена  $\widehat{g}(x)$ .

Из последнего соотношения вытекает, что элементы  $a_j$  можно рассматривать как моменты масс  $\alpha_i$ , сосредоточенных в точках  $\theta_i$  (см. раздел 6.2.2).

Рассмотрим матрицу Ганкеля

$$\Theta_{r-1}(\mathbf{a}) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{r-1} \\ a_1 & a_2 & \cdots & a_r \\ \vdots & \vdots & \cdots & \vdots \\ a_{r-1} & a_r & \cdots & a_{2r-2} \end{pmatrix}, \quad (6.2.50)$$

которая является аналогом матрицы  $\Delta_{r-1}$  раздела 6.2.2. Как следует из леммы 6.2.1, определитель  $|\Theta_{r-1}(\mathbf{a})|$  матрицы  $\Theta_{r-1}(\mathbf{a})$  при  $r = u$  отличен от нуля, а при  $r > u$   $|\Theta_{r-1}(\mathbf{a})| = 0$ . Если же  $0 < r < u$ , то определитель  $|\Theta_{r-1}(\mathbf{a})|$  может принимать любые значения: как нулевые так и ненулевые. Отсюда непосредственно вытекает

**Лемма 6.2.8** *Если  $u$  — рекуррентный ранг последовательности  $\mathbf{a}$ , то  $u$  последовательности  $(|\Theta_{u-1}(\mathbf{a})|, |\Theta_u(\mathbf{a})|, \dots, |\Theta_r(\mathbf{a})|)$  первая координата отлична от нуля, а все остальные координаты равны 0.*

Лемма, по существу, определяет алгоритм для вычисления ранга  $u$  рекуррентной последовательности  $\mathbf{a}$ . А именно, ранг  $\mathbf{a}$  равен максимальному числу  $u$ , для которого отличен от нуля определитель  $|\Theta_{u-1}(\mathbf{a})|$ .

В частности, одним из возможных способов вычисления коэффициентов  $g_j$  в (6.2.48) состоит в следующем. Сначала находим с помощью вышеописанного алгоритма рекуррентный ранг  $u$  последовательности  $\mathbf{a}$ . Затем вычисляем многочлен  $O_u(x, a_0, a_1, \dots, a_{2u-1})$  (см. (6.2.11)), названный выше многочленом локаторов ошибок. Коэффициенты многочлена  $\frac{1}{\Delta_{u-1}} O_u(x, a_0, a_1, \dots, a_{2u-1}) = g_r + g_{r-1}x + \cdots + g_1x^{r-1} + x^r$  и определяют коэффициенты  $g_j$  в рекуррентном соотношении (6.2.48).

Другой способ вычисления коэффициентов  $g_j$  состоит в следующем. Система (6.2.48), в которой элементы  $g_j$  рассматриваются как неизвестные, имеет единственное решение, так как ее матрица коэффициентов, равная  $\Theta_{u-1}(\mathbf{a})$ , невырождена. Решив эту систему, мы найдем элементы  $g_j$ .

## 6.2.8 Один несидромный алгоритм декодирования кода Рида-Соломона

До сих пор мы рассматривали синдромные алгоритмы, которые вычисляют вектор  $\mathbf{e}$ , исходя из уравнения (6.2.1), а затем и кодовый вектор  $\mathbf{a} = \mathbf{a}' - \mathbf{e}$ . Далее мы рассмотрим простейший вариант алгоритма, который непосредственно вычисляет решение  $\mathbf{x}$  уравнения (6.1.4). Этот алгоритм имеет некоторые общие черты с алгоритмом декодирования Судана, рассматриваемый в следующем разделе.

Будем рассматривать векторы кода Рида-Соломона  $RS_q(n, d)$ ,  $n = q$ , типа 2 как последовательности  $\mathbf{a}_f$  значений многочлена  $f(x)$  степени не выше  $n - d$  во всех точках множества  $\mathcal{A} = \mathbb{F}_q$  (см. следствие 5.0.1). Очевидно, что если известны значения  $a_{\beta_j} = f(\beta_j)$  многочлена  $f(x)$  в любых различных точках  $\beta_j \in \mathbb{F}_q$ ,  $j = 1, \dots, n - d + 1$ , то мы можем вычислить все коэффициенты многочлена  $f(x)$  и восстановить кодовый вектор  $\mathbf{a}_f \in RS_q(n, d)$ . Вычислить многочлен  $f(x)$  можно различными способами.

Во-первых, можно рассматривать равенства  $a_{\beta_j} = f(\beta_j)$ ,  $j = 1, \dots, n - d + 1$  как систему линейных уравнений относительно коэффициентов многочлена  $f(x)$ . Ранг этой системы совпадает с числом  $n - d + 1$  неизвестных (числом коэффициентов многочлена  $f(x)$ ) и поэтому она всегда имеет единственное решение.

Во-вторых, для явного вычисления многочлена  $f(x)$  можно использовать хорошо известную, так называемую, интерполяционную формулу. Поясним подробнее, что это такое.

Рассмотрим многочлены  $r(x) = \prod_{j=1}^{n-d+1} (x - \beta_j)$  и  $r_j(x) = \frac{r(x)}{x - \beta_j}$ ,  $j = 1, \dots, n - d + 1$ . Очевидно,  $\gamma_j = r_j(\beta_j) \neq 0$ , и  $r_j(\beta_i) = 0$ , если  $i \neq j$ .

Следующее соотношение однозначно определяет многочлен  $f(x)$  степени не выше  $n - d$ , который принимает значение  $a_{\beta_j}$  в точке  $\beta_j$ ,  $j = 1, \dots, n - d + 1$ :

$$f(x) = \frac{a_{\beta_1}}{\gamma_1} r_1(x) + \frac{a_{\beta_2}}{\gamma_2} r_2(x) + \dots + \frac{a_{\beta_{n-d+1}}}{\gamma_{n-d+1}} r_{n-d+1}(x). \quad (6.2.51)$$

Предположим, что мы, используя результаты раздела (6.2.7), вычислили число ошибок  $u = wt(\mathbf{e})$ , поразивших вектор  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$ ,  $\mathbf{a} \in RS_q(n, d)$ , а затем и многочлен локаторов ошибок  $O_u(x, b_0, \dots, b_{2u-1})$  или  $F_{\mathfrak{B}}(x)$  (см. раздел (6.2.3)).

Пусть  $\beta \in \mathcal{A} \subseteq \mathbb{F}_q$  и  $O_u(\beta, b_0, \dots, b_{2u-1}) \neq 0$ . Это означает, что  $\beta \notin \mathfrak{B}$ , т.е., что координата искаженного вектора  $\mathbf{a}'$ , индексированная элементом  $\beta$ , принимает правильное значение. Последовательно перебирая элементы поля  $\mathbb{F}_q = \mathcal{A}$ , найдем  $n - d + 1$  элементов  $\beta_j \in \mathcal{A}$ , для которых координата  $a_{\beta_j}$  вектора  $\mathbf{a}'$  принимает правильное значение. Это позволяет вычислить многочлен  $f(x)$  и тем самым кодовую последовательность  $\mathbf{a}$ , не вычисляя вектор ошибок  $\mathbf{e}$ .

## 6.2.9 Краткий обзор некоторых результатов по декодированию кодов Рида-Соломона

Важнейшей проблемой в декодировании кода Рида-Соломона является его декодирование за пределами кодового расстояния, т.е. при числе ошибок  $t$  большем  $\frac{d-1}{2}$ , с полиномиальной относительно его длины сложностью. Этой проблеме за последние 10 лет посвящено значительное число работ и получены весьма интересные результаты. Две из них [31] (В.М. Сидельников) и [63] (В. Гурусвами, М. Судан) мы без каких-либо доказательств рассмотрим в данном разделе.

### Алгоритм декодирования Гурусвами-Судана

Пусть  $\mathbf{a}' = \mathbf{a} + \mathbf{e}$  — вектор кода Рида-Соломона  $\mathfrak{K}(B_{\mathcal{A}}^{(d)}) = RS_q(n, d)$ ,  $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$ , (см. раздел 5.0.3) на выходе комбинаторного канала связи, в котором происходит не более, чем  $t$ , т.е.  $wt(\mathbf{e}) \leq t$ . Мы не предполагаем, что  $d \geq 2t + 1$ , т.е. мы рассматриваем, вообще говоря, декодирование за пределами кодового расстояния кода Рида-Соломона. Естественно, что алгоритм Судана работает правильно, если число  $t$  некоторым образом ограничено сверху. Подобная оценка будет приведена далее.

Мы полагаем, что

$$\mathbf{a} = (a_1, \dots, a_n) = (f(\alpha_1), \dots, f(\alpha_n)), \quad (6.2.52)$$

т.е. предполагаем, что координаты кодового вектора  $\mathbf{a} \in RS_q(n, d)$  являются значениями многочлена  $f(x)$  степени не выше  $s = n - d$  в точках множества  $\mathcal{A}$  (см. следствие 5.0.1).

Обозначим через  $c_j$   $j$ -ую координату вектора  $\mathbf{a}'$ , т.е.  $c_j = a_j + e_j$ . Рассмотрим множество пар  $\mathcal{P} = \{(a_1, c_1), \dots, (a_n, c_n)\}$  как подмножество точек двумерного пространства  $\mathbb{F}_q \times \mathbb{F}_q$ .

Пусть  $D(x, y) \in \mathbb{F}_q[x, y]$  — многочлен от двух переменных. Мы говорим, что множество  $\mathcal{P}$  проходит через многочлен  $D(x, y)$ , если  $D(a_j, c_j) = 0$  для всех  $j = 1, \dots, n$ .

Если  $\mathbf{e} = 0$ , т.е. ошибок нет, то множество  $\mathcal{P}$ , очевидно, проходит через многочлен вида  $y - f(x)$ , где  $f(x)$  — многочлен, который определяет кодовый вектор  $\mathbf{a}$  в соответствии с соотношением (6.2.52).

Если  $F(x)$  — один из многочленов локаторов ошибок для вектора  $\mathbf{a}'$ , то то множество  $\mathcal{P}$ , очевидно, проходит через многочлен вида  $F(x)(y - f(x))$ ,  $\deg F(x) \leq t$ ,  $\deg f(x) \leq n - d$ . Заметим, что уравнение (6.1.4) в случае  $d < 2t + 1$  может иметь несколько решений  $(\mathbf{a}, \mathbf{e})$ , поэтому последний многочлен определен неоднозначно.

Таким образом, всегда найдется многочлен  $D(x, y)$  вида

$$D(x, y) = R(x, y)(y - f(x)), \quad \deg f(x) \leq n - d, \quad (6.2.53)$$

у которого многочлен  $(y - f(x))$  проходит через максимально возможное число точек множества  $\mathcal{P}$ .

Многочлен  $D(x, y)$ , проходящий через множество точек  $\mathcal{P}$ , может быть найден с помощью решения, так называемой, задачи интерполяции его значений в заданных точках, наподобие уже рассмотренной задачи в разделе 6.2.8 построения многочлена от двух переменных наименьшей степени одной переменной, принимающих заданное значение в заданных точках. А именно, мы хотим найти коэффициенты многочлена в некотором смысле наименьшей степени, у которого значения в точках множества  $\mathcal{P}$  равны нулю.

Очень важной проблемой является определение понятия "степень многочлена  $\Lambda(x, y)$ " от двух переменных. Обычное его определение как  $\max i + j$ , где максимум берется по всем моном  $x^i y^j$ , входящим с ненулевым коэффициентом в многочлен  $\Lambda(x, y)$ , не подходит: из соотношения (6.2.53) мы видим, что степень по переменной  $x$  и переменной  $y$  у многочлена  $D(x, y)$ , который мы хотим построить, существенно различны: степень по  $x$  примерно в  $n - d$  раз выше степени по  $y$ . Поэтому, если использовать обычное определение степени многочлена, то мы будем получать в качестве решения интерполяционной задачи многочлены, которые не могут быть представлены в виде (6.2.53).

**Определение 6.2.1** Пусть  $\Lambda(x, y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \omega_{i,j} x^i y^j$  — многочлен над полем  $\mathbb{F}_q$  и  $s, u$  — целые числа.  $(s, u)$ -степень  $N_{s,u}$  многочлена  $\Lambda(x, y)$  мы определим как  $\max is + ju$ , где максимум берется по всем парам  $(i, j)$  таким, что  $\omega_{i,j} \neq 0$ .

В случае  $u = s = 1$   $N_{1,1}$  — это обычная степень многочлена  $\Lambda(x, y)$ . Далее мы будем рассматривать только случай  $s = n - d$ ,  $u = 1$ .

Размерность пространства многочленов, образованное всеми многочленами,  $(s, 1)$ -степень которых не превосходит  $h$ , мы обозначаем через  $N_{s,1}(h)$ . Таким образом,  $N_{s,1}(h)$  — число мономов  $x^i y^j$ , у которых  $is + j \leq h$ . Вычисление числа  $N_{s,1}(h)$  является делом не очень сложным. Вместе с тем делать мы этого не будем. Отметим только, что при больших  $h$  число  $N_{s,1}(h)$  приблизительно равно  $\frac{h^2}{2s}$ .

Нашей задачей является построение многочлена  $D_{\mathcal{P}}(x, y)$  с наименьшей  $(s, 1)$ -степенью  $h$ , который проходит через все точки множества  $\mathcal{P}$ .

Коэффициенты  $\omega_{i,j}$  многочлена  $\Lambda(x, y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \omega_{i,j} x^i y^j$ , у которого  $(s, 1)$ – степень не превосходит  $h$  и который проходит через все точки множества  $\mathcal{P}$ , удовлетворяют следующей системе линейных уравнений

$$\sum_{ui+j \leq h} \omega_{i,j} \alpha^i \beta^j = 0 \text{ для всех } (\alpha, \beta) \text{ из множества } \mathcal{P}. \quad (6.2.54)$$

Система (6.2.54) имеет  $N_{s,1}(h)$  неизвестных  $\omega_{i,j}$  и  $n = |\mathcal{P}|$  уравнений. Предположим что число  $h$  выбрано так, что система (6.2.54) имеет одно (или небольшое число) решение, которое определяет многочлен  $\mathcal{Q}_{\mathcal{P}}(x, y)$ . Очевидно, для этого достаточно предположить, что  $N_{s,1}(h) \geq n$ .

Вычислив многочлен  $\mathcal{Q}_{\mathcal{P}}(x, y)$ , мы находим все его множители вида  $y - f(x)$ ,  $\deg f(x) < s$ . Это относительно простая задача, выполняемая за полиномиальное время. На этот счет имеется обширная литература.

Каждый многочлен  $f(x)$  определяет кодовый вектор  $\mathbf{a}_f$  в соответствии с соотношением (6.2.52). Список всех таких  $\mathbf{a}_f$  мы обозначим через  $\mathcal{L}(\mathcal{Q}_{\mathcal{P}}(x, y))$ .

Основное утверждение, полученное Суданом состоит в следующем.

**Теорема 6.2.1** Пусть  $\mathbf{a}'$  — искаженный кодовый вектор кода Руда-Соломона  $RS_q(n, d)$ .

Тогда список  $\mathcal{L}(\mathcal{Q}_{\mathcal{P}}(x, y))$  содержит все кодовые векторы, отстоящие от  $\mathbf{a}'$  на расстояние меньшее, чем

$$n - \delta > \left\lceil n \left( 1 - \sqrt{2R} \right) \right\rceil = n - \sqrt{2n(n-d)}, \quad (6.2.55)$$

где  $R = \frac{n-d}{n}$  — скорость передачи с помощью кода  $RS_q(n, d)$  и  $\delta$  — наименьшее целое такое, что  $N_{s,1}(\delta) > \frac{n}{2}$ .

Следует отметить, что теорема может быть усилена. Для этого вместо многочлена  $\mathcal{Q}_{\mathcal{P}}(x, y)$  рассматривается подобный многочлен  $\mathcal{Q}_{\mathcal{P},m}(x, y)$ , который определяется тем, что он проходит через каждую точку множества  $\mathcal{P}$  с кратностью  $m$ .

Можно показать, что если

$$N_{s,1} > \frac{nm(m-1)}{2}, \quad (6.2.56)$$

то существует ненулевой многочлен  $\mathcal{Q}_{\mathcal{P},m}(x, y)$ , проходящей через каждую точку множества  $\mathcal{P}$  с кратностью  $m$ .

Если в теореме 6.2.1 вместо многочлена  $\mathcal{Q}_{\mathcal{P}}(x, y)$  использовать многочлен  $\mathcal{Q}_{\mathcal{P},m}(x, y)$ , то получим

**Теорема 6.2.2 (Теорема Гурусвами-Судана)** Пусть  $\mathbf{a}'$  — искаженный кодовый вектор кода Руда-Соломона  $RS_q(n, d)$ .

Тогда список  $\mathcal{L}(\mathcal{Q}_{\mathcal{P},m}(x, y))$  содержит все кодовые векторы, отстоящие от  $\mathbf{a}'$  на расстояние меньшее, чем

$$n - \left\lceil \frac{\delta}{m} \right\rceil > \left\lceil n \left( 1 - \sqrt{R \frac{m+1}{m}} \right) \right\rceil = n - \sqrt{\frac{m+1}{m} n(n-d)}, \quad (6.2.57)$$

где  $R = \frac{n-d+1}{n}$  — скорость передачи с помощью кода  $RS_q(n, d)$  и  $\delta$  — наименьшее целое такое, что  $N_{s,1}(\delta) > \frac{n}{2}$ .



Эта теорема показывает, что если  $m \rightarrow \infty$ , то алгоритм позволяет корректировать ошибки, произошедшие в  $t < n - n\sqrt{R}$  разрядах кодового вектора. Заметим, что декодирование в пределах кодового расстояния, позволяет корректировать ошибки, произошедшие только в  $t < \frac{n(1-R)}{2} = \frac{d}{2}$  разрядах кодового вектора, т.е. алгоритм декодирования Гурусвами-Судана позволяет исправлять существенно большее число ошибок, чем  $\frac{d}{2}$  — число ошибок, которые корректируются традиционными алгоритмами, изложенными в разделе 6.

## Обобщение понятия многочлен локаторов ошибок. Результаты работы [31]

В разделе 6.2.3 был в явном виде представлен (равенство (6.2.11)) многочлен локаторов ошибок  $O_u(x, m_0, m_1, \dots, m_{2u-1})$ , корнями которого являются элементы  $\beta_j$ , если моменты  $m_i$ ,  $i = 0, \dots, 2u - 1$  могут быть представлены в виде

$$m_i = \sum_{j=1}^u k_j \beta_j^i, \quad k_j \in \overline{\mathbb{F}}_q \setminus \{0\}, \quad u \geq 1, \quad i = 0, \dots, 2u - 1, \quad (6.2.58)$$

с некоторыми элементами  $k_j$ , принадлежащими некоторому расширению  $\overline{\mathbb{F}}_q$  поля  $\mathbb{F}_q$ . Отметим, что многочлен  $O_u(x, m_0, m_1, \dots, m_{2u-1})$  определяется всеми  $2u$  первыми моментами  $m_i$  и может быть выписан только в случае, если все они известны. Если же число известных первых моментов меньше, чем  $2u$ , то при заданном  $u$  элементы  $\beta_j$ , вообще говоря определяются неоднозначно.

Пусть  $\mathfrak{N}_{u,r} = \mathfrak{N}(m_0, m_1, \dots, m_{2u-r})$  — множество всех  $u$ -элементных множеств  $\mathfrak{B} = \{\beta_1, \dots, \beta_u\} \subseteq \overline{\mathbb{F}}_q$ , для которых существуют элементы  $k_j \in \overline{\mathbb{F}}_q \setminus \{0\}$ , для которых выполнены соотношения (6.2.58) для  $i = 0, \dots, 2u - r$ . Эти множества  $\mathfrak{B}$  мы называем  $u$ -решениями уравнения (6.2.58). Таким образом,  $\mathfrak{N}_{u,r}$  — множество всех  $u$ -решений уравнения (6.2.58).

В работе автора [31] выписан в явном виде симметрический многочлен  $O_{u,r}(x_1, \dots, x_r) = O_u(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r}) \in \mathbb{F}_q[x_1, \dots, x_r]$  от  $r$  переменных степени  $u - r + 1$  по каждому переменному, который обладает следующими свойствами.

- Если  $\mathfrak{B} \subseteq \mathfrak{N}_{u,r}$ , то любое  $r$ -элементное подмножество  $\mathfrak{C} = \{\beta_{j_1}, \dots, \beta_{j_r}\} \subseteq \mathfrak{B}$  множества  $\mathfrak{B}$  является нулем многочлена  $O_u(x_1, \dots, x_r)$ , т.е.  $O_{u,r}(\beta_{j_1}, \dots, \beta_{j_r}) = 0$ .
- Если
  - а)  $\mathfrak{C} = \{\beta_{j_1}, \dots, \beta_{j_r}\}$  —  $r$ -элементное подмножество  $\overline{\mathbb{F}}_q$  является нулем многочлена  $O_u(x_1, \dots, x_r)$ ,
  - б) степень многочлена  $O_u(\beta_{j_1}, \dots, \beta_{j_{r-1}}, x)$  равна  $u - r + 1$ ,
  - с) корни многочлена  $O_{u,r}(\beta_{j_1}, \dots, \beta_{j_{r-1}}, x)$  различны и отличны от  $\beta_{j_1}, \dots, \beta_{j_{r-1}}$ , тогда найдется  $u$ -элементное множество  $\mathfrak{B} \in \mathfrak{N}_{u,r}$  такое, что  $\mathfrak{B} = \mathfrak{C} \cup \mathfrak{D}_O$ , где  $\mathfrak{D}_O$  — множество корней многочлена  $O_{u,r}(\beta_{j_1}, \dots, \beta_{j_{r-1}}, x)$ .
- Если  $\mathfrak{C} = \{\beta_{j_1}, \dots, \beta_{j_r}\}$  — корень многочлена  $O_{u,r}(x_1, \dots, x_r)$  и многочлен  $O_{u,r}(\beta_{j_1}, \dots, \beta_{j_{r-1}}, x)$  тождественно равен нулю, то найдется множество  $\mathfrak{D}$  с меньшим, чем  $u - r$  числом элементов, для которого множество  $\mathfrak{B} = \mathfrak{C} \cup \mathfrak{D}$  с меньшим, чем  $u$  числом элементов, является решением уравнений (6.2.58) для  $i = 0, \dots, 2u - r$ .

- Если  $\mathfrak{C} = \{\beta_{j_1}, \dots, \beta_{j_r}\}$  — корень многочлена  $O_{u,r}(x_1, \dots, x_r)$  и степень ненулевого многочлена  $O_{u,r}(\beta_{j_1}, \dots, \beta_{j_{r-1}}, x)$  меньше  $u - r + 1$ , то решений  $\mathfrak{B}$  уравнения (6.2.58) для  $i = 0, \dots, 2u - r$ , которые включают в себя множество  $\mathfrak{C} \setminus \{\beta_{j_r}\}$ , не существует.

Рассмотрим многочлен

$$D_{u,r}(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r}) = \begin{vmatrix} 1 & \cdots & 1 & m_0 & \cdots & m_{u-r} \\ x_1 & \cdots & x_r & m_1 & \cdots & m_{u-r+1} \\ x_1^2 & \cdots & x_r^2 & m_2 & \cdots & m_{u-r+2} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ x_1^u & \cdots & x_r^u & m_u & \cdots & m_{2u-r} \end{vmatrix} \quad (6.2.59)$$

Предположим, что  $D_{u,r}(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r})$  является многочленом степени  $u$  по каждой переменной  $x_j$ . Определим многочлен  $O_{u,r}(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r})$  с помощью соотношения

$$O_{u,r}(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r}) = \left( \prod_{i < j} (x_i - x_j) \right)^{-1} D_{u,r}(x, m_0, m_1, \dots, m_{2u-r}). \quad (6.2.60)$$

Заметим, что многочлен  $O_{u,r}(x_1, \dots, x_r, m_0, m_1, \dots, m_{2u-r})$  несомненно является обобщением многочлена локаторов ошибок из раздела 6.2.3, соотношение (6.2.11). Вместе с тем до конца не ясно как наиболее эффективно его использовать для декодирования кода Рида-Соломона.

# Глава 7

## Коды Рида-Маллера

Мы рассматриваем только классические двоичные коды Рида-Маллера. Следует также сказать, что известны несколько классов кодов, которые можно рассматривать как обобщением классических двоичных кодов Рида-Маллера на  $q$ -значный случай. Эти коды мы не рассматриваем.

### 7.0.10 Булевы функции и многочлены Жегалкина

Через  $\mathbb{F}_2^m$  мы обозначаем множество всех двоичных векторов длины  $n$ . Множество  $\mathbb{F}_2^m$  является  $m$ -мерным линейным пространством над полем  $\mathbb{F}_2$  в обычном понимании этого понятия. Элементы  $\mathbb{F}_2^m$  мы обозначаем полужирными буквами:  $\mathbf{a} = (a_1, \dots, a_m)$ ,  $\mathbf{x} = (x_1, \dots, x_m)$  и т.п.

Булевой функцией  $f(\mathbf{x})$  называется функция, отображающая множество  $\mathbb{F}_2^m$  (или в другой терминологии линейное пространство) в множество  $\mathbb{F}_2$  (конечное поле) из двух элементов. Коротко это обозначается так:  $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ .

Очевидно, каждая булева функция  $f(\mathbf{x})$  может быть задана таблицей ее значений, т.е. таблицей, в каждой строке которой расположен вектор  $\mathbf{a} \in \mathbb{F}_2^m$  и соответствующее этому вектору значение булевой функции  $f(\mathbf{a}) \in \mathbb{F}_2$ . Число различных строчек таблицы равно  $2^m$  — числу элементов пространства  $\mathbb{F}_2^m$ .

Число различных булевых функций равно  $2^{2^m}$ . Это непосредственно вытекает из табличного задания булевой функции.

Множество всех булевых функций является линейным пространством  $LP_m$  над полем  $\mathbb{F}_2$  размерности  $2^m$ . Скажем несколько слов о способах представления и естественных базисах пространства  $LP_m$ .

Очевидным и часто очень полезным способом представления элементов пространства  $LP_m$  является его представление в виде векторов значений булевых функций. Для того, чтобы явно построить одно из таких представлений, мы упорядочим каким-либо образом элементы  $m$ -мерного пространства  $\mathbb{F}_2^m$ , т.е. запишем множество  $\mathbb{F}_2^m$  в виде последовательности  $m$ -мерных векторов:  $\{\alpha_0, \dots, \alpha_{2^m-1}\} = \mathbb{F}_2^m$ . Порядок следования элементов множества  $\{\alpha_0, \dots, \alpha_{2^m-1}\}$ , как правило, не существен. Главное то, что он (порядок) зафиксирован.

В этом случае булевой функции  $f(\mathbf{x})$  мы сопоставляем вектор ее значений

$$\overline{f(\mathbf{x})} = (f(\alpha_0), \dots, f(\alpha_{2^m-1})). \quad (7.0.1)$$

Мы говорим, что вектор  $\overline{f(\mathbf{x})}$  представляет функцию  $f(x_1, \dots, x_m)$ . И наоборот, вектор  $\mathbf{a} \in \mathbb{F}_2^m$  представляет булеву функцию  $f(\mathbf{x})$ , если  $\mathbf{a} = \overline{f(\mathbf{x})}$ .

Вес  $wt(f(\mathbf{x}))$  вектора  $\overline{f(\mathbf{x})}$  называется также весом булевой функции  $f(\mathbf{x})$  и обозначается как  $wt(f(\mathbf{x}))$ . Таким образом  $wt(f(\mathbf{x}))$  — это число значений функции  $f(\mathbf{x})$  равных 1, когда  $\mathbf{x}$  пробегает все элементы пространства  $\mathbb{F}_2^m$ .

Далее под пространством  $LP_m$  будем понимать  $2^m$ -мерное пространство, образованное всеми векторами вида (7.0.1). Каждому вектору из  $LP_m$  соответствует булева функция, для которой этот вектор является ее вектором значений.

Координаты векторов из  $LP_m$  будем нумеровать элементами пространства  $\mathbb{F}_2^m$ . Таким образом,  $j$ -ой координатой вектора  $(a_{\alpha_0}, \dots, a_{\alpha_{2^m-1}}) \in LP_m$  является координата  $a_\alpha$ , для которой  $\alpha = \alpha_j$ .

Другим естественным базисом пространства  $LP_m$  является базис  $\Omega_m$ , образованный векторами

$$\omega_{\mathbf{a}} = (f_{\mathbf{a}}(\alpha_0), \dots, f_{\mathbf{a}}(\alpha_{2^m-1})), \quad \mathbf{a} \in \mathbb{F}_2^m, \quad (7.0.2)$$

где  $f_{\mathbf{a}}(\mathbf{x})$  — булева функция, для которой  $f_{\mathbf{a}}(\alpha) = 1$ , если  $\mathbf{a} = \alpha$ , и  $f_{\mathbf{a}}(\alpha) = 0$ , если  $\alpha \neq \mathbf{a}$ . Другими словами, у вектора  $\omega_{\mathbf{a}}$  координата, индексированная элементом  $\mathbf{a}$ , равна 1, а все остальные равны 0.

Еще одним естественным базисом пространства  $LP_m$  является базис, связанный с многочленами Жегалкина, к изучению которых мы и переходим.

Многочленом Жегалкина  $f(x_1, \dots, x_m)$  в России принято называть обычный многочлен  $f(\mathbf{x}) \in \mathbb{F}_2[x_1, \dots, x_m]$  от  $m$  переменных с коэффициентами из поля  $\mathbb{F}_2$ . Очевидно, каждый многочлен Жегалкина  $f(\mathbf{x})$  можно трактовать как булеву функцию, значения которой на наборе  $\mathbf{x}$  совпадают со значениями этого многочлена в точке  $\mathbf{x}$ .

В виду того, что  $x^2 = x$  при  $x \in \mathbb{F}_2$ , то в качестве многочленов Жегалкина, рассматриваемых как булевы функции, можно рассматривать только многочлены, которые являются суммой мономов вида  $x_{i_1} \cdots x_{i_k}$ , в которых каждая переменная входит в первой степени. Таким образом, каждый многочлен Жегалкина  $f(x_1, \dots, x_m)$  может быть записан в виде

$$f(x_1, \dots, x_m) = \sum_{k=0}^m \sum_{1 \leq i_1 < \dots < i_k \leq m} a_{i_1, \dots, i_k} x_{i_1} \cdots x_{i_k}, \quad a_{i_1, \dots, i_k} \in \mathbb{F}_2. \quad (7.0.3)$$

Заметим, что в последней сумме сложение осуществляется в поле  $\mathbb{F}_2$  (по mod 2). Таким образом, каждый многочлен Жегалкина является булевой функцией. Верно и обратное утверждение: каждая булева функция может быть представлена в виде (7.0.3).

В частности, многочлен Жегалкина

$$\mathbf{x}^{(\mathbf{a})} = x_1^{(a_1)} \cdots x_m^{(a_m)}, \quad \text{где } x^{(a)} = \begin{cases} x, & \text{если } a = 1, \\ \bar{x} = x + 1, & \text{если } a = 0 \end{cases}, \quad (7.0.4)$$

является булевой функцией, которая, как легко установить, принимает значение 1, если  $\mathbf{x} = \mathbf{a}$ , и  $\mathbf{x}^{(\mathbf{a})} = 0$ , если  $\mathbf{x} \neq \mathbf{a}$ .

**Теорема 7.0.3** *Каждая булева функция  $f(x_1, \dots, x_m)$  может быть представлена единственным образом в виде многочлена Жегалкина.*

**Доказательство.** Очевидно,

$$f(x_1, \dots, x_m) = \sum_{f(\mathbf{a})=1} \mathbf{x}^{(\mathbf{a})}, \quad (7.0.5)$$

где суммирование в сумме производится по всем  $\mathbf{a} \in \mathbb{F}_2^m$ , для которых  $f(\mathbf{a}) = 1$ . Это соотношение доказывает, что каждая булева функция представима в виде многочлена Жегалкина.

Единственность вытекает из того, что размерности пространства, образованного всеми булевыми функциями, совпадает с размерностью пространства образованного всеми многочленами Жегалкина.  $\square$

Как следует из теоремы 7.0.3, пространство многочленов Жегалкина  $LG_m = \mathbb{F}_2[x_1, \dots, x_m]$  изоморфно пространству  $LG_m$ . Из соотношения (7.0.5) следует, что многочлены  $\mathbf{x}^{(\mathbf{a})}$ ,  $\mathbf{a} \in \mathbb{F}_2^m$  образуют базис  $\Omega_m$  пространства  $LG_m$ , который мы обозначили тем же символом, что и уже рассмотренный базис пространства  $LP_m$ .

**Следствие 7.0.3** Множество  $\Xi_m$ , образованное всеми мономами  $x_{i_1} \cdots x_{i_k}$ ,  $1 \leq i_1 < \dots < i_k \leq m$ ,  $k = 0, \dots, m$ , является базисом пространства  $LG_m$ .

**Доказательство.** Множество  $\Xi_m$  действительно является базисом  $LG_m$ , ибо, по определению, каждый многочлен Жегалкина представим в виде (7.0.3) и  $|\Xi_m| = \sum_{k=0}^m \binom{m}{k} = 2^m = \dim LG_m = \dim LP_m$ .  $\square$

Базис  $\Xi_m$  называется мономимальным базисом пространства  $LG_m$  и является другим, отличным от  $\Omega_m$ , естественным базисом пространства  $LG_m$ .

Матрица перехода от базиса  $\Xi_m$  к базису  $\Omega_m$  пространства  $LG_m$  представляет собой  $2^m \times 2^m$  — матрицу  $R$ , каждая строка которой представляет собой вектор-строку значений одного из мономов  $x_{i_1} \cdots x_{i_k}$ . (Упражнение) По существу, матрица  $R$  осуществляет переход от векторов, координатами которых являются коэффициенты  $a_{i_1, \dots, i_k}$  многочлена Жегалкина  $g(\mathbf{x})$ , к вектору  $\overline{g(\mathbf{x})}$ , координатами которого являются значения функции  $g(\mathbf{x})$ .

Степенью  $\deg x_{i_1} \cdots x_{i_k}$  монома  $x_{i_1} \cdots x_{i_k}$  называется число  $k$  — число входящих в него переменных. Степень  $\deg g(\mathbf{x})$  многочлена Жегалкина  $g(\mathbf{x})$  определяется как максимальная степень монома, входящего в многочлен  $g(\mathbf{x})$  с ненулевым коэффициентом  $a_{i_1, \dots, i_k}$  (см. (7.0.3)).

## 7.0.11 Элементарные свойства кода Риды-Маллера

**Определение 7.0.2 (Кода Риды-Маллера)** Подпространство пространства  $\mathbb{F}_2^{2^m}$ , образованное векторами значений многочленов Жегалкина, степень которых не превосходит  $r$ , называется двоичным кодом Риды-Маллера длины  $N = 2^m$  и порядка  $r$  (сокращенно  $RM$ -кодом) и обозначается через  $RM_{r,m}$  или короче — через  $RM_r$ .

Можно сказать и несколько иначе и короче: подпространство (код)  $RM_{r,m}$  образовано всеми векторами  $\overline{g(\mathbf{x})}$ , у которых  $\deg g(\mathbf{x}) \leq r$ .

Множество всех булевых функций  $g(\mathbf{x})$  от  $m$  переменных, у которых  $\deg g(\mathbf{x}) \leq r$ , будем обозначать через  $\widehat{RM}_{r,m}$

**Теорема 7.0.4** Кодовое расстояние  $d$  и размерность  $k$   $RM$ -кода  $RM_{r,m}$  равны  $d = 2^{m-r}$  и  $k = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$ , соответственно.

**Доказательство.** Утверждение теоремы об размерности  $RM$ -кода следует из того, что базис подпространства, образованного многочленами, степень которых не превосходит  $r$ , состоит из всех мономов  $x_{i_1} \dots x_{i_k}$ ,  $0 \leq k \leq r$ . Очевидно, число таких мономов равно  $\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$ .

Переходим к доказательству утверждения о кодовом расстоянии. Согласно Лемме 14.3.1 достаточно показать, вес  $wt(\overline{f(\mathbf{x})})$  ненулевого вектора  $\overline{f(\mathbf{x})} \in RM_r$  (вес функции  $f(\mathbf{x})$ ) не менее  $2^{m-r}$ .

Доказательство проведем индукцией по  $m$  и  $r$ . Если  $m = 1$ , то утверждение теоремы проверяется непосредственно. Пусть теперь утверждение теоремы выполнено для всех  $m' < m$  и всех  $r' \leq r$ .

Каждую булеву  $f(x_1, \dots, x_m) \neq 0$  функцию представим в виде

$$f(x_1, \dots, x_m) = x_1 f(1, x_2, \dots, x_m) + (x_1 + 1) f(0, x_2, \dots, x_m). \quad (7.0.6)$$

(Упражнение.)

Координаты вектора  $\overline{f(\mathbf{x})}$ , которые мы индексировали элементами пространства  $\mathbb{F}_2^m$ , разделим на две части: координаты, у которых  $x_1 = 1$ , и координаты, у которых  $x_1 = 0$ .

Отсюда,

$$wt(f(x_1, x_2, \dots, x_m)) = wt(f(1, x_2, \dots, x_m)) + wt(f(0, x_2, \dots, x_m)). \quad (7.0.7)$$

Если обе функции  $f(1, x_2, \dots, x_m)$  и  $f(0, x_2, \dots, x_m)$  являются ненулевыми, то отсюда и из индуктивного предположения вытекает, что  $wt(f(x_1, x_2, \dots, x_m)) \geq 2^{m-1-r} + 2^{m-1-r} = 2^{m-r}$ .

Если  $f(0, x_2, \dots, x_m) = 0$ , то из равенства (7.0.6) следует, что  $\deg f(1, x_2, \dots, x_m) \leq r - 1$ . Отсюда и из индуктивного предположения вытекает, что  $wt(f(\mathbf{x})) \geq 2^{m-r}$ .

Совершенно аналогично доказывается, что  $wt(f(\mathbf{x})) \geq 2^{m-r}$ , если  $f(1, x_2, \dots, x_m) = 0$ .  $\square$

**Лемма 7.0.9** Пусть  $l_1(\mathbf{x}), \dots, l_s(\mathbf{x})$ ,  $s \leq m$ , — набор линейных функций.

Тогда

$$\sum_{\mathbf{x} \in \mathbb{F}_2^m} l_1(\mathbf{x}) \dots l_s(\mathbf{x}) = \begin{cases} 0, & \text{если } s < m, \text{ либо, если } s = m \text{ и функции } l_1(\mathbf{x}), \dots, l_s(\mathbf{x}) \\ & \text{являются линейно-зависимыми,} \\ 1, & \text{если } s = m \text{ и функции } l_1(\mathbf{x}), \dots, l_s(\mathbf{x}) \\ & \text{являются линейно-независимыми} \end{cases}. \quad (7.0.8)$$

**Доказательство.** Второе равенство в (7.0.16) следует из того, что линейная система уравнений  $l_j(\mathbf{x}) = 1$ ,  $j = 1, \dots, m$ , имеет только одно решение, поэтому в сумме  $\sum_{\mathbf{x} \in \mathbb{F}_2^m} l_1(\mathbf{x}) \dots l_s(\mathbf{x})$  имеется только одно ненулевое слагаемое, равное 1.

Предположим теперь, что  $s < m$ . Как нетрудно установить (Упражнение), что

$$\sum_{\mathbf{x} \in \mathbb{F}_2^m} x_{i_1} \dots x_{i_s} = \begin{cases} 0, & \text{если } s < m, \\ 1, & \text{если } s = m \end{cases}. \quad (7.0.9)$$

Поэтому  $\sum_{\mathbf{x} \in \mathbb{F}_2^m} l_1(\mathbf{x}) \cdots l_s(\mathbf{x}) = 0$ .

Предположим теперь, что  $s = m$  и функции  $l_j(\mathbf{x}) = 1$ ,  $j = 1, \dots, m$ , являются линейно-зависимыми (над полем  $\mathbb{F}_2$ ),  $l_m(\mathbf{x}) = \sum_{j=1}^{m-1} a_j l_j(\mathbf{x})$ ,  $a_j \in \mathbb{F}_2$ . Отсюда следует (Упражнение), что  $l_1(\mathbf{x}) \cdots l_m(\mathbf{x}) = l_1(\mathbf{x}) \cdots l_{m-1}(\mathbf{x}) \sum_{j=1}^{m-1} a_j$ , т.е. в этом случае произведение  $l_1(\mathbf{x}), \dots, l_m(\mathbf{x})$  совпадает с произведением линейных функций с меньшим, чем  $m$  сомножителей. Это доказывает первое равенство в (7.0.16).  $\square$

**Теорема 7.0.5** Кодом, двойственным к коду  $RM_{r,m}$  является код  $RM_{m-r-1,m}$ .

**Доказательство.** Покажем, что для любого  $\mathbf{x} = \overline{f(x_1, \dots, x_m)} \in RM_{r,m}$  и любого  $\mathbf{y} = \overline{g(x_1, \dots, x_m)} \in RM_{m-r-1,m}$  выполнено

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{\mathbf{x} \in \mathbb{F}_2^m} f(x_1, \dots, x_m) g(x_1, \dots, x_m) = 0. \quad (7.0.10)$$

Действительно, пусть  $i_1 < \dots < i_s$ . В виду того, что  $\mathbf{x} = \overline{f}$  и  $\mathbf{y} = \overline{g}$ , где  $\deg f \leq r$  и  $\deg g \leq m - r - 1$ , из равенства (7.0.9), непосредственно, вытекает равенство (7.0.10).

Для того, чтобы завершить доказательство теоремы, достаточно заметить, что  $\dim RM_{r,m} + \dim RM_{m-r-1,m} = N = 2^m$ .  $\square$

**Следствие 7.0.4** Для любой булевой функции  $f$  от  $m$  переменных степени меньшей  $m$  имеет место равенство

$$\sum_{\alpha \in \mathbb{F}_2^m} f(\alpha) = 0. \quad (7.0.11)$$

**Лемма 7.0.10** Пусть  $L = \langle \mathbf{a}_1, \dots, \mathbf{a}_r \rangle$  — подпространство размерности  $r \leq m$  пространства  $\mathbb{F}_2^m$ , натянутое на множество векторов  $\{\mathbf{a}_1, \dots, \mathbf{a}_r\}$ ,  $\alpha$  — вектор пространства  $\mathbb{F}_2^m$ ,  $L^\perp = \langle \mathbf{b}_1, \dots, \mathbf{b}_{m-r} \rangle$  — пространство, двойственное к пространству  $L$ , и  $\phi_{L+\alpha}(\mathbf{x})$  — характеристическая функция смежного класса  $L + \alpha$ , т.е.  $\phi_{L+\alpha}(\mathbf{x})$  — функция, для которой

$$\phi_{L+\alpha}(\mathbf{x}) = \begin{cases} 1, & \text{если } \mathbf{x} \in L + \alpha, \\ 0, & \text{если } \mathbf{x} \notin L + \alpha \end{cases}. \quad (7.0.12)$$

Тогда

$$\phi_{L+0}(\mathbf{x}) = \phi_L(\mathbf{x}) = (\mathbf{b}_1(\mathbf{x}) + 1) \cdots (\mathbf{b}_{m-r}(\mathbf{x}) + 1) \text{ и } \phi_{L+\alpha}(\mathbf{x}) = \phi_L(\mathbf{x} + \alpha), \quad (7.0.13)$$

где  $\mathbf{b}_j(\mathbf{x}) = \langle \mathbf{b}_j, \mathbf{x} \rangle$  — линейная функция.

**Доказательство.** Второе равенство в (7.0.13) очевидно. Переходим к доказательству первого.

По определению, пространство  $L^\perp$ , двойственное к  $L$ , состоит из всех векторов  $\mathbf{b} \in \mathbb{F}_2^m$ , для которых скалярное произведение  $\langle \mathbf{a}, \mathbf{b} \rangle$  равно нулю всех  $\mathbf{a} \in L$ . Если  $\mathbf{b}_1, \dots, \mathbf{b}_{m-r}$  — базис линейного пространства  $L^\perp$ , то, очевидно,  $\mathbf{b}_j(\mathbf{x}) = 0$ ,  $j = 1, \dots, m - r$ , тогда и только тогда, когда  $\mathbf{x} \in L$ . Это утверждение доказывает первое равенство в (7.0.13).  $\square$

**Следствие 7.0.5 (из теоремы 7.0.5)** Пусть  $L_{r+1}$  — подпространство размерности  $r+1 \leq m$  пространства  $\mathbb{F}_2^m$ .

Тогда при любом  $\alpha \in \mathbb{F}_2^m$

$$\sum_{\mathbf{x} \in L_{r+1} + \alpha} f(\mathbf{x}) = 0, \quad (7.0.14)$$

если  $\deg f(\mathbf{x}) \leq r$ .

**Доказательство.** При  $r+1 = m$  доказательство вытекает из соотношения (7.0.9). Для доказательства следствия при  $r+1 < m$  достаточно показать, что характеристическая функция может быть представлена в виде многочлена Жегалкина, степень которого не выше  $m - r - 1$ .

Действительно, если это так, то

$$\sum_{\mathbf{x} \in L + \alpha} f(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{F}_2^m} \phi_{L+\alpha}(\mathbf{x}) f(\mathbf{x}), \quad \deg \phi_{L+\alpha}(\mathbf{x}) f(\mathbf{x}) < m, \quad (7.0.15)$$

и из следствия 7.0.4 вытекает требуемое равенство (7.0.14).  $\square$

**Лемма 7.0.11** Рассмотрим линейные функции  $l_j^{(L)}(\mathbf{x})$ ,  $j = 1, \dots, r$ , определенные на пространстве  $L$ , которые являются ограничением линейных функций  $l_j(\mathbf{x})$ ,  $j = 1, \dots, r$ , на подпространство  $L$ , т.е.  $l_j^{(L)}(\mathbf{x}) = l_j(\mathbf{x})$ , если  $\mathbf{x} \in L$ .

Тогда

$$\sum_{\mathbf{x} \in L} l_1(\mathbf{x}) \cdots l_s(\mathbf{x}) = \begin{cases} 0, & \text{если функции } l_1^{(L)}(\mathbf{x}), \dots, l_r^{(L)}(\mathbf{x}) \\ & \text{являются линейно-зависимыми,} \\ 1, & \text{если функции } l_1^{(L)}(\mathbf{x}), \dots, l_r^{(L)}(\mathbf{x}) \\ & \text{являются линейно-независимыми} \end{cases}. \quad (7.0.16)$$

**Доказательство** непосредственно вытекает из леммы (7.0.9).  $\square$

**Следствие 7.0.6** Пусть  $L$  — подпространство размерности  $r+1 \leq m$  пространства  $\mathbb{F}_2^m$ .

Тогда

$$\sum_{\mathbf{x} \in L + \alpha} f(\mathbf{x}) = 0, \quad (7.0.17)$$

если  $\deg f(\mathbf{x}) \leq r$ .

Следующее утверждение является обобщением следствия 7.0.6.

**Теорема 7.0.6** Пусть  $L$  — подпространство размерности  $r \leq m$  пространства  $\mathbb{F}_2^m$ ,  $\alpha \in \mathbb{F}_2^m$  и  $f(\mathbf{x})$  — булева функция порядка нелинейности  $t \geq r$ .

Тогда степень нелинейности функции

$$g(\mathbf{x}) = \sum_{\mathbf{x} \in L + \alpha} f(\mathbf{x}), \quad (7.0.18)$$

не выше  $t - r$ .



**Доказательство.** Достаточно показать, что степень нелинейности функции  $g_0(\mathbf{x}) = \sum_{\mathbf{x} \in L+\alpha} f_0(\mathbf{x})$ , где  $f_0(\mathbf{x}) = x_{i_1} \cdots x_{i_t}$ ,  $i_1 < \cdots < i_t$ , не выше  $t - r$ . Это следует из легко проверяемого соотношения (Упражнение)  $\deg \sum_{\mathbf{x} \in L_0+\alpha} f_0(\mathbf{x}) \leq t-1$ , где  $L_0$  — одномерное пространство.  $\square$

По сложившемуся у специалистов мнению коды Рида-Маллера являются слабыми кодами (имеют малое по сравнению с максимально возможным кодовое расстояние), но в тоже время являются кодами с простым декодированием. В следующем разделе мы рассмотрим некоторые из этих относительно простых алгоритмов декодирования и связанные с ними другие задачи.

## 7.1 Декодирование кода Рида-Маллера

Обычно корректирующую способность кода характеризуют величиной его кодового расстояния  $d$ . Вместе с тем не менее естественно, а для некоторых приложений и более естественно, представляется характеристика корректирующей способности числом ошибок  $\hat{t}$ , которые код исправляет почти всегда. Более подробно и точно понятия корректирующая способность кода, сложность декодирования рассмотрены выше в разделе 6.1.

В настоящем параграфе показано, что если  $r = \text{const}$  и  $m \rightarrow \infty$ , то код  $RM_{r,m}$  исправляет почти все ошибки кратности  $\hat{t} = \frac{1}{2}(1 - \hat{\epsilon}_m)2^m$  с помощью алгоритма декодирования со сложностью  $O(m^{r-1}2^m)$ , где  $\hat{\epsilon}_m = \hat{\epsilon}_{m,r}$  — некоторая функция, стремящаяся к нулю при  $m \rightarrow \infty$ .

Скорость стремления к нулю функции  $\hat{\epsilon}_m$  в конечном итоге определяет качество алгоритма декодирования: чем быстрее стремится к нулю  $\hat{\epsilon}_m$ , тем лучше его корректирующая способность.

Заметим, что ниже в параграфе 7.1.7 для алгоритма декодирования кода  $RM_{r,m}$  по минимуму расстояния получены нижние оценки функции  $\epsilon_{r,m}$ , при выполнении которых исправляются почти все ошибки кратности  $\hat{t} \approx \frac{1}{2}(1 - \epsilon_m)2^m$  (Следствие 7.1.2).

Этот алгоритм при  $r \geq 2$  не является полиномиальным, т.е. его сложность, как функция от длины кода, растет быстрее скорости роста любого полинома фиксированной степени.

Для рассмотренных в этом разделе полиномиальных алгоритмов декодирования кода  $RM_{r,m}$  функция  $\epsilon_m$  стремится к нулю значительно медленнее, чем ее нижняя оценка из следствия 7.1.2. В связи с этим естественно рассмотреть следующую задачу: какова максимальная скорость стремления к нулю  $\epsilon_m$  при том или ином ограничении на сложность алгоритма декодирования, в частности, какова максимальная скорость стремления к нулю полиномиального алгоритма декодирования РМ-кода второго порядка.

С одной стороны, как следует из следствия 7.1.2 для кода  $RM_{2,m}$  существует неполиномиальный алгоритм декодирования, для которого  $\epsilon_m \approx Cm2^{-\frac{m}{2}}$  и сложность реализации  $O(m2^m)$ . С другой стороны, для полиномиального алгоритма декодирования, рассмотренного в §7.1.5,  $\epsilon_m \gtrsim C'm^{\frac{1}{2}}2^{-\frac{m}{4}}$ , где  $C, C'$  — постоянные.

Таким образом, для неполиномиального и известных полиномиальных алгоритмов декодирования РМ-кода второго порядка имеется существенный зазор между числами ошибок при которых эти алгоритмы работают почти всегда правильно. В настоящее время не ясно как сузить этот зазор.

### 7.1.1 Алгоритм декодирования RM-кода первого порядка по максимуму правдоподобия и "быстрое" умножение вектора на матрицу Адамара

Код Рида-Маллера  $RM_{1,m}$  первого порядка состоит из всех векторов  $\bar{f}$  значений аффинных функций  $f_{\mathbf{a}}(\mathbf{x}) = a_1 + \dots + a_m + a_0$ ,  $a_j \in \mathbb{F}_2$ . Их число равно  $2 \cdot 2^m$ , т.е. является полиномиальным от его длины  $N = 2^m$  кода. Поэтому декодирование кода  $RM_{1,m}$  даже наиболее сильным алгоритмом декодирования по максимуму правдоподобия является полиномиальным.

Заметим, что алгоритм декодирования по максимуму правдоподобия для любого вектора  $\mathbf{a}' \in \mathbb{F}_2^m$  вычисляет один из ближайших к нему в метрике Хемминга кодовый вектор  $\mathbf{a} \in RM_{1,m}$ . Реализация этого алгоритма обычно осуществляется следующим образом.

Рассмотрим  $2^m \times 2^m$ -матрицу

$$A_m = \|(-1)^{\langle \mathbf{a}, \mathbf{b} \rangle}\|, \quad \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^m, \quad \text{где } \langle \mathbf{a}, \mathbf{b} \rangle = a_1 b_1 + \dots + a_m b_m. \quad (7.1.1)$$

Пусть  $\mathbb{F}_2^m = \{\alpha_1, \dots, \alpha_N\}$ ,  $N = 2^m$ . Строки и столбцы матрицы  $A$  будем индексировать элементами множества  $\{\alpha_1, \dots, \alpha_N\}$ .

Пусть  $\mathbf{y} \in \mathbb{F}_2^{2^m}$  и  $\tilde{\mathbf{y}} = ((-1)^{y_1}, \dots, (-1)^{y_N})$ ,  $N = 2^m$ . Хорошо известно, что

$$\tilde{\mathbf{y}} A_m = (\delta_{\alpha_1}, \dots, \delta_{\alpha_N}), \quad N = 2^m, \quad (7.1.2)$$

где

$$\delta_{\alpha_j} = N - 2d(\mathbf{y}, \overline{f_{\alpha_j}(\mathbf{x})}) \quad (7.1.3)$$

и  $d$  — метрика Хемминга. (Упражнение)

Соотношение (7.1.3) показывает, что индекс  $\alpha_s$  координаты вектора  $\mathbf{y}A$  с максимальным значением определяет вектор  $\overline{f_{\alpha_s}(\mathbf{x})}$  значений аффинной функции  $f_{\alpha_s}(\mathbf{x})$ , который наиболее близок в метрике Хемминга к вектору  $\mathbf{y}$ .

Таким образом, декодирование кода  $RM_{1,m}$  можно свести к умножению вектора  $\tilde{\mathbf{y}}$  с действительными координатами на матрицу Адамара  $A_m$ . Исходя из стандартного определения умножения вектора на матрицу, сложность  $T_m$  вычисления произведения  $\mathbf{y}A_m$ , оценивается сверху величиной  $2^{2m} = N^2$ . Вместе с тем, как мы сейчас покажем, что сложность  $T_m$  умножения вектора на матрицу Адамара  $A_m$  может быть понижена до величины  $m2^m$ , т.е.  $T_m \leq m2^m$ .

Снижение сложности можно осуществить с помощью следующего простого соображения, которое бывает полезным и для решения многих других подобных задач. Предположим, что матрица  $A_m$  представлена в виде

$$A_m = A_m^{(1)} \dots A_m^{(m)} \quad (7.1.4)$$

произведения матриц  $A_m^{(j)}$ , каждая из которых имеет малое число ненулевых элементов. В этом случае умножение  $\mathbf{y}A_m$  реализуется как цепочка последовательных умножений вектора на матрицы  $A_m^{(j)}$ . В результате сложность умножения матрицы на вектор будет оцениваться сверху величиной  $T_m^{(1)} + \dots + T_m^{(m)}$ , где  $T_m^{(j)}$  — сложность умножения вектора на матрицу  $A_m^{(j)}$ .

В рассматриваемом нами случае каждая матрица  $A_m^{(j)}$  содержит два ненулевых элемента  $\pm 1$  в каждой ее строке и столбце, поэтому  $T_m^{(j)} = 2^m$  и, следовательно,  $T_m \leq T_m^{(1)} + \dots + T_m^{(m)} = m2^m$ . Построить такие удобные матрицы  $A_m^{(j)}$  можно следующим образом.

Пусть  $A = \|a_{i,j}\|$  —  $k \times k$ –матрица,  $B = \|b_{u,v}\|$  —  $s \times s$ –матрица.  $ks \times ks$ –матрица  $A \otimes B$  (тензорное или, как его еще называют, кронекерово произведение матриц  $A$  и  $B$ ) определяется следующим образом

$$A \otimes B = \|a_{i,j}B\| = \|Ab_{u,v}\| = \|a_{i,j}b_{u,v}\|, \quad i, j = 1, \dots, k, \quad u, v = 1, \dots, s. \quad (7.1.5)$$

Как хорошо известно, и это достаточно просто проверить, что матрицу  $A_m$  можно представить в виде

$$A_m = A_1 \otimes A_1 \otimes \dots \otimes A_1 = \otimes A_1^m, \quad (7.1.6)$$

где  $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = ((-1)^{ab}), a, b \in \mathbb{F}_2$ , — матрица Адамара порядка 2. (Упражнение)

**Лемма 7.1.1** *Равенство (7.1.4) будет выполнено, если в качестве матриц  $A_m^{(j)}$ ,  $j = 1, \dots, t$ , взять матрицу  $A_m^{(j)} = I_{2^{j-1}} \otimes A_1 \otimes I_{2^{m-j}}$ , где  $I_{2^j}$  — единичная матрица порядка  $2^j$ .*

*Каждая матрица  $A_m^{(m-j)}$  имеет в каждом столбце и строке по два ненулевых элемента  $\pm 1$ .*

**Доказательство.** Как нетрудно проверить, матрицу  $A_m$  с учетом (7.1.6) можно представить в следующем виде (Упражнение).

$$A_m = I_2 \otimes A_{m-1} \cdot A_1^{m-1} \otimes I_{2^{m-1}}. \quad (7.1.7)$$

В качестве матрицы  $A_m^{(m)}$  в (7.1.4) возьмем матрицу  $A_1^{m-1} \otimes I_{2^{m-1}}$ . Этот же процесс продолжим и для матрицы  $A_{m-1}$  в (7.1.6), а именно, в качестве матрицы  $A_m^{(m-1)}$  возьмем матрицу  $I_2 \otimes A_1 \otimes I_{2^{m-2}}$ , для которой справедливо соотношение  $A_m = I_4 \otimes A_{m-2} \cdot I_2 \otimes A_1 \otimes I_{2^{m-2}} \cdot A_1^{m-1} \otimes I_{2^{m-1}}$ .

Продолжая этот процесс, мы установим, что если в качестве матрицы  $A_m^{(m-j)}$  мы возьмем матрицу  $I_{2^{j-1}} \otimes A_1 \otimes I_{2^{m-j}}$ , то соотношение (7.1.4) будет выполнено.

Также очевидно, что каждая матрица  $A_m^{(m-j)}$  имеет в каждом столбце и строке по два ненулевых элемента  $\pm 1$ .  $\square$

**Следствие 7.1.1** *Умножение вектора  $\tilde{y}$  с действительными координатами на матрицу  $A_m$  может быть реализовано за  $m2^m$  операций сложения и вычитания в поле действительных чисел  $R$ .*

Отсюда непосредственно вытекает

**Теорема 7.1.1** *Сложность алгоритма декодирования по максимуму правдоподобия кода Ридда-Маллера первого порядка не более, чем  $O(m2^m)$ .*

Известны многочисленные другие результаты, касающиеся сложности декодирования RM-кодов первого порядка. Обычно эти алгоритмы "работают" только при числе ошибок в кодовом векторе меньшем, чем  $2^{m-2} - 1$  — примерно половине кодового расстояния кода  $RM_{1,m}$ . Это ограничение на число ошибок позволяет, в частности, понизить сложность декодирования  $RM_{1,m}$  до  $O(2^m)$  (см. [17]).

Следует также отметить, что для криптографии интересны алгоритмы декодирования "сильно укороченных" RM-кодов первого порядка, т.е. кодов, образованных небольшой частью разрядов полного RM-кода. Это совсем другая тема, которой в данной книге мы касаться не будем.

Для RM-кодов порядка  $r > 1$  также известны [6] "быстрые" алгоритмы вычисления произведения

$$\tilde{\mathbf{y}} A_{m,r}, \quad (7.1.8)$$

где  $A_{m,r}$  —  $2^m \times 2^{\dim RM_{m,r}}$  — матрица, столбцами которой являются всевозможные столбцы  $\tilde{\mathbf{a}} = ((-1)^{a_1}, \dots, (-1)^{a_{2^m}})^T$ , где  $\mathbf{a} = (a_1, \dots, a_{2^m}) \in RM_{m,r}$ , и  $\tilde{\mathbf{y}}$  —  $2^m$ -мерный вектор с действительными координатами. Сложность его реализации равна  $O(2^{\dim RM_{m,r}})$  операций сложения и вычитания.

### 7.1.2 Полиномиальный алгоритм декодирования RM-кода порядка $r > 1$

Группой автоморфизмов кода RM-кода  $r$ -го порядка является полная аффинная группа  $GA_m$ , состоящая из всех отображений пространства  $\mathbb{F}_2^m$  в себя вида

$$\sigma : \mathbf{x} \rightarrow \mathbf{x}A + \alpha, \quad \mathbf{x} \in \mathbb{F}_2^m, \quad (7.1.9)$$

где  $\alpha \in \mathbb{F}_2^m$  и  $A$  — невырожденная  $m \times m$ -матрица с элементами из  $\mathbb{F}_2$ . Таким образом, если  $\overline{f(\mathbf{x})} \in RM_{r,m}$ , то и  $\overline{g(\mathbf{x})} \in RM_{r,m}$ , где  $g(\mathbf{x}) = f(\mathbf{x}A + \alpha)$ .

Так как код  $RM_{r,m}$  является линейным, то вектор

$$\overline{f_{A,\alpha}} = \overline{f(\mathbf{x})} + \overline{f(\mathbf{x}A + \alpha)}, \quad \mathbf{x} \in \mathbb{F}_2^m, \quad (7.1.10)$$

также принадлежит коду  $RM_{r,m}$ . Следующее замечание является существенным для дальнейшего изложения.

Для того, чтобы вычислить вектор  $\overline{f_{A,\alpha}}$  нет нужды знать представление функции  $\overline{f(\mathbf{x})}$  в виде многочлена Жегалкина. Для вычисления  $\overline{f_{A,\alpha}}$  достаточно сложить вектор  $\overline{f(\mathbf{x})}$  с вектором  $\overline{f(\mathbf{x}A + \alpha)}$ , который является вектором  $\overline{f(\mathbf{x})}$  с переставленными координатами в соответствии перестановкой  $\sigma$  (см. (7.1.9)).

Если зафиксировать элементы  $A, \alpha$  и заставить функцию  $f$  пробежать все элементы  $RM_{r,m}$ , то множество векторов  $\overline{f_{A,\alpha}}$  будет образовывать некоторый линейный подкод кода  $RM_{r,m}$ , который мы будем обозначать через  $RM_{r,m}(A, \alpha)$ .

Далее мы ограничимся рассмотрением только случая: матрица  $A$  является единичной матрицей  $E$ , т.е. мы будем рассматривать только отображения, которые порождаются сдвигами  $\sigma : \mathbf{x} \rightarrow \mathbf{x} + \alpha$ ,  $\alpha \in \mathbb{F}_2^m$ , пространства  $\mathbb{F}_2^m$ . В этом случае функция

$$f_{E,\alpha} = f_\alpha(\mathbf{x}) = f(\mathbf{x}) + f(\mathbf{x} + \alpha) \quad (7.1.11)$$

называется производной булевой функции  $f$  по направлению  $\alpha$ .

**Лемма 7.1.2** Если  $\alpha \neq 0$ , то линейное пространство  $RM_{r,m}(\alpha) = \{\overline{f_\alpha} | f \in \widehat{RM}_{r,m}\}$ , состоит из всех векторов  $\overline{g} \in RM_{r-1,m}$ , определяемых булевыми функциями  $g(\mathbf{x}) \in \widehat{RM}_{r-1,m}$ , для которых справедливо

$$g(\mathbf{x}) + g(\mathbf{x} + \alpha) = 0. \quad (7.1.12)$$

Размерность  $\dim RM_{r,m}(\alpha)$  пространства  $RM_{r,m}(\alpha)$  равна

$$\dim RM_{r,m}(\alpha) = \dim RM_{r-1,m-1} = \sum_{j=0}^{r-1} \binom{m-1}{j}. \quad (7.1.13)$$

**Доказательство.** Очевидно, из определения функции  $f_\alpha$  следует, что соотношение (7.1.12) выполнено для всех функций  $f(\mathbf{x}) \in \widehat{RM}_{r,m}(\alpha)$ .

Следовательно, осталось доказать, что линейное пространство  $\widehat{RM}_{r,m}(\alpha)$  состоит из всех таких функций, у которых многочлен Жегалкина имеет степень не выше  $r-1$ .

Если  $\deg f \leq r$ , то из соотношения (7.1.11) и теоремы 7.0.6 следует, что  $\deg f_\alpha \leq r-1$ . То же самое нетрудно доказать и непосредственно (Упражнение).

Очевидно, отображение  $\sigma_\alpha : f \rightarrow f_\alpha$ ,  $f \in RM_{r,m}$ , является линейным отображением линейного пространства  $RM_{r,m}$  в линейное пространство  $RM_{r-1,m}$ . Вычислим размерность  $\dim RM_{r,m}(\alpha)$  — образа этого отображения.

Пусть  $A \in M_m(\mathbb{F}_2)$  — невырожденная матрица такая, что  $\alpha = \mathbf{e}_1 A$ , где  $\mathbf{e}_1 = (1, 0, \dots, 0)$  — единичный вектор. Очевидно,  $f_\alpha = f'_{\mathbf{e}_1}$ , где  $f'(\mathbf{x}) = f(\mathbf{x}A)$ . Если функция  $f$  пробегает все элементы пространства  $\widehat{RM}_{r,m}$ , то функция  $f'$  также пробегает все элементы пространства  $\widehat{RM}_{r,m}$ . Поэтому  $\dim RM_{r,m}(\alpha) = \dim RM_{r,m}(\mathbf{e}_1)$ . Следовательно, мы без ограничения общности можем полагать, что  $\alpha = \mathbf{e}_1$  и вычислять размерность пространства  $\dim RM_{r,m}(\mathbf{e}_1)$ .

Очевидно, если  $f(\mathbf{x}) = x_1 x_{i_2} \cdots x_{i_t}$ ,  $1 < i_2 < \cdots < i_t \leq m$ , то

$$f_{\mathbf{e}_1} = x_1 x_{i_2} \cdots x_{i_t} + (x_1 + 1) x_{i_2} \cdots x_{i_t} = x_{i_2} \cdots x_{i_t}. \quad (7.1.14)$$

Отсюда непосредственно вытекает, что базисом пространства  $RM_{r,m}(\mathbf{e}_1)$  являются все мономы  $x_{i_2} \cdots x_{i_t}$ ,  $1 < i_2 < \cdots < i_t \leq m$ . Следовательно,  $\dim \widehat{RM}_{r,m}(\mathbf{e}_1) = \dim \widehat{RM}_{r-1,m-1} = \sum_{j=0}^{r-1} \binom{m-1}{j}$ .  $\square$

Как следует из доказанной теоремы каждый вектор  $\overline{f_\alpha} \in RM_{r,m}(\alpha)$  имеет  $2^{m-1}$  одинаковых пар координат:  $f_\alpha(\mathbf{x})$  и  $f_\alpha(\mathbf{x} + \alpha)$ . Выберем в каждой такой паре одну координату и рассмотрим вектор  $\overline{f_\alpha}^*$  длины  $2^{m-1}$ , каждая координата которого является одной координатой из пары  $f_\alpha(\mathbf{x})$  и  $f_\alpha(\mathbf{x} + \alpha)$ . Указанное "выкалывание" половины координат у вектора  $\overline{f_\alpha}$  мы представим в виде линейного отображения  $\Phi_\alpha$ , которое проектирует вектор  $\overline{f_\alpha} \in RM_{r,m}(\alpha)$  в вектор  $\overline{f_\alpha}^*$ , который принадлежит коду  $RM_{r-1,m-1}$ .

Пусть  $g(\mathbf{x}) \in RM_{r-1,m}$  — булева функция, для которой выполнено равенство (7.1.12), и  $A_\alpha$  — невырожденная матрица, для которой справедливо  $\alpha = \mathbf{e}_1 A_\alpha$ . Как следует из доказательства теоремы,  $\overline{f_\alpha} = \overline{f'_{\mathbf{e}_1}}$ , где  $f'(\mathbf{x}) = f(\mathbf{x}A)$ .

Отсюда следует, что в качестве  $\Phi_\alpha$  можно взять отображение, которое выкалывает координату  $g(\alpha_j)$  у вектора  $\overline{g(\mathbf{x})} = (g(\alpha_1), \dots, g(\alpha_{2^m})) \in RM_{r,m}(\alpha)$  только тогда, когда первая координата у вектора  $\alpha_j A_\alpha$  равна 1. В этом случае образ  $\Phi_\alpha(\overline{g(\mathbf{x})}) = \overline{g'(0, x_2, \dots, x_m)}$  будет, очевидно, вектором RM-кода  $RM_{r-1,m-1}$ .

### 7.1.3 Основная идея полиномиального декодирования RM-кода $r$ -го порядка

Предположим, что  $\overline{f(\mathbf{x})} \in RM_{r,m}$  и  $\mathbf{e} \in \mathbb{F}_2^{2^m}$  — вектор, который мы будем называть вектором ошибки. Вектор  $\overline{f(\mathbf{x})}' = \overline{f(\mathbf{x})} + \mathbf{e}$  мы называем кодовым вектором, искаженным  $t$  ошибками, где  $t = wt(\mathbf{e})$  (вес вектора  $\mathbf{e}$ ).

Задача декодирования вектора  $\overline{f(\mathbf{x})}'$ , рассматриваемая в настоящем разделе, состоит в следующем. Имея в наличии только вектор  $\overline{f(\mathbf{x})}'$ , надо вычислить вектор  $\overline{f(\mathbf{x})} \in RM_{r,m} \subset RM_{r,m}$ , ближайший к  $\overline{f(\mathbf{x})}'$ , или, что одно и то же, все коэффициенты  $a_{i_1, \dots, i_k}$ ,  $0 \leq k \leq r$ , в представлении функции  $f(\mathbf{x})$  в виде многочлена Жегалкина (см. (7.0.3)). Заметим, что имеются и другие определения задачи декодирования кода (см. раздел 6.1).

Как следует из определения производной булевой функции и это уже было замечено выше, для вычисления вектора  $\overline{f_\alpha}$  достаточно сложить вектор  $\overline{f(\mathbf{x})}$  с вектором  $\overline{f(\mathbf{x}A + \alpha)}$ . Последний вектор является вектором  $\overline{f(\mathbf{x})}$ , у которого координаты переставлены в соответствии с перестановкой  $\sigma : \mathbf{x} \rightarrow \mathbf{x} + \alpha$ . Отсюда вытекает, что искаженный вариант  $\overline{f_\alpha}'$  производной  $\overline{f_\alpha}$  можно получить в следующем виде

$$\overline{f_\alpha}' = \overline{f(\mathbf{x})}' + \overline{f(\mathbf{x} + \alpha)}' = \overline{f_\alpha} + \mathbf{e} + \mathbf{e}_\alpha, \quad (7.1.15)$$

где  $\overline{f(\mathbf{x} + \alpha)}'$  — вектор  $\overline{f(\mathbf{x})}'$ , у которого координаты переставлены в соответствии с перестановкой  $\sigma$  и  $\mathbf{e}_\alpha$  — вектор ошибки  $\mathbf{e}$ , у которого координаты переставлены в соответствии с перестановкой  $\sigma_\alpha$  его координат.

Как следует из леммы 7.1.2, вектор  $\overline{f_\alpha}$  является кодовым вектором RM-кода  $RM_{r-1,m}$  с дублированными координатами (координаты  $f_\alpha(\mathbf{x})$  и  $f_\alpha(\mathbf{x} + \alpha)$  у вектора  $\overline{f_\alpha}$  совпадают). Отсюда и из (7.1.15) следует, что  $\overline{f_\alpha}'$  является кодовым вектором RM-кода  $RM_{r-1,m}$ , искаженным  $t' = wt(\mathbf{e} + \mathbf{e}_\alpha)$  ошибками.

Предположим, что мы каким-либо образом правильно декодировали искаженный вектор  $\overline{f_\alpha}'$ , т.е. правильно определили вектор  $\overline{f_\alpha}$  и, следовательно, правильно определили коэффициенты  $b_{j_1, \dots, j_s}$  в многочлене Жегалкина

$$f_\alpha(\mathbf{x}) = \sum_{s=0}^{r-1} \sum_{j_1 < \dots < j_s} b_{j_1, \dots, j_s} x_{j_1} \cdots x_{j_s}. \quad (7.1.16)$$

Как следует из определения функции  $f_\alpha(\mathbf{x})$  (см. соотношение (7.1.11)), коэффициенты  $b_{j_1, \dots, j_{r-1}}$  линейно выражаются через коэффициенты  $a_{i_1, \dots, i_r}$  в представлении (7.0.3) функции  $f(\mathbf{x})$  в виде многочлена Жегалкина. Эти линейные соотношения мы трактуем как систему линейных уравнений относительно коэффициентов  $a_{i_1, \dots, i_r}$ , в которой правыми частями являются известные коэффициенты  $b_{j_1, \dots, j_{r-1}}$ .

Эту систему довольно просто выписать в явном виде, но этого делать в данном месте мы не будем. Вместе с тем укажем, что она (система) имеет  $\binom{m}{r-1}$  (число различных  $b_{j_1, \dots, j_s}$ ) уравнений и  $\binom{m}{r}$  неизвестных  $a_{i_1, \dots, i_r}$ .

Если объединить для нескольких различных значений  $\alpha$  указанные системы линейных уравнений, то в итоге мы получим общую систему линейных уравнений, которая, как будет показано ниже, имеет единственное решение при хорошо выбранных значениях параметра  $\alpha$ .

Таким образом, если правильно найдены все коэффициенты  $b_{i_1, \dots, i_{r-1}}$ , то решив указанную систему линейных уравнений, мы вычислим все коэффициенты  $a_{i_1, \dots, i_r}$  многочлена Жегалкина, представляющего функцию  $f$ .

Оставшиеся невычисленными коэффициенты  $a_{i_1, \dots, i_s}$ ,  $0 \leq s < r$ , функции  $f$  могут быть определены следующим образом.

Пусть

$$\widehat{f}(\mathbf{x}) = \sum_{i_1 < \dots < i_r} a_{i_1, \dots, i_r} x_{i_1} \cdots x_{i_r} \quad (7.1.17)$$

— функция, образованная уже вычисленными коэффициентами  $a_{i_1, \dots, i_r}$ . Тогда, очевидно, вектор  $\overline{f(\mathbf{x})}' + \widehat{f}(\mathbf{x})$  является вектором кода  $RM_{r-1, m}$ , искаженного  $t$  ошибками и может быть декодирован уже рассмотренными методами.

Таким образом, мы сводим декодирование искаженного вектора кода  $RM_{r, m}$  к декодированию нескольких искаженных векторов кода  $RM_{r-1, m}$ , порядок которого, по крайней мере, на единицу меньше, чем  $r$ , и решению системы линейных уравнений с  $\binom{m}{r}$  неизвестными.

При этом следует отметить, что число ошибок  $t'$ , которые поражают векторы  $\overline{f_\alpha}$  кода  $RM_{r-1, m}$ , вообще говоря, будет большим, чем  $t$ . Очевидно, для числа  $t'$  справедливы оценки  $0 \leq t' \leq 2t$ . Кроме ошибки в векторе  $\overline{f_\alpha}$  не являются независимыми, даже если таковыми являлись ошибки в векторе  $\overline{f}$ .

Заметим, что совершенно таким же способом декодирование векторов кода  $RM_{r-1, m}$  можно свести к декодированию векторов кода  $RM_{r-2, m}$  и т.д.

Не вдаваясь особенно в подробности, укажем, что сложность  $T(r, m)$  реализации рассматриваемого алгоритма декодирования кода Рида-Маллера  $RM_{r, m}$  равна

$$T(r, m) = O\left(\left(\binom{m}{r}\right)^3 + Cm2^m T(r-1, m)\right), \quad (7.1.18)$$

где  $\binom{m}{r}^3$  — число операций, требуемых для решения системы линейных уравнений с  $\binom{m}{r}$  неизвестными методом исключения Гаусса, и  $C'm$  — приблизительное число различных значений  $\alpha$ , которые необходимо использовать для составления общей невырожденной системы линейных уравнений относительно коэффициентов  $a_{i_1, \dots, i_r}$ ,  $C''2^m$  — число операций, необходимых для вычисления "искаженной" производной  $\overline{f_\alpha}'$  по направлению  $\alpha$  (см. (7.1.15)), и  $C = C'C''$ .

Как видно из соотношения (7.1.18) число  $T(r, m)$  при  $m \rightarrow \infty$  и  $r = \text{const}$  полиномиально зависит от числа  $2^m$  — длины кода  $RM_{r, m}$ .

Выпишем упомянутую выше систему уравнений в случае  $r = 1$  и  $r = 2$ .

#### 7.1.4 Декодирование кода $RM_{1, m}$ первого порядка

В случае  $r = 1$  каждая функция  $f \in RM_{1, m}$  является аффинной и имеет вид  $f(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle + a_0 = a_1 x_1 + \dots + a_m x_m + a_0$ . Производная  $f_\alpha(\mathbf{x})$  по направлению  $\alpha$  имеет вид  $f_\alpha(\mathbf{x}) = \langle \mathbf{a}, \alpha \rangle = b_\alpha$ , т.е. является постоянной.

При декодировании искаженного вектора  $\overline{f_\alpha}', f_\alpha \in RM_{0, m}$ , мы сначала вычисляем вектор  $\overline{f_\alpha}' = \overline{f(\mathbf{x})}' + \overline{f(\mathbf{x} + \alpha)}' = \overline{b_\alpha} + \mathbf{e} + \mathbf{e}_\alpha = \overline{b'_\alpha}$ . Постоянную  $b_\alpha$  естественно вычислять мажоритарным алгоритмом, а именно в качестве  $b_\alpha$  принять то значение, которое наиболее часто встречается среди координат вектора  $\overline{f_\alpha}'$ .

Система линейных уравнений относительно коэффициентов  $a_j$  функции  $f$  имеет вид

$$\langle \mathbf{a}, \alpha^{(j)} \rangle = b'_{\alpha^{(j)}}, \quad j = 1, \dots, m', \quad (7.1.19)$$

где  $\Omega = \{\alpha^{(1)}, \dots, \alpha^{(m')}\}$  — произвольное множество элементов пространства  $\mathbb{F}_2^m$ . Если в качестве  $\Omega$  взять множество из  $m' = m$  линейно-независимых векторов, то система (7.1.19) будет иметь единственное решение  $\mathbf{a}$ , которое определяет форму (линейную функцию)  $\langle \mathbf{a}, \mathbf{x} \rangle$ . Коэффициент  $a_0$  функции  $f$  можно определить, например, с помощью декодирования искаженного вектора  $\overline{f'_\alpha} + \langle \mathbf{a}, \mathbf{x} \rangle$  кода  $RM_{0,m}$ .

Оценим вероятность правильного декодирования искаженного вектора  $\overline{f'} = \overline{f} + \mathbf{e}$  кода  $RM_{1,m}$  рассмотренным алгоритмом.

Следующее утверждение мы принимаем без доказательства. Если появление всех векторов ошибок  $\mathbf{e}$  веса  $t = wt(\mathbf{e})$  является равновероятным, то вероятность  $P_t$  события  $b'_\alpha = b_\alpha$  близка к 1, если  $t < \frac{1}{2}(N - C\sqrt[4]{N})$ , где  $C$  — достаточно большая постоянная. Причина, по которой в последней формуле из  $N$  вычитается  $C\sqrt[4]{N}$ , а не  $C\sqrt{N}$  заключается в том, число ошибок в векторе  $\overline{f'_\alpha}$  равно числу  $t' = wt(\mathbf{e} + \mathbf{e}_\alpha)$ , а не числу  $t = wt(\mathbf{e})$ . Если  $t \approx \frac{N}{2}(1 - \epsilon)$ ,  $\epsilon < 1$ , то, как нетрудно вычислить,  $t' \approx \frac{N}{2}(1 - \epsilon^2)$ .

Отсюда следует, что вероятность  $P_{t,m}$  события  $b'_\alpha = b_\alpha$  для  $m$  различных значений  $\alpha$  близка к 1, если  $t < \frac{1}{2}(N - \rho(m)\sqrt[4]{N})$ , где  $\rho(m)$  — медленно растущая функция. Например, в качестве  $\rho(m)$  можно взять функцию  $\rho(m) = C\sqrt{m}$ .

Как нетрудно подсчитать, сложность этого алгоритма декодирования равна  $T = O(m2^m)$ .

Заметим, что такое же сложность имеет алгоритм декодирования РМ-кода первого порядка по максимуму правдоподобия (см. раздел 7.1.1). Вместе с тем алгоритм декодирования по максимуму правдоподобия исправляет почти всегда существенно большее число ошибок (см. раздел 7.1.7, следствие 7.1.2), чем рассмотренный алгоритм, т.е. в данном случае предпочтительно использовать алгоритм декодирования по максимуму правдоподобия. Совершенно иная картина имеет место для кода  $RM_{2,m}$ .

### 7.1.5 Декодирование кода $RM_{2,m}$

В случае  $r = 2$  каждая функция  $f \in RM_{2,m}$  имеет вид

$$f(\mathbf{x}) = \sum_{i < j} a_{i,j} x_i x_j + a_1 x_1 + \dots + a_m x_m + a_0. \quad (7.1.20)$$

Производная  $f_\alpha(\mathbf{x})$  по направлению  $\alpha$  имеет вид

$$f_\alpha(\mathbf{x}) = f(\mathbf{x} + \alpha) - f(\mathbf{x}) = a_0 + f(\alpha) + \sum_{i=1}^m b_i(\alpha) x_i, \quad (7.1.21)$$

где  $b_i(\alpha) = \sum_{j=1}^m a_{i,j}^* \alpha_j$ ,  $a_{j,j} = 0$  и  $a_{i,j}^* = \begin{cases} a_{i,j}, & \text{если } i < j, \\ a_{j,i}, & \text{если } i > j. \end{cases}$

Для декодирования искаженного вектора  $\overline{f'_\alpha}, f_\alpha \in RM_{1,m}$ , мы используем алгоритм декодирования кода  $RM_{1,m}$  по максимуму правдоподобия (см. раздел 7.1.2), которой имеет сложность  $O(m2^m)$  (см. раздел 7.1.7). После вычисления вектора  $\overline{f'_\alpha}^*, \overline{f_\alpha}^* \in RM_{1,m}$ , ближайшего к  $\overline{f'_\alpha}$ , мы определяем значение констант  $b_i^*(\alpha)$ ,  $i = 1, \dots, m$ , таких, что



$f_\alpha^*(\mathbf{x}) = \sum_{i=1}^m b_i^*(\alpha) x_i + b_0$ . Таким образом, для каждого заданного значения параметра (вектора)  $\alpha$  мы получаем совокупность из  $m$  линейных уравнений

$$\sum_{j=1}^m a_{i,j}^* \alpha_j = b_i^*(\alpha), \quad i = 1, \dots, m, \quad (7.1.22)$$

относительно неизвестных значений коэффициентов  $a_{i,j}$ .

Если положить в (7.1.22)  $\alpha = \mathbf{e}_s = (0, \dots, 0, 1, 0, \dots, 0)$  (единица на  $s$ -ом месте), то мы получим систему из  $m$  линейных уравнений

$$a_{i,s}^* = b_i^*(\mathbf{e}_s), \quad i = 1, \dots, m. \quad (7.1.23)$$

относительно неизвестных  $a_{i,j}$ ,  $i < j$ . Рассмотрим систему линейных уравнений, которая является объединением систем (7.1.23) для различных  $s$ . Эта система, называемая далее объединенной, имеет  $\binom{m}{2}$  неизвестных  $a_{i,j}$ ,  $i < j$  и  $m^2$  уравнений.

Заметим, что из определения величин  $b_i(\mathbf{e}_s)$  следует, что  $b_i(\mathbf{e}_s) = b_s(\mathbf{e}_i)$ . Поэтому, если  $b_i^*(\mathbf{e}_s) \neq b_s^*(\mathbf{e}_i)$ , то это событие свидетельствует о том, что одно из значений  $b_i^*(\mathbf{e}_s)$  или  $b_s^*(\mathbf{e}_i)$  определено неправильно.

Если же  $b_i^*(\mathbf{e}_s) = b_s^*(\mathbf{e}_i)$  для всех  $i, s$ ,  $i \neq s$ , то объединенная система будет иметь единственное решение  $a_{i,j} = b_i^*(\mathbf{e}_s)$ ,  $i < j$ .

В общем случае объединение систем линейных уравнений (7.1.22), получаемых при разных значениях  $\alpha$ , образуют систему линейных уравнений относительно неизвестных значений коэффициентов  $a_{i,j}$ .

Так как число различных коэффициентов  $a_{i,j}$  равно  $\binom{m}{2} = \frac{m(m-1)}{2}$ , то для однозначной разрешимости этой системы необходимо выбрать не менее, чем  $\frac{m-1}{2}$  различных векторов  $\alpha$ , и затем декодировать для каждого из них искаженный вектор  $\bar{f}_\alpha', f_\alpha \in RM_{1,m}$ .

Из сказанного выше вытекает, что сложность реализации рассмотренного алгоритма декодирования не более, чем  $O(m2^m)$ .

Оценим вероятность правильного декодирования искаженного вектора  $\bar{f}' = \bar{f} + \mathbf{e}$  кода  $RM_{2,m}$  с помощью рассмотренного алгоритма декодирования.

Заметим, что из следствия 7.1.2 вытекает, что с помощью алгоритма декодирования по максимуму правдоподобия кода  $RM_{1,m}$  мы почти всегда правильно вычислим вектор  $\bar{f}_\alpha^* \in RM_{1,m}$ , если  $wt(\mathbf{e} + \mathbf{e}_\alpha) < \frac{1}{2}(N - C_r m^{\frac{1}{2}} \sqrt{N})$ .

Вместе с тем нельзя утверждать, что вероятность появления всех векторов ошибок  $\mathbf{e} + \mathbf{e}_\alpha$  определенного веса  $t'$  является равновероятным, если равновероятно появление всех векторов  $\mathbf{e}$  веса  $t$ . Это происходит из-за того, что вектор  $\mathbf{e} + \mathbf{e}_\alpha$  состоит из двух одинаковых половинок: координаты  $e_{\alpha_j}$  и  $e_{\alpha_j + \alpha}$  вектора  $\mathbf{e} + \mathbf{e}_\alpha$ , индексированные векторами  $\alpha_j$  и  $\alpha_j + \alpha$ , одинаковы. Поэтому следствие 7.1.2, доказанное при условии равной вероятности всех векторов ошибок веса  $t$ , в данной ситуации неприменимо.

Дело спасает следующее замечание. Если выколоть в векторе  $\bar{f}_\alpha$  одну координату из пары одинаковых координат, индексированных векторами  $\alpha_j$  и  $\alpha_j + \alpha$ , то мы получим вектор  $\bar{f}_\alpha^\Delta$  длины  $2^{m-1}$ , который является вектором кода  $RM_{1,m-1}$ . Об этом подробнее написано в конце раздела 7.1.2.

Ту же самую процедуру по выкалыванию сделаем и для вектора  $\mathbf{e} + \mathbf{e}_\alpha$ . В результате получим вектор ошибок  $\{\mathbf{e} + \mathbf{e}_\alpha\}^\Delta$  длины  $2^{m-1}$ . Как легко установить, что если заставить

вектор  $\mathbf{e}$  пробежать все векторы веса  $t'$ , то вектор  $\{\mathbf{e} + \mathbf{e}_\alpha\}^\Delta$  будет пробегать все векторы веса  $t$ , где  $0 \leq t \leq \min(2t', 2^{m-1})$ , при этом каждый вектор  $\{\mathbf{e} + \mathbf{e}_\alpha\}^\Delta$  фиксированного веса  $t$  будет появляться одинаково часто. (Упражнение)

Отсюда следует, что следствие применимо к искаженной половине  $\overline{f_\alpha}^{\Delta'} = \overline{f_\alpha}^\Delta + \{\mathbf{e} + \mathbf{e}_\alpha\}^\Delta$ .

Следующее утверждение мы принимаем без доказательства. Если появление всех векторов ошибок  $\mathbf{e}$  веса  $t = wt(\mathbf{e})$  является равновероятным и  $t < \frac{1}{2}(N - C_1 m^{\frac{1}{4}} \sqrt[4]{N})$ , то почти всегда  $wt(\mathbf{e} + \mathbf{e}_\alpha) < \frac{1}{2}(N - C'_1 m^{\frac{1}{2}} \sqrt{N})$  при достаточно больших  $C'_1$ .

Отсюда следует, что если  $t < \frac{1}{2}(N - C_1 m^{\frac{1}{4}} \sqrt[4]{N})$ , то вектор  $\overline{f_\alpha} + \mathbf{e} + \mathbf{e}_\alpha$  будет почти всегда декодирован правильно с помощью алгоритма максимального правдоподобия.

Для получения общей системы уравнений нам необходимо провести  $m$  актов декодирования при различных  $\alpha$ . Это позволит вычислить все коэффициенты  $a_{i,j} = b_i^*(\mathbf{e}_s)$ ,  $i < j$ .

Как легко установит, все эти  $m$  декодирований будут правильными, если  $t < \frac{1}{2}(N - \rho(m) \sqrt[4]{m} \sqrt[4]{N})$ , где  $\rho(m)$  — медленно растущая функция. Например, в качестве  $\rho(m)$  можно взять функцию  $\rho(m) = C \sqrt[4]{m}$ .

Таким образом, мы показали, что если число ошибок  $t = wt(\mathbf{e})$ , которыми поражен вектор  $\overline{f} + \mathbf{e}$  меньше, чем  $t < \frac{1}{2}(N - C \sqrt{m} \sqrt[4]{N})$ , то почти всегда рассмотренный алгоритм декодирования выдаст правильный вектор  $\overline{f}$ .

Сделаем несколько замечаний, которые позволяют усилить корректирующую способность рассмотренного алгоритма. Заметим, что производные  $\overline{f_\alpha}$  при различных  $\alpha$  связаны одна с другой линейными соотношениями. Поэтому, например, если  $\alpha^{(1)} + \alpha^{(2)} + \alpha^{(3)} = 0$ , то, как следует из (7.1.21),  $f_{\alpha^{(1)}} + f_{\alpha^{(2)}} + f_{\alpha^{(3)}} = \text{const}$ . Это и подобные этому соображения позволяют исправить с помощью особых алгоритмов ошибки, которые могли возникнуть при вычислении  $\overline{f_\alpha}^*$ . Подобные алгоритмы рассмотрены в работах [12] и [1].

Заметим, что сложность переборного алгоритма декодирования RM-кода второго порядка по максимуму правдоподобия (см. раздел 7.1.1) имеет порядок  $2^{1 + \binom{m}{1} + \binom{m}{2}}$ , где  $1 + \binom{m}{1} + \binom{m}{2}$  — размерность кода  $RM_{1,m}$ , т.е. сложность алгоритма декодирования по максимуму правдоподобия не является полиномиальной от его длины  $N = 2^m$ . в то время как рассмотренный алгоритм имеет сложность  $O(m^2 2^m)$ , т.е. является полиномиальным.

Вместе с тем алгоритм декодирования по максимуму правдоподобия исправляет почти всегда существенно большее число ошибок (см. раздел 7.1.7, следствие 7.1.2), чем рассмотренный алгоритм, т.е. в данном случае имеется альтернатива в использовании алгоритмов декодирования по максимуму правдоподобия и рассмотренного алгоритма: если мы хотим исправить максимальное число ошибок, то мы используем алгоритм декодирования по максимуму правдоподобия, если нам хватает для этого вычислительных мощностей. Если же это не так (не хватает вычислительных мощностей), то мы вынуждены использовать рассмотренный алгоритм декодирования или ему подобный.

### 7.1.6 Эффективность алгоритма декодирования в случае $r = 2$

В данном разделе эффективность алгоритма декодирования оценивается следующими двумя параметрами:

- 1. Сложностью алгоритма, т.е. числом операций необходимых для его реализации.

- 2. Максимальным числом ошибок в канале связи, при которых алгоритм декодирования работает почти всегда правильно.

Это не очень строгие понятия. Более развернутая их трактовка имеется в разделе 6.1.

Далее мы будем предполагать, что искаженный вектор  $\overline{f(\mathbf{x})}' = \overline{f(\mathbf{x})} + \mathbf{e}$  появляется выходе двоичного дискретного симметричного канала связи (ДСК), описанного в разделе 6.1, если на его вход подан вектор  $\overline{f(\mathbf{x})}$ . Таким образом, мы полагаем, что каждая координата вектора  $\overline{f(\mathbf{x})}$  искажается в канале независимо одна от другой, а вероятность того, что фиксированная координата вектора ошибки  $\mathbf{e}$  принимает значение 1, равна  $p$ ,  $0 \leq p < \frac{1}{2}$ . Это стандартные предположения, при которых изучаются эффективность алгоритмов декодирования.

Мы рассмотрим случайные величины  $\xi_\alpha$ ,  $\alpha \in \mathbb{F}_2^m$ , которые принимают значение 1 с вероятностью  $p = \frac{1-\varepsilon}{2}$  и значение 0 с вероятностью  $q = \frac{1+\varepsilon}{2}$ ,  $1 \geq \varepsilon \geq 0$ . Отметим, что запись вероятностей  $p$  и  $q$  в указанном виде  $\frac{1\pm\varepsilon}{2}$ , как будет видно ниже, является весьма удобной. Мы предполагаем, что случайные величины  $\xi_\alpha$ ,  $\alpha \in \mathbb{F}_2^m$ , являются независимыми. Обозначим через  $\bar{\xi}$  вектор  $\bar{\xi} = (\xi_{\alpha_1}, \dots, \xi_{\alpha_N})$ ,  $N = 2^m$ .

Как нетрудно установить,

$$P(\xi_\alpha + \xi_\beta = 1) = \frac{1 - \varepsilon^2}{2}, \quad \alpha \neq \beta. \quad (7.1.24)$$

(Упражнение) Тривиальным обобщением равенства (7.1.24) является соотношение

$$P(f(\alpha) + \xi_\alpha + f(\beta) + \xi_\beta = 1) = \frac{1 - (-1)^{f(\alpha)+f(\beta)}\varepsilon^2}{2}, \quad \alpha \neq \beta. \quad (7.1.25)$$

Введенные случайные величины  $\xi_\alpha$  позволяют сказать, что в рассматриваемой модели канала связи координата, индексированная элементом  $\alpha$ , искаженного вектора  $\overline{f(\mathbf{x})}'$  имеет вид  $f(\alpha) + e_\alpha$ , где  $e_\alpha$  — является реализацией случайной величины  $\xi_\alpha$ .

Обозначим через  $\mathbf{M}\kappa$  математическое ожидание или в другой терминологии среднее значение случайной величины  $\kappa$ .

Заметим, что из равенства (7.1.25) следует, что

$$\mathbf{M}(-1)^{f(\alpha)+\xi_\alpha} = (-1)^{f(\alpha)}\varepsilon \text{ и } \mathbf{M}(-1)^{f(\alpha)+\xi_\alpha+f(\beta)+\xi_\beta} = \begin{cases} (-1)^{f(\alpha)+f(\beta)}\varepsilon^2 & \text{if } \alpha \neq \beta \\ 1 & \text{if } \alpha = \beta \end{cases}. \quad (7.1.26)$$

Отсюда следует, что среднее число  $N_p$  ошибок в векторе  $\overline{f(\mathbf{x})}'$  будет равно

$$N_p = \mathbf{M}wt(\bar{\xi}) = \sum_{\mathbf{x} \in \mathbb{F}_2^m} \mathbf{M}wt(\xi_{\mathbf{x}}) = p2^m = 2^{m-1}(1 - \varepsilon), \quad (7.1.27)$$

Вычислить число ошибок  $N'_p$  в векторе  $\overline{f_\alpha(\mathbf{x})}'$  несколько сложнее. Имея в виду соотношение (7.1.26), где положено  $f(\mathbf{x}) = 0$ , получим при  $\alpha \neq 0$

$$N'_p = \sum_{\mathbf{x} \in \mathbb{F}_2^m} \mathbf{M}wt(\xi_{\mathbf{x}} + \xi_{\mathbf{x}+\alpha}) = \frac{1}{2} \sum_{\mathbf{x} \in \mathbb{F}_2^m} \mathbf{M}(1 - (-1)^{\xi_{\mathbf{x}}+\xi_{\mathbf{x}+\alpha}}) = 2^{m-1}(1 - \varepsilon^2) = 2^{m+1}pq. \quad (7.1.28)$$

Из равенства (7.1.28) следует, что среднее число ошибок  $N'_p$  в векторе  $\overline{f_\alpha(\mathbf{x})}'$  больше, чем среднее число ошибок в векторе  $\overline{f(\mathbf{x})}'$ , зато вектор  $\overline{f_\alpha(\mathbf{x})}$  принадлежит коду  $PM_{r-1,m}$ , если вектор  $\overline{f(\mathbf{x})}$  принадлежит коду  $PM_{r,m}$ .

### 7.1.7 Оценка вероятности ошибки декодирования кода по критерию максимального правдоподобия

Под декодированием двоичного кода  $\mathcal{K}$  длины  $n$  по критерию максимального правдоподобия или, другое название этого декодирования, — по критерию минимального расстояния, мы понимаем алгоритм  $\mathcal{A}_{\mathcal{K}}$ , у которого входом является вектор  $\mathbf{x} \in \mathbb{F}_2^n$ , а выходом — вектор  $\mathbf{y} \in \mathcal{K}$ , который является ближайшим в метрике Хемминга к вектору  $\mathbf{x}$  среди всех кодовых векторов кода  $\mathcal{K}$ .

Предположим, что вектор  $\mathbf{x}$  появился на выходе двоичного симметричного канала связи с вероятностью ошибки  $p$ , если на его вход был подан вектор  $\mathbf{y}_0 \in \mathcal{K}$ . Другими словами,  $\mathbf{x} = \mathbf{y}_0 + \mathbf{e}$ , где вектор ошибок  $\mathbf{e}$  является реализацией случайной величины  $\bar{\xi}$  (см. раздел 7.1.6).

Предположим, что вектор  $\mathbf{e}$  является реализацией случайной величины  $\bar{\xi}$ , а вектор  $\mathbf{y}_0 \in \mathcal{K}$  случайно и равновероятно выбирается среди всех элементов кода  $\mathcal{K}$ .

Вероятностью  $P_{er}(p, \mathcal{K})$  ошибочного декодирования по минимуму расстояния кода  $\mathcal{K}$ , мы называем вероятность неправильной работы алгоритма  $\mathcal{A}_{\mathcal{K}}$ , т.е.  $P_{er}(p, \mathcal{K})$  — вероятность того, что  $\mathbf{y} \neq \mathbf{y}_0$ .

Пусть  $\mathbf{x} \in \mathbb{F}_2^n$  и  $X \subseteq \mathbb{F}_2^n$ . Расстоянием  $d(\mathbf{x}, X)$  между вектором  $\mathbf{x}$  и множеством  $X$  называется величина

$$d(\mathbf{x}, X) = \min_{\mathbf{y} \in X} d(\mathbf{x}, \mathbf{y}). \quad (7.1.29)$$

Вектор  $\mathbf{e}$  мы называем выделенным для кода  $\mathcal{K}$ , если

$$d(\mathbf{e}, \mathcal{K} \setminus \{0\}) \leq wt(\mathbf{e}), \quad (7.1.30)$$

и называем невыделенным для кода  $\mathcal{K}$  в противном случае.

Заметим, что если  $d(\mathbf{e}, \mathbf{z}) \leq wt(\mathbf{e})$  для некоторого  $\mathbf{z} \in \mathcal{K}$ , то для любого  $\mathbf{y}_0 \in \mathcal{K}$  справедливо неравенство  $d(\mathbf{e} + \mathbf{y}_0, \mathbf{z} + \mathbf{y}_0) \leq d(\mathbf{y}_0, \mathbf{y}_0 + \mathbf{e}) = wt(\mathbf{e})$ . Отсюда следует, что если на выходе канала связи появился вектор  $\mathbf{y}_0 + \mathbf{e}$ , где  $\mathbf{e}$  — выделенный вектор и  $\mathbf{y}_0 \in \mathcal{K}$ , то, он не всегда будет правильно декодирован алгоритмом  $\mathcal{A}_{\mathcal{K}}$ , ибо в коде  $\mathcal{K}$  существует вектор  $\mathbf{z} + \mathbf{y}_0 \neq \mathbf{y}_0$ , который расположен на расстоянии меньшем или равном  $d(\mathbf{y}_0, \mathbf{y}_0 + \mathbf{e}) = wt(\mathbf{e})$ .

Таким образом, алгоритмом декодирования  $\mathcal{A}_{\mathcal{K}}$  достоверно правильно декодирует вектор  $\mathbf{y}_0 + \mathbf{e}$  тогда и только тогда, когда вектор  $\mathbf{e}$  является невыделенным для кода  $\mathcal{K}$ . Если же вектор  $\mathbf{e}$  является выделенным, то алгоритмом декодирования  $\mathcal{A}_{\mathcal{K}}$  может выдать как вектор  $\mathbf{y}_0$ , так и вектор  $\mathbf{y}_0 + \mathbf{z}$ , отличный от  $\mathbf{y}_0$ , т.е. в этом случае алгоритм  $\mathcal{A}_{\mathcal{K}}$  не работает достоверно правильно.

Предположим, что в канале связи произошло  $t$  ошибок, т.е. произошло событие  $wt(\xi) = t$ . Условная вероятность  $P(p, \mathcal{K} / wt(\xi) = t)$  для этого случая, очевидно, удовлетворяет равенству

$$P_{er}(p, \mathfrak{K}/wt(\xi) = t) \leq \frac{M(t, \mathfrak{K})}{\binom{n}{t}}, \quad (7.1.31)$$

где  $M(t, \mathfrak{K})$  — число выделенных векторов веса  $t$  для кода  $\mathfrak{K}$ . Величину  $P_{er}(p, \mathfrak{K}/wt(\xi) = t)$  мы называем условной вероятности ошибочного декодирования по критерию минимального расстояния или вероятностью ошибки по критерию минимального расстояния.

Пусть  $wt(\mathbf{x}) = s$ . Число  $H(t, s)$  векторов  $\mathbf{e}$  веса  $t$ , для которых справедливо  $d(\mathbf{e}, \mathbf{x}) \leq t$ , равно

$$H(t, s) = \sum_{\frac{s}{2} \leq j \leq t} \binom{s}{j} \binom{n-s}{t-j}. \quad (7.1.32)$$

(Упражнение)

**Лемма 7.1.3** Для линейного двоичного кода  $\mathfrak{K}$  имеет место оценка

$$M(t, \mathfrak{K}) \leq \sum_{\mathbf{x} \in \mathfrak{K}, \mathbf{x} \neq 0} H(t, wt(\mathbf{x})) = \sum_{0 < s \leq 2t} \eta_s H(t, s), \quad (7.1.33)$$

где  $\eta_s$  — число векторов веса  $s$  в коде  $\mathfrak{K}$ .

Лемма очевидна.

Последующие результаты этого раздела получены с помощью достаточно громоздких, но, по существу, тривиальных оценок правой части (7.1.33) применительно к коду  $RM_{r,m}$ . Заметим, что подобные результаты могут быть получены и для многих других линейных кодов.

**Теорема 7.1.2** Для условной вероятности  $P_{er}(p, \mathfrak{K}/wt(\xi) = t)$ ,  $t < \frac{N}{2}$ , ошибочного декодирования по критерию минимального расстояния кода Руда-Маллера  $RM_{r,m}$  длины  $N = 2^m$  и размерности  $\dim RM_{r,m} = \sum_{j=0}^r \binom{N}{j}$  при  $m \rightarrow \infty$ ,  $r = \text{const}$  и числе ошибок  $t = \frac{N - \lambda\sqrt{N}}{2}$ ,  $\lambda > 0$ , справедлива оценка

$$P_{er}(p, \mathfrak{K}/wt(\xi) = t) \leq C \exp_2 \left( -\frac{1}{2 \ln 2} \lambda^2 \varepsilon(r) + \dim RM_{r,m} \right)^{\frac{1}{2}}, \quad (7.1.34)$$

где  $\varepsilon(r) = (2^r - 1)^{-1}$  и  $C$  — абсолютная постоянная.

В частности, при

$$\lambda = 2((2^r - 1) \ln 2 \dim RM_{r,m})^{\frac{1}{2}} \quad (7.1.35)$$

получаем, что

$$P_{er}(p, \mathfrak{K}/wt(\xi) = t) \leq C \exp_2(-\dim RM_{r,m}) = C |RM_{r,m}|^{-1}. \quad (7.1.36)$$

**Доказательство.** Заметим, что для кода  $RM_{r,m}$  величина  $\eta_s$  равна нулю, если  $0 < s < N2^{-r}$  или  $N(1 - 2^{-r}) < s < N$ . Отсюда и из (7.1.33) получим

$$M(t, \mathfrak{K}) \leq |RM_{r,m}| \max H(t, s), \quad (7.1.37)$$

где максимум берется по все четным  $s$  из интервала  $[N2^{-r}, N(1-2^{-r})]$  изменения параметра  $s$ .

Для доказательства теоремы с учетом соотношения (7.1.31), достаточно показать, что  $\max H(t, s)$  существенно меньше числа  $\binom{N}{t}$ .

Заметим, что для любого целого и неотрицательного числа  $s$  справедливо

$$\sum_{i=0}^s \binom{s}{i} \binom{N-s}{t-i} = \binom{N}{t}. \quad (7.1.38)$$

Сумма  $H(t, s) = \sum_{\frac{s}{2} \leq i \leq t} \binom{s}{i} \binom{N-s}{t-i}$  является частью суммы (7.1.38). Поэтому для доказательства указанного выше утверждения надо показать, что в случае  $s \in [N2^{-r}, N(1-2^{-r})]$  сумма  $H(t, s)$  образована слагаемыми, величина которых существенно меньше максимальных значений слагаемых в сумме (7.1.38).

Положим  $t = \frac{1}{2}(N - \lambda\sqrt{N})$  и  $i = \frac{s}{2} + j$ , где  $s$  — четное число. Представим функцию  $H(t, s)$  в виде

$$H(t, s) = \sum_{j=0}^{\frac{1}{2}s} \binom{s}{\frac{1}{2}s + i} \binom{N-s}{\frac{1}{2}(N-s-\lambda\sqrt{N})-i}. \quad (7.1.39)$$

Функции  $\binom{s}{\frac{1}{2}s+i}$  и  $\binom{N-s}{\frac{1}{2}(N-s-\lambda\sqrt{N})-i}$  являются убывающими функциями параметра  $i$ . Поэтому наибольшим является первый член суммы в (7.1.39). Следовательно

$$H(t, s) \leq \binom{s}{\frac{1}{2}s} \binom{N-s}{\frac{1}{2}(N-s-\lambda\sqrt{N})} \rho(s). \quad (7.1.40)$$

где  $\rho(s)$  — некоторая медленно растущая функция. В частности, для нее справедлива оценка  $\rho(s) \leq \frac{s}{2} + 1$ , где  $\frac{s}{2} + 1$  — число слагаемых в сумме (7.1.39). Как нетрудно показать, используя асимптотическое представление для биномиальных коэффициентов (см. (2.0.1)), для функции справедлива и более сильная оценка

$$\rho(s) \leq C_1 \sqrt{N}, \quad (7.1.41)$$

где  $C_1$  — постоянная, не зависящая от  $s$ .

Из соотношения  $\binom{2k}{k-u} \leq C_2 k^{-\frac{1}{2}} \exp_2\{2kH(\frac{k-u}{2k})\}$ , где  $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$  — функция энтропии, справедливого при больших  $k$  и  $0 \leq u \leq C_3 k$ ,  $0 \leq C_3 < 1$  (см. (2.0.44)) вытекает, что

$$H(t, s) \leq C_4 N^{-\frac{1}{2}} \exp_2 \left\{ s + (N-s) H \left( \frac{N-s-\lambda\sqrt{N}}{2(N-s)} \right) \right\}. \quad (7.1.42)$$

С другой стороны,

$$\binom{N}{t} = C_5 N^{-\frac{1}{2}} \exp_2 \left\{ NH \left( \frac{t}{N} \right) \right\} = C_5 N^{-\frac{1}{2}} \exp_2 \left\{ NH \left( \frac{N-\lambda\sqrt{N}}{2N} \right) \right\}. \quad (7.1.43)$$

Отсюда и из (7.1.42) получим, что

$$\frac{H(t, s)}{\binom{N}{t}} \leq C_6 \exp_2 \left\{ s + (N-s) H \left( \frac{N-s-\lambda\sqrt{N}}{2(N-s)} \right) - NH \left( \frac{1}{2} - \frac{\lambda}{2\sqrt{N}} \right) \right\}. \quad (7.1.44)$$

Функция  $s + (N - s)H\left(\frac{N-s-\lambda\sqrt{N}}{2(N-s)}\right)$ , зависящая от параметра  $s$ , является монотонно убывающей на интервале  $[2^{-r}N, (1 - 2^{-r})N]$  изменения  $s$ . Поэтому она принимает максимальное значение  $N\left(2^{-r} + (1 - 2^{-r})H\left(\frac{1}{2} - \frac{\lambda}{2(1-2^{-r})\sqrt{N}}\right)\right)$  при  $s = 2^{-r}N$ .

Используя соотношение

$$H\left(\frac{1}{2}(1-x)\right) = 1 - \ln^{-1} 2 \sum_{j=1}^{\infty} \frac{x^{2j}}{2j(2j-1)} < 1 - \frac{x^2}{2 \ln 2}, \quad (7.1.45)$$

получим, что

$$2^{-r} + (1 - 2^{-r})H\left(\frac{1}{2} - \frac{\lambda}{2(1-2^{-r})\sqrt{N}}\right) - H\left(\frac{1}{2} - \frac{\lambda}{2\sqrt{N}}\right) < -\frac{\lambda^2}{2N(2^r - 1) \ln 2} \quad (7.1.46)$$

Из этой оценки и (7.1.44) вытекает оценка

$$\frac{H(t, s)}{\binom{N}{t}} \leq C_7 \exp_2 \left\{ \frac{\varepsilon(r) \lambda^2}{2 \ln 2} \right\} \quad (7.1.47)$$

Утверждение теоремы вытекает из последенного соотношения и неравенства (7.1.31).  $\square$

Следующее следствие непосредственно вытекает из теоремы 7.1.2.

**Следствие 7.1.2** Пусть  $m \rightarrow \infty$ ,  $r = \text{const}$ . Алгоритм  $\mathfrak{A}_{RM_r, m}$  декодирования кода  $RM_{r, m}$  по минимуму расстояния исправляет правильно почти все ошибки  $\mathbf{e}$ , если  $t = wt(\mathbf{e}) < \frac{1}{2}(N - C_r m^{\frac{r}{2}} \sqrt{N})$ , где  $C_r$  — некоторая постоянная, зависящая только от  $r$ .

Заметим, что теорема 7.1.2 впервые была доказана в работе [13].

## 7.2 Другие способы представления векторов RM-кода

Мы рассматривали RM-код как множество векторов, координаты которых являются значений на пространстве  $\mathbb{F}_2^m$  некоторых многочленов над  $\mathbb{F}_2$  от  $m$  переменных в точках пространства  $\mathbb{F}_2^m$ .

Пространство  $\mathbb{F}_2^m$  можно рассматривать и как аддитивную группы конечного поля  $\mathbb{F}_{2^m}$ . В этом случае в пространстве  $\mathbb{F}_2^m$  появляется дополнительная операция (умножение). Как будет показано ниже, возможно рассматривать многочлены, порождающие RM-код, как многочлены над полем конечным полем  $\mathbb{F}_{2^m}$  от одной переменной, принимающие значения в поле  $\mathbb{F}_2$ . Эта техника, как будет видно ниже, поможет нам найти новые семейства "хороших" подкодов RM-кодов и выявить новые их свойства. В частности, использование поля  $\mathbb{F}_{2^m}$ , позволяет представить RM-код в циклическом виде. Далее мы будем рассматривать только поле характеристики 2, хотя многие результаты этого раздела могут быть получены и для полей характеристики  $p > 2$ .

Функцию  $Tr(x) = x + x^2 + \dots + x^{2^{m-1}}$ ,  $x \in \mathbb{F}_{2^m}$ , в более общем случае мы рассматривали в разделе 5.1.3, соотношение (6.1.4). Мы будем изучать функции вида  $Tr(f(x))$ , где  $f(x) = \sum_{i=0}^t \alpha_i x^i$  — многочлен с коэффициентами из поля  $\mathbb{F}_{2^m}$ .

Если рассматривать элемент  $x$  как  $m$ -мерный двоичный вектор, у которого координатами являются коэффициентами в представлении  $x$  в некотором базисе поля  $\mathbb{F}_{2^m}$  над

полем  $\mathbb{F}_2$ , то функция  $Tr(x) \in \mathbb{F}_2$  будет булевой функцией, ибо, как нетрудно установить,  $Tr^2(x) = Tr(x)$ . (Упражнение) Подобные функции были уже использованы в одном из представлений циклических кодов (см. Теорему 5.1.2).

**Замечание 7.2.1** Пусть  $\Omega = \{\omega_1, \dots, \omega_m\}$  — какой-либо базис поля  $\mathbb{F}_{p^m}$  над полем  $\mathbb{F}_p$ . Запишем произвольный элемент  $\mathbf{x} \in \mathbb{F}_{2^m}$  в виде

$$\mathbf{x} = x_1\omega_1 + \dots + x_m\omega_m, \quad x_j \in \mathbb{F}_p. \quad (7.2.1)$$

Отсюда вытекает, что функция  $Tr(f(\mathbf{x}))$ ,  $f(\mathbf{x}) = \sum_{i=0}^t \alpha_i \mathbf{x}^i \in \mathbb{F}_{2^m}[\mathbf{x}]$ , может быть представлена как многочлен от переменных  $x_1, \dots, x_m \in \mathbb{F}_p$ , принимающих значение в поле  $\mathbb{F}_p$  с коэффициентами из поля  $\mathbb{F}_p$ , следующим образом

$$\begin{aligned} Tr(f(\mathbf{x})) &= \sum_{i=0}^t Tr(\alpha_i(x_1\omega_1 + \dots + x_m\omega_m)^i) = \\ &= \sum_{i=0}^t \sum_{1 \leq j_1, \dots, j_i \leq m} x_{j_1} \dots x_{j_i} Tr(\alpha_i \omega_{j_1} \dots \omega_{j_i}). \end{aligned} \quad (7.2.2)$$

Мы будем использовать понятие "циклотомический класс"  $C_h$ , введенное в начале раздела 5.2.5. Напомним, что числа  $j$  и  $j'$  принадлежат одному циклотомическому классу  $C_h = \{hp^s \bmod (p^m - 1) \mid s = 0, \dots, m-1\}$ , если  $j' = jp^u \equiv hp^s \bmod (p^m - 1)$  для некоторых  $u, s$ ,  $0 \leq u, s < m$ .

Пусть  $0 \leq j \leq p^m - 1$  и  $j = j_0 + j_1p + \dots + j_{m-1}p^{m-1}$ ,  $j_i = \{0, \dots, p-1\}$ , — представление целого числа  $j$  по основанию  $p$  и  $\bar{j} = \{j_0, j_1, \dots, j_{m-1}\}$ . Очевидно, вектор  $\overline{j\bar{p}} = \{j_{m-1}, j_0, \dots, j_{m-2}\}$  является циклическим сдвигом вектора  $\bar{j}$  на один разряд вправо.

Циклотомический вес  $ws(j)$  числа  $j$  определяется как  $ws(j) = j_0 + \dots + j_{m-1}$ , где последняя сумма вычисляется в поле действительных чисел. Очевидно,  $ws(j) = ws(j')$ , если  $j$  и  $j'$  принадлежат одному циклотомическому классу  $C_h$ .

**Лемма 7.2.1** Степень ненулевого многочлена  $Tr(\alpha(x_1\omega_1 + \dots + x_m\omega_m)^j)$  от переменных  $x_1, \dots, x_m$ , принимающих значения в поле  $\mathbb{F}_p$ , не превосходит числа  $ws(j)$ .

**Доказательство.** Нетрудно установить, что

$$Tr(\alpha(x_1\omega_1 + \dots + x_m\omega_m)^j) = Tr(\alpha \prod_{u=0}^{m-1} (x_1\omega_1^{p^u} + \dots + x_m\omega_m^{p^u})^{j_u}). \quad (7.2.3)$$

Степень каждого многочлена  $(x_1\omega_1^{p^u} + \dots + x_m\omega_m^{p^u})^{j_u}$ , очевидно, не превосходит  $j_u$ . Следовательно, степень многочлена  $Tr(\alpha(x_1\omega_1 + \dots + x_m\omega_m)^j)$  не превосходит числа  $ws(j)$ . (Упражнение.)  $\square$

Как и прежде, через  $\overline{Tr}(f(\mathbf{x}))$ ,  $f(\mathbf{x}) \in \mathbb{F}_{p^m}[\mathbf{x}]$ , будем обозначать вектор значений функции  $Tr(f(\mathbf{x}))$ , т.е.  $\overline{Tr}(f(\mathbf{x})) = (Tr(f(\alpha_1)), \dots, Tr(f(\alpha_{p^m})))$ , где  $\{\alpha_1, \dots, \alpha_{p^m}\} = \mathbb{F}_{p^m}$ .

**Теорема 7.2.1** Пусть  $p = 2$  и  $LT_r$  линейное пространство, натянутое на функции  $\overline{Tr}(\alpha \mathbf{x}^j) = \overline{Tr}(\alpha(x_1\omega_1 + \dots + x_m\omega_m)^j)$ ,  $\alpha \in \mathbb{F}_{2^m}$ , у которых  $ws(j) \leq r$ .

Тогда  $LT_r = RM_r$ .



**Доказательство.** Из леммы 7.2.1 следует, что  $LT_m \subseteq RM_r$ .

Для доказательства обратного включения покажем, что  $\dim LT_m \geq \dim RM_r$ .

Рассмотрим множество  $\mathfrak{C}_r$  всех чисел  $j$ , у которых  $wc(j) \leq r$ . Очевидно,  $\mathfrak{C}_r$  состоит из всех двоичных векторов  $\bar{j}$  (определение см. в разделе 5.2.5), вес (в данном двоичном случае это обычный вес  $wt(\bar{j})$  вектора в Хемминговом пространстве) которых не превосходит  $r$ . Таким образом,  $|\mathfrak{C}_r| = 1 + \binom{m}{1} + \dots + \binom{m}{r}$ .

Очевидно, множество  $\mathfrak{C}_r$  является объединением некоторых циклотомических классов  $C_h$ :

$$\mathfrak{C}_r = \bigcup_{wc(h) \leq r} C_h, \quad (7.2.4)$$

где объединение производится по всем различным циклотомическим классам  $C_h$ , представители  $h$  которых имеют циклотомический вес не выше  $r$ .

Как нетрудно установить (Упражнение), размерность пространства  $\{Tr(\alpha \mathbf{x}^j) | \alpha \in \mathbb{F}_{2^m}\}$  равна  $|C_h|$ , где  $C_h$  — циклотомический класс, к которому принадлежит число  $j$ .

С другой стороны, очевидно, что множество ненулевых многочленов  $\{Tr(\alpha_j \mathbf{x}^j) | j \in J\}$ , где  $J$  произвольное множество чисел, принадлежащих различным циклотомическим классам  $C_h$ , является линейно-независимым.

Отсюда следует, пространство, натянутое на множество многочленов  $\{Tr(\mathbf{x}^j) | j \in \mathfrak{C}_r; \alpha \in \mathbb{F}_{2^m}\}$  имеет размерность не меньшую, чем

$$\sum_{wc(h) \leq r} |C_h| = |\mathfrak{C}_r| = 1 + \binom{m}{1} + \dots + \binom{m}{r}, \quad (7.2.5)$$

где суммирование в сумме  $\sum_{wc(h) \leq r}$  производится по всем различным циклотомическим классам  $C_h$ , представители  $h$  которых имеют циклотомический вес не выше  $r$ . Это доказывает теорему.  $\square$

Теорема 7.2.1 позволяет в следующей главе построить и изучить несколько интересных подкодов RM-кода.



# Глава 8

## Некоторые частные классы кодов

### 8.1 Вспомогательные результаты. Вычисление некоторых тригонометрических сумм.

Положим  $Tr(x) = x + x^2 + \dots + x^{2^{m-1}}$ .

**Лемма 8.1.1** Если  $b \neq 0$ , то

$$\sum_{\mathbf{x} \in \mathbb{F}_{2^m}} (-1)^{Tr(b\mathbf{x})} = 0. \quad (8.1.1)$$

**Доказательство.** (Упражнение)

Положим

$$Q(a, b) = \sum_{\mathbf{x} \in \mathbb{F}_{2^m}} (-1)^{Tr(a\mathbf{x}^3 + b\mathbf{x})} \quad (8.1.2)$$

**Лемма 8.1.2** Имеют место соотношения.

Если число  $m = 2t - 1$  нечетное число и  $a \neq 0$ , то

$$|Q(a, b)| = \begin{cases} 0, & \text{если } Tr(b) = 1, \\ 2^{\frac{m+1}{2}}, & \text{если } Tr(b) = 0 \end{cases}. \quad (8.1.3)$$

Если число  $m = 2t$  четное число и  $a \neq 0$ , то

$$|Q(a, b)| = \begin{cases} 2^{\frac{m}{2}}, & \text{если уравнение } 1 + az^3 = 0, \\ & \text{не имеет решений в поле } \mathbb{F}_{2^m}, \\ 2^{\frac{m+2}{2}}, & \text{если уравнение } 1 + az^3 = 0, \\ & \text{имеет решение в поле } \mathbb{F}_{2^m} \text{ и } Tr_4(ba^{-\frac{1}{3}}) = 0, \\ 0, & \text{если уравнение } 1 + az^3 = 0, \\ & \text{имеет решение в поле } \mathbb{F}_{2^m} \text{ и } Tr_4(ba^{-\frac{1}{3}}) \neq 0 \end{cases}, \quad (8.1.4)$$

где  $Tr_4(x) = \sum_{s=0}^t x^{2^{2s}}$  — линейная над  $\mathbb{F}_4$  функция, отображающая элементы поля  $\mathbb{F}_{2^m}$  в элементы поля  $\mathbb{F}_4$ .

Если  $a = 0$  и  $b \neq 0$ , то

$$Q(a, b) = 0. \quad (8.1.5)$$

**Доказательство.** Очевидно,

$$\begin{aligned} Q^2(a, b) &= \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(a\mathbf{x}^3 + b\mathbf{x} + a\mathbf{y}^3 + b\mathbf{y})} = \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(a(\mathbf{y} + \mathbf{z})^3 + b(\mathbf{y} + \mathbf{z}) + a\mathbf{y}^3 + b\mathbf{y})} = \\ &= \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(a(\mathbf{z}\mathbf{y}^2 + \mathbf{z}^2\mathbf{y} + a\mathbf{z}^3) + b\mathbf{z})} = \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(a\mathbf{y}^2(\mathbf{z} + a\mathbf{z}^4) + a\mathbf{z}^3 + b\mathbf{z})}. \end{aligned} \quad (8.1.6)$$

Заметим, что последнее равенство следует из соотношения  $Tr(\mathbf{z}) = Tr(\mathbf{z}^2)$ .

Очевидно, при  $a \neq 0$

$$= \sum_{\mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(a\mathbf{y}^2(a\mathbf{z}^4 + \mathbf{z}))} = \begin{cases} 0, & \text{если } a\mathbf{z}^4 + \mathbf{z} \neq 0, \\ 2^m, & \text{если } a\mathbf{z}^4 + \mathbf{z} = 0 \end{cases}. \quad (8.1.7)$$

Отсюда

$$Q^2(a, b) = 2^m \widetilde{\sum} (-1)^{Tr(1 + b\mathbf{z})}, \quad (8.1.8)$$

где суммирование в сумме  $\widetilde{\sum}$  производится по всем корням уравнения  $a\mathbf{z}^4 + \mathbf{z} = 0$ , принадлежащим полю  $\mathbb{F}_{2^m}$ .

Очевидно, корнями уравнения  $\mathbf{z} + a\mathbf{z}^4 = 0$ ,  $a \neq 0$ , являются  $\mathbf{z}_0 = 0$  и корни уравнения  $1 + a\mathbf{z}^3 = 0$ .

Если число  $m$  является нечетным, то последнее уравнение имеет одно решение  $\mathbf{z}_0 = a^{-\frac{1}{3}}$ , ибо число 3 не делит число  $2^m - 1$  — порядок мультипликативной группы поля  $\mathbb{F}_{2^m}$ . В этом случае из соотношения (8.1.8) следует

$$Q^2(a, b) = 2^m \left( 1 + (-1)^{Tr(1 + ba^{-\frac{1}{3}})} \right) = 2^m \left( 1 - (-1)^{Tr(ba^{-\frac{1}{3}})} \right), \quad (8.1.9)$$

в виду того, что в рассматриваемом случае  $Tr(1) = 1$ . (Упражнение)

Если же число  $m$  является четным, то уравнение  $1 + a\mathbf{z}^3 = 0$ ,  $a \neq 0$ , либо не имеет решения в поле  $\mathbb{F}_{2^m}$ , либо имеет три различных решения:  $\mathbf{z}_0, \xi\mathbf{z}_0, \xi^2\mathbf{z}_0$ , где  $\xi$  — ненулевой, отличный от 1, элемент поля  $\mathbb{F}_4 \subseteq \mathbb{F}_{2^m}$ . В этом случае из соотношения (8.1.8) следуют соотношения (8.1.4).

Заметим, что второе и третье равенства в (8.1.4) следует из того, что при  $c \in \mathbb{F}_{2^m}$

$$\sum_{\xi \in \mathbb{F}_4} (-1)^{Tr(\xi c)} = \begin{cases} 0, & \text{если } T_4(c) \neq 0, \\ 4, & \text{если } T_4(c) = 0 \end{cases}, \quad (8.1.10)$$

. (Упражнение)  $\square$

**Следствие 8.1.1** Число решений  $N(a, b)$  уравнения

$$Tr(a\mathbf{x}^3 + b\mathbf{x}) = 0, \quad \mathbf{x} \in \mathbb{F}_{2^l} \quad (8.1.11)$$

равное

$$N(a, b) = \frac{1}{2}(2^m - Q(a, b)), \quad m > 2, \quad (8.1.12)$$

положительно, т.е. уравнение (8.1.11) всегда имеет решение.

Положим

$$s(a\mathbf{x}) = \sum_{i=0}^t (a\mathbf{x})^{2^i+1}, \quad a \in \mathbb{F}_{2^m} \quad (8.1.13)$$

и

$$T(a, b) = \sum_{\mathbf{x} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{x})+b\mathbf{x})}. \quad (8.1.14)$$

Как легко установить, что

$$s(a\mathbf{z} + a\mathbf{y}) = s(a\mathbf{z}) + s(a\mathbf{y}) + \sum_{i=0}^t ((a\mathbf{z})^{2^i} a\mathbf{y} + (a\mathbf{y})^{2^i} a\mathbf{z}), \quad a, b \in \mathbb{F}_{2^m}. \quad (8.1.15)$$

**Лемма 8.1.3** Пусть  $m = 2t - 1$  и  $a \neq 0$ .

Тогда имеет место соотношение

$$|T(a, b)| = 2^m \left( 1 + (-1)^{Tr(\frac{b}{a})} \right) = \begin{cases} 0, & \text{если } Tr(\frac{b}{a}) = 1, \\ 2^{\frac{m+1}{2}}, & \text{если } Tr(\frac{b}{a}) = 0 \end{cases}. \quad (8.1.16)$$

**Доказательство.** Очевидно,

$$\begin{aligned} T^2(a, b) &= \sum_{\mathbf{x}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{x})+b\mathbf{x})+s(a\mathbf{y})+b\mathbf{y})} = \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{z}+a\mathbf{y})+s(a\mathbf{y})+b\mathbf{z})} = \\ &= \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{z})+\sum_{i=0}^t ((a\mathbf{z})^{2^i} a\mathbf{y} + (a\mathbf{y})^{2^i} a\mathbf{z}) + b\mathbf{z})} = \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{z})+a\mathbf{y}\sum_{i=0}^t ((a\mathbf{z})^{2^i} + (a\mathbf{z})^{2^{-i}}) + b\mathbf{z})} = \\ &= 2^m \widetilde{\sum} (-1)^{Tr(s(a\mathbf{z})+b\mathbf{z})}, \end{aligned} \quad (8.1.17)$$

где суммирование в сумме  $\widetilde{\sum}$  производится по всем корням уравнения

$$\sum_{i=0}^t ((a\mathbf{z})^{2^i} + (a\mathbf{z})^{2^{-i}}) = 0, \quad (8.1.18)$$

которые принадлежат полю  $\mathbb{F}_{2^m}$ .

Так как  $(a\mathbf{z})^{2^{-i}} = (a\mathbf{z})^{2^{m-i}}$ , то  $\sum_{i=0}^t ((a\mathbf{z})^{2^i} + (a\mathbf{z})^{2^{-i}}) = \sum_{i=1}^{m-1} (a\mathbf{z})^{2^i} = f(\mathbf{x})$ . Многочлен  $f(\mathbf{x})$ , очевидно, при  $\mathbf{x} \in \mathbb{F}_m$  совпадает с функцией  $(Tr_{m-1}(a\mathbf{x}))^2$ , где  $Tr_{m-1}(\mathbf{y})$  — функция след для поля  $\mathbb{F}_{2^{m-1}}$ . Все корни многочлена  $Tr_{m-1}(\mathbf{y})$  степени  $2^{m-2}$  принадлежат полю  $\mathbb{F}_{2^{m-1}}$  (Упражнение).

Поэтому множество корней многочлена  $(Tr_{m-1}(\mathbf{y}))^2$ , принадлежащими полю  $\mathbb{F}_{2^m}$ , являются элементы поля  $\mathbb{F}_2 = \mathbb{F}_{2^m} \cap \mathbb{F}_{2^{m-1}}$ . Отсюда следует, что корнями уравнения (8.1.18), принадлежащими полю  $\mathbb{F}_{2^m}$ , являются элементы 0 и  $a^{-1}$ .

Отсюда и из соотношения (8.1.17) вытекает равенство (8.1.16).  $\square$

Положим

$$T(a, a', b) = \sum_{\mathbf{x} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{x})+s(a'\mathbf{x})+b\mathbf{x})}. \quad (8.1.19)$$

Лемму 8.1.3 обобщим следующим образом:

**Лемма 8.1.4** Пусть  $m = 2t - 1$  (нечетное) и  $a, a' \neq 0, a \neq a'$ .

Тогда имеет место соотношение

$$|T(a, a', b)|^2 = \left| \sum_{\mathbf{x} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{x}) + s(a'\mathbf{x}) + b\mathbf{x})} \right|^2 =$$

$$= \begin{cases} 2^m \left( 1 + (-1)^{Tr(s(\frac{a^2}{a^2+a'^2}) + s(\frac{aa'}{a^2+a'^2}) + \frac{ab}{a^2+a'^2})} \right), & \text{если } Tr(\frac{a}{a+a'}) = 1, \\ 2^m \left( 1 + (-1)^{Tr(s(\frac{a'^2}{a^2+a'^2}) + s(\frac{aa'}{a^2+a'^2}) + \frac{a'b}{a^2+a'^2})} \right), & \text{если } Tr(\frac{a'}{a+a'}) = 1 \end{cases}. \quad (8.1.20)$$

**Доказательство.** Сначала заметим, что  $Tr(\frac{a}{a+a'}) + Tr(\frac{a'}{a+a'}) = Tr(1) = 1$ . Поэтому все пары  $(a, a')$  удовлетворяют одному из условий  $Tr(\frac{a}{a+a'}) = 1$  или  $Tr(\frac{a'}{a+a'}) = 1$ , если  $a \neq a', a \neq 0, a' \neq 0$ .

Доказательство использует доказательство леммы 8.1.3. В частности, последнее равенство в (8.1.17) в условиях леммы примет вид

$$T^2(a, a', b) = \sum_{\mathbf{z}, \mathbf{y} \in \mathbb{F}_{2^m}} (-1)^{Tr(s(a\mathbf{z}) + s(a'\mathbf{z}) + a\mathbf{y} \sum_{i=0}^t ((a\mathbf{z})^{2^i} + (a\mathbf{z})^{2^{-i}}) + a'\mathbf{y} \sum_{i=0}^t ((a'\mathbf{z})^{2^i} + (a'\mathbf{z})^{2^{-i}}) + b\mathbf{z})} =$$

$$= 2^m \widetilde{\sum} (-1)^{Tr(s(a\mathbf{z}) + s(a'\mathbf{z}) + b\mathbf{z})}, \quad (8.1.21)$$

где суммирование в сумме  $\widetilde{\sum}$  производится по всем корням уравнения

$$a \sum_{i=0}^t ((a\mathbf{z})^{2^i} + (a\mathbf{z})^{2^{-i}}) + a' \sum_{i=0}^t ((a'\mathbf{z})^{2^i} + (a'\mathbf{z})^{2^{-i}}) =$$

$$= a(a\mathbf{z} + Tr(a\mathbf{z})) + a'(a'\mathbf{z} + Tr(a'\mathbf{z})) = \mathbf{z}(a^2 + a'^2) + aTr(a\mathbf{z}) + a'Tr(a'\mathbf{z}) = 0, \quad (8.1.22)$$

которые принадлежат полю  $\mathbb{F}_{2^m}$ .

Отсюда следует, что корнями последнего уравнения могут быть только следующие множества значений  $\mathbf{z}$ :

- i.  $\{0, \frac{1}{a+a'}\}$ , если  $Tr(\frac{a}{a+a'}) = 1, Tr(\frac{a'}{a+a'}) = 1$ ,
- ii.  $\{0, \frac{a}{a^2+a'^2}\}$ , если  $Tr(\frac{a}{a+a'}) = 1, Tr(\frac{a'}{a+a'}) = 0$ ,
- iii.  $\{0, \frac{a'}{a^2+a'^2}\}$ , если  $Tr(\frac{a}{a+a'}) = 0, Tr(\frac{a'}{a+a'}) = 1$ ,
- iv.  $\{0\}$ , если  $Tr(\frac{a}{a+a'}) = 0, Tr(\frac{a'}{a+a'}) = 0$ .

Отметим, что пункты i. и iv. не могут реализоваться, так как  $Tr(\frac{a}{a+a'}) + Tr(\frac{a'}{a+a'}) = Tr(\frac{a}{a+a'} + \frac{a'}{a+a'}) = Tr(1) = 1$ .

Поэтому корнями уравнения (8.1.22) являются либо множество  $\{0, \frac{a}{a^2+a'^2}\}$ , либо множество  $\{0, \frac{a'}{a^2+a'^2}\}$ . Для определенности, без ограничения общности, мы будем полагать, что множество  $\{0, \frac{a}{a^2+a'^2}\}$  является множеством корней уравнения (8.1.22).

Таким образом из (4.1.1) вытекает, что

$$T^2(a, a', b) = 2^m \left( 1 + (-1)^{Tr \left( s\left(\frac{a^2}{a^2+a'^2}\right) + s\left(\frac{aa'}{a^2+a'^2}\right) + \frac{ab}{a^2+a'^2} \right)} \right). \quad (8.1.23)$$

Из этого равенства вытекает утверждение доказываемой леммы.  $\square$

Заметим, что лемму 8.1.4 можно доказать и несколько иначе: а именно, основываясь на соотношении (8.6.1), можно использовать для ее доказательства лемму 8.1.3. Этот способ по мнению автора не проще приведенного доказательства леммы 8.1.4.

Как вытекает из леммы 8.1.20 и из теоремы Диксона о представлении многочлена степени два над полем  $\mathbb{F}_2$  в каноническом виде (см., например, [7]), непосредственно вытекает

**Следствие 8.1.2** *При любых  $a, a', b \in \mathbb{F}_q$ ,  $a \neq a'$ , функция  $Tr(s(a\mathbf{x}) + s(a'\mathbf{x}) + b\mathbf{x})$  второго порядка может быть в новых переменных  $\mathbf{y} = \mathbf{x}A$ , где  $\mathbf{x} = (x_1, \dots, x_m)$  и  $A$  — невырожденная матрица, представлена в виде*

$$Tr(s(a\mathbf{x}) + s(a'\mathbf{x}) + b\mathbf{x}) = \sum_{i=1}^{\frac{m-1}{2}} y_{2i-1}y_{2i} + \alpha y_m, \quad \alpha \in \mathbb{F}_2. \quad (8.1.24)$$

## 8.2 Код Кердока

В этом разделе мы используем хорошо известные конструкции Дельсарта и Геталса кода Кердока, изложенные, например, в книге [7]. Вместе с тем наши методы доказательств основных результатов существенно отличаются от весьма непростых методов, которые были использованы Дельсартом и Геталсом.

**Определение 8.2.1** [Код Кердока] *Пусть  $m = 2t - 1$ ,  $t > 1$  — нечетное число и  $s(a\mathbf{x})$  — функция определенная равенством (8.1.13), где  $m = 2t - 1$ . Рассмотрим множество  $\mathfrak{K}(m)$  векторов, образованное всеми векторами длины  $n = 2^{m+1} = 2^{2t}$  и вида*

$$\Upsilon(a, b, \varepsilon, \gamma) = (\overline{Tr(s(a\mathbf{x}) + b\mathbf{x} + \varepsilon)} \mid \overline{Tr(s(a\mathbf{x}) + (a+b)\mathbf{x} + \gamma + \varepsilon)}), \quad \gamma, \varepsilon \in \mathbb{F}_2, a, b \in \mathbb{F}_{2^{2t-1}}, \quad (8.2.1)$$

*составленных из двух "половинок"  $\overline{Tr(s(a\mathbf{x}) + b\mathbf{x} + \varepsilon)}$  и  $\overline{Tr(s(a\mathbf{x}) + (a+b)\mathbf{x} + \gamma + \varepsilon)}$ , каждая длиной  $\frac{n}{2} = 2^m$ .*

*Множество векторов  $\mathfrak{K}(m)$  называется кодом Кердока.*

Заметим, что код Кердока  $\mathfrak{K}(m)$  не является линейным кодом: сумма  $\Upsilon(a, b, \varepsilon, \gamma) + \Upsilon(a', b', \varepsilon', \gamma')$  двух его векторов, вообще говоря, не принадлежит  $\mathfrak{K}(m)$ . Это следует из следующих соображений. Вектор  $\overline{Tr(s(a\mathbf{x})) + Tr(s(a'\mathbf{x})) + b\mathbf{x} + b'\mathbf{x}}$ , который является левой половиной суммы векторов  $\Upsilon(a, b, \varepsilon, \gamma)$  и  $\Upsilon(a', b', \varepsilon', \gamma')$ , может быть представлен как вектор  $\overline{Tr(s((a+a')\mathbf{x}) + b''\mathbf{x} + b\mathbf{x} + b'\mathbf{x})}$  с некоторым  $b'' \in \mathbb{F}_{2^m}$ , зависящим от  $a$  и  $a'$ . Вместе с тем правая половина суммы этих векторов не имеет требуемого вида  $\overline{Tr(s((a+a')\mathbf{x}) + (a+a')\mathbf{x} + (b'+b)\mathbf{x} + b''\mathbf{x})}$ .

**Теорема 8.2.1** *Пусть  $m$  — нечетное число.*

*Двоичный код Кердока  $\mathfrak{K}(m)$  длины  $n = 2^{m+1}$  имеет следующие параметры:*

i. Число элементов  $\mathfrak{K}(m)$  равно  $4 \cdot 2^{2m} = n^2$ .

ii. Кодовое расстояние  $d$  кода  $\mathfrak{K}(m)$  равно  $d = 2^m - 2^{\frac{1}{2}(m-1)} = \frac{1}{2}(n - \sqrt{n})$ .

iii. Пусть  $A(j)$  число пар векторов  $(\Upsilon, \Upsilon')$  кода Кердока  $\mathfrak{K}(m)$ , для которых  $d(\Upsilon, \Upsilon') = j$ . Тогда число  $A(j)$  принимает ненулевые значения только при  $j = 0, \frac{1}{2}(n \pm \sqrt{n}), n$ . Спектр взаимных расстояний представлен в следующей таблице.

Таблица 1.

Расстояние $d(\Upsilon, \Upsilon')$	0	$\frac{1}{2}(n - \sqrt{n})$	$\frac{n}{2}$	$\frac{1}{2}(n + \sqrt{n})$	$n$
Число пар векторов $(\Upsilon, \Upsilon')$ с взаимным кодовым расстоянием $d(\Upsilon, \Upsilon')$	$n^2$	$\frac{1}{2}n^3(n-2)$	$2n^3-2n^2$	$\frac{1}{2}n^3(n-2)$	$n^2$

iv. Код Кердока  $\mathfrak{K}(m)$  лежит на границе (2.0.34) Теоремы 2.0.8, т.е. он имеет максимально возможное число элементов среди всех антиподальных кодов с кодовым расстоянием  $d = \frac{1}{2}(n - \sqrt{n})$ .

**Доказательство.** Утверждение п. i. очевидно.

Переходим к доказательству утверждения п. ii. Для этого мы докажем, что скалярное произведение  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a', b', \varepsilon', \gamma'))$ ,  $(a, b, \varepsilon, \gamma) \neq (a', b', \varepsilon', \gamma')$ , двух векторов из  $\mathfrak{K}(m)$  принимает одно из трех значений: 0 и  $\pm 2^{\frac{m}{2}}$ .

а.) Пусть  $a \neq a'$  и  $a \neq 0, a' \neq 0$ . В виду того, что  $Tr(\frac{a}{a+a'}) + Tr(\frac{a'}{a+a'}) = Tr(1) = 1$ , без ограничения общности будем полагать, что  $Tr(\frac{a}{a+a'}) = 1$ . Покажем, что в этом случае одно из скалярных произведений

$$\begin{aligned} & (\overline{Tr(s(a\mathbf{x}) + b\mathbf{x} + \varepsilon)}, \overline{Tr(s(a'\mathbf{x}) + b'\mathbf{x} + \varepsilon')}) = (-1)^{\varepsilon+\varepsilon'} T(a, a', b + b') \\ & \text{и} \\ & (\overline{Tr(s(a\mathbf{x}) + (a+b)\mathbf{x} + \gamma + \varepsilon)}, \overline{Tr(s(a'\mathbf{x}) + (a'+b')\mathbf{x} + \gamma' + \varepsilon')}) = \\ & = (-1)^{\varepsilon+\varepsilon'+\gamma+\gamma'} T(a, a', b + b' + a + a') \end{aligned} \quad (8.2.2)$$

равно 0, в то время как модуль другого равен  $2^t = 2^{\frac{m+1}{2}}$ .

Действительно, как нетрудно увидеть, из утверждения леммы 8.1.4 (равенство (8.1.20)) с учетом соотношения

$$Tr\left(\frac{a(b+b')}{a^2+a'^2}\right) + Tr\left(\frac{a(a+a'+b+b')}{a^2+a'^2}\right) = Tr\left(\frac{a(a+a')}{a^2+a'^2}\right) = Tr\left(\frac{a}{a+a'}\right) = 1 \quad (8.2.3)$$

вытекает, что  $T(a, a', b + b') = 0$ ,  $T(a, a', b + b' + a + a') = \pm 2^t$ , либо  $T(a, a', b + b') = \pm 2^t$ ,  $T(a, a', b + b' + a + a') = 0$ . Отсюда следует, что

$$|T(a, a', b + b') \pm T(a, a', b + b' + a + a')| = 2^t. \quad (8.2.4)$$

Из последнего равенства, очевидно, вытекает вышеприведенное утверждение о скалярных произведениях (8.2.2). Таким образом, самый сложный случай п.ii. доказан.

б.) Пусть либо  $a \neq 0, a' = 0$ , либо  $a' \neq 0, a = 0$ . Покажем, что в этом случае одно из скалярных произведений



$$\begin{aligned}
& (\overline{Tr(s(a\mathbf{x}) + b\mathbf{x} + \varepsilon)}, \overline{Tr(b'\mathbf{x} + \varepsilon')}) = (-1)^{\varepsilon+\varepsilon'} T(a, b + b') \\
& \text{и} \\
& (\overline{Tr(s(a\mathbf{x}) + (a + b)\mathbf{x} + \gamma + \varepsilon)}, \overline{Tr(+b'\mathbf{x} + \gamma' + \varepsilon')}) = \\
& = (-1)^{\varepsilon+\varepsilon'+\gamma+\gamma'} T(a, b + b' + a)
\end{aligned} \tag{8.2.5}$$

равно 0, в то время как модуль другого равен  $2^t = 2^{\frac{m+1}{2}}$ .

Это утверждение также как в предыдущем случае вытекает из леммы 8.1.3 (равенство (8.1.20)).

с.) Пусть  $a = a'$ ,  $b + b' \neq 0$ . В этом случае скалярное произведение  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b', \varepsilon', \gamma'))$ , очевидно, равно нулю.

d.) Случай  $a = a'$ ,  $b = b'$ ,  $(\varepsilon, \gamma) \neq (\varepsilon', \gamma')$  тривиален:  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = 0$ , если  $\gamma + \gamma' \neq 0$ , и  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = -2^m$ , если  $\gamma + \gamma' = 0$ , а  $\varepsilon + \varepsilon' \neq 0$ .

Утверждение п.ii. полностью доказано.

Переходим к доказательству п.iii.

Очевидно, число пар  $(a, b, \varepsilon, \gamma)$  и  $(a', b', \varepsilon', \gamma')$ , для которых выполнены условия а.) или б.), равно  $4n^2 \left( \left( \frac{n}{2} \right)^2 - \frac{n}{2} \right) = n^4 - 2n^3$ . Для этих пар выполнено равенство

$$|(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma'))| = 2^{\frac{m+1}{2}}.$$

Так как код  $\mathfrak{K}_m$  вместе с вектором  $\Upsilon$  содержит ему противоположный, то число пар  $\Upsilon, \Upsilon' \in \mathfrak{K}_m$ , для которых  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = -2^{\frac{m}{2}}$  равно числу пар, для которых  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = 2^{\frac{m+1}{2}}$ .

Эти расчеты позволяют заполнить вторую и четвертую колонки Таблицы 1.

Число пар  $(a, b, \varepsilon, \gamma)$  и  $(a', b', \varepsilon', \gamma')$ , для которых выполнено условие с.), очевидно, равно  $8n \left( \left( \frac{n}{2} \right)^2 - \frac{n}{2} \right) = 2n^3 - 4n^2$ .

Число пар  $(a, b, \varepsilon, \gamma)$  и  $(a', b', \varepsilon', \gamma')$ , для которых выполнено условие d.) и  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = 0$ , очевидно, равно  $8 \left( \frac{n}{2} \right)^2 = 2n^2$ . Число пар, для которых выполнено условие d.) и  $(\Upsilon(a, b, \varepsilon, \gamma), \Upsilon(a, b, \varepsilon', \gamma')) = \pm n$  также равно  $2n^2$ .

Эти расчеты позволяют заполнить остальные колонки Таблицы 1.

Утверждение п.iv. проверяется непосредственно.  $\square$

**Замечание 8.2.1** Коды Кердока являются одним из наиболее интересных объектов теории кодирования. С их помощью могут быть построены многие другие комбинаторные конструкции.

Известно несколько различных способов построения кодов Кердока. Наиболее интересным из них является конструкция, использующая кольцо  $\mathbf{Z}_4$  вычетов по модулю 4. Коды над кольцом Галуа, частным случаем которого является кольцо  $\mathbf{Z}_4$ , впервые были рассмотрены А.А. Нечаевым. Его подход позволил построить ряд интересных классов кодов, среди которых есть и код Кердока.

В частности, А.А. Нечаев показал, что если выколоть из кода Кердока два разряда, то он может быть представлен в циклическом виде [29]. Затем этот результат был многократно повторен.

Заметим, что кольцо Галуа само по себе является весьма интересным объектом, свойства которого похожи на свойства конечного поля. Хорошее изложение свойств колец Галуа и кодов над ними, в частности, кода Кердока имеется в книге [4].

Покажем, что вектор  $\Upsilon \in K(m)$  является одним из векторов кода Риды-Маллера  $RM_{2,m+1}$ , где  $m+1 = 2t$  — четное число. Для этого достаточно показать, что вектор  $\Upsilon$  является вектором значений  $\overline{f(\mathbf{x})}$ ,  $\mathbf{x} \in \mathbb{F}_2^{2^{m+1}}$  некоторой булевой функции  $f(\mathbf{x})$ , представленной многочленом Жегалкина, степень которого не превосходит 2.

Как следует из теоремы 7.2.1, вектор  $Tr(s(a\mathbf{x}) + b\mathbf{x})$ , где  $\mathbf{x} = x_1\omega_1, \dots, x_m\omega_m$ , является вектором значений некоторой булевой функции  $f(x_1, \dots, x_m)$ . Непосредственно из определения 8.2.1 кода Кердока  $K(m)$  следует, что вектор  $\Upsilon$  представляет собой вектор значений функции  $g_\Upsilon(x_1, \dots, x_m, x_{m+1}) = f(x_1, \dots, x_m) + x_{m+1}l(x_1, \dots, x_m) + \varepsilon$ ,  $\varepsilon \in \mathbb{F}_2$ , где  $x_{m+1} = \gamma$  и  $l(x_1, \dots, x_m)$  — линейная функция, которая представляет линейную над  $\mathbb{F}_2$  функцию  $Tr(a\mathbf{x})$ ,  $\mathbf{x} = x_1\omega_1 + \dots + x_m\omega_m$ .

Отсюда и из леммы 8.1.3 вытекает, что ранг функции  $g_\Upsilon(x_1, \dots, x_m, x_{m+1})$  (при  $s(a\mathbf{x}) \neq 0$ ) равен  $m+1$ , т.е. ее с помощью аффинной замены  $\mathbf{x} = \mathbf{y}A + \alpha$  переменных  $\mathbf{x} = (x_1, \dots, x_m, x_{m+1})$  с невырожденной матрицей  $A$  можно представить как  $g((x_1, \dots, x_m, x_{m+1})A + \alpha) = \sum_{i=1}^t y_{2i-1}y_{2i} + \varepsilon$ .

Кроме того, из теоремы 8.2.1 следует, что ранг любой суммы  $g_\Upsilon(x_1, \dots, x_m, x_{m+1}) + g_{\Upsilon'}(x_1, \dots, x_m, x_{m+1})$  либо равен  $m+1$ , либо эта функция является аффинной. Доказательство этого нетривиальное свойства, по существу, и является содержанием доказательства теоремы 8.2.1.

## 8.3 Код Препарата

Пусть  $m$  — нечетное число,  $n = 2^m - 1$  и  $X \subset \mathbb{F}_{2^m}$  и  $Y \subset \mathbb{F}_{2^m}$  — два подмножества элементов поля  $\mathbb{F}_{2^m}$ . Пусть

$$\varphi_X(x) = \begin{cases} 1, & \text{если } x \in X, \\ 0, & \text{если } x \notin X \end{cases} \quad (8.3.1)$$

— характеристическая функция множества  $X$ .

Пусть  $\overline{\mathbb{F}_{2^m}} = (\alpha_1, \alpha_2, \dots, \alpha_{2^m})$  — последовательность, образованная всеми элементами поля  $\mathbb{F}_{2^m}$ , выписанными в каком-либо определенном порядке.

Символом  $(X, Y) = (\varphi_X, \varphi_Y)$  мы обозначаем двоичную последовательность длины  $2^{m+1}$ , которая является конкатенацией двоичных последовательностей

$$\varphi_X = (\varphi_X(\alpha_1), \varphi_X(\alpha_2), \dots, \varphi_X(\alpha_{2^m})) \text{ и } \varphi_Y = (\varphi_Y(\alpha_1), \varphi_Y(\alpha_2), \dots, \varphi_Y(\alpha_{2^m})). \quad (8.3.2)$$

Таким образом,  $(X, Y)$  — двичная последовательность, ненулевые координаты которой индексированы множествами  $X$  и  $Y$ .

### Определение 8.3.1 [77] (Определение кода Препарата $P_m$ )

Расширенный код Препарата  $P_m$  образован всеми двоичными последовательностями  $(X, Y) \subset \mathbb{F}_2^{2^{m+1}}$ , для которых выполнены следующие условия

- (i). Число элементов каждого из множеств  $X$  и  $Y$  — четно, т.е.  $\sum_{\alpha \in X} \varphi_X(\alpha) = \sum_{\alpha \in Y} \varphi_Y(\alpha) = 0$ .
- (ii).  $\sum_{x \in X} x = \sum_{y \in Y} y$ .

$$(iii). \sum_{x \in X} x^3 + (\sum_{x \in X} x)^3 = \sum_{y \in Y} y^3.$$

Заметим, что код  $P_m$  является нелинейным. Действительно, если  $(X, Y), (X', Y') \in P_m$ , то последовательность  $(X + X', X + Y')$  не обязательно принадлежит коду  $P_m$  в виду того, что для нее, вообще говоря, не выполнено условие (iii).. (Упражнение)

### Теорема 8.3.1

- (a) Кодовое расстояние кода Препарата  $P_m$  равно 6.
- (b) Число элементов кода Препарата  $P_m$  равно  $2^{2^m-2m}$ .

**Доказательство.** Пусть  $(X, Y), (X', Y') \in P_m$ . Если  $wt(\varphi_X + \varphi_{X'}) + wt(\varphi_Y + \varphi_{Y'}) > 4$ , то, очевидно,  $d((X, Y), (X', Y')) \geq 6$ , в виду того, что вес каждой последовательности  $(\varphi_X | \varphi_Y)$  и  $(\varphi_{X'} | \varphi_{Y'})$  является четным.

Таким образом, осталось показать, не существует пар  $(X, Y), (X', Y')$  различных векторов кода  $P_m$  таких, что  $wt(\varphi_X + \varphi_{X'}) + wt(\varphi_Y + \varphi_{Y'}) \leq 4$ .

Очевидно,  $\varphi_X + \varphi_{X'} = \varphi_{X \Delta X'}$ , где  $X \Delta X' = (X \cup X') \setminus (X' \cap X)$  — симметрическая разность множеств  $X$  и  $X'$ .

Не существует пар  $(X, Y), (X', Y') \in P_m$  таких, что  $wt(\varphi_X + \varphi_{X'}) = 2$ ,  $wt(\varphi_Y + \varphi_{Y'}) = 0$ . (Упражнение)

Покажем, что не существуют пар  $(X, Y), (X', Y') \in P_m$  таких, что  $wt(\varphi_X + \varphi_{X'}) + wt(\varphi_Y + \varphi_{Y'}) = 4$ .

Предположим, что  $wt(\varphi_Y + \varphi_{Y'}) = 0$ , т.е. предположим, что  $Y = Y'$ . В этом случае из пп. (i)-(iii) вытекает, что

$$\sum_{x \in X} \varphi_X(x) + \sum_{x' \in X'} \varphi_{X'}(x') = 0, \quad \sum_{x \in X} x + \sum_{x' \in X'} x' = 0, \quad \sum_{x \in X} x^3 + \sum_{x' \in X'} x'^3 = 0. \quad (8.3.3)$$

Из последних равенств вытекает, что

$$\sum_{z \in Z} \varphi_Z(z) = 0, \quad \sum_{z \in Z} z = 0, \quad \sum_{z \in Z} z^2 = 0, \quad \sum_{z \in Z} z^3 = 0, \quad \sum_{z \in Z} z^4 = 0, \quad (8.3.4)$$

где  $Z = X \Delta X'$ . Последнее соотношение выполняется только в случае  $|Z| > 4$ .

Следовательно, в рассматриваемом случае  $wt(\varphi_X + \varphi_{X'}) + wt(\varphi_Y + \varphi_{Y'}) > 4$ .

Пусть теперь  $wt(\varphi_Y + \varphi_{Y'}) = 2$ . Покажем, что в этом случае  $wt(\varphi_X + \varphi_{X'}) > 2$ .

Действительно, если  $wt(\varphi_X + \varphi_{X'}) = 2$ , то с одной стороны из соотношений пп. (ii), (iii) определения 8.3.1 следует, что

$$\sum_{z \in Z} z = \sum_{z' \in Z'} z', \quad \sum_{z \in Z} z^3 + (\sum_{x \in X} x)^3 + (\sum_{x \in X} x + \sum_{z \in Z} z)^3 = \sum_{z' \in Z'} z'^3, \quad (8.3.5)$$

где  $Z = X \Delta X'$ ,  $Z' = Y \Delta Y'$  и  $|Z| = |Z'| = 2$ .

Докажем, что система (8.3.5) с двумя уравнениями не имеет решения.

Сначала предположим, что  $\sum_{x \in X} x = 0$ , т.е. докажем, что система

$$\sum_{z \in Z} z = \sum_{z' \in Z'} z', \quad \sum_{z \in Z} z^3 + (\sum_{z \in Z} z)^3 = \sum_{z' \in Z'} z'^3, \quad |Z| = |Z'| = 2, \quad (8.3.6)$$

не имеет решения.

Как нетрудно проверить, из (8.3.6) вытекают равенства  $\sum_{z \in Z} z^3 + (\sum_{z \in Z} z)^3 = z_1 z_2^2 + z_1^2 z_2$  и  $\sum_{z' \in Z'} z'^3 = (z_1 + z_2)^3 + z'_1 z'_2 (z_1 + z_2)$ , где  $Z = \{z_1, z_2\}$ ,  $Z' = \{z'_1, z'_2\}$ . Следовательно,  $z_1 z_2 + z'_1 z'_2 + (z_1 + z_2)^2 = 0$ . Положим теперь  $z'_1 = z_1 + h$ ,  $z'_2 = z_2 + h$ . Заметить, что в виду первого равенства в (8.3.6) такой элемент  $h \in \mathbb{F}_{2^m}$  всегда существует.

В результате получим равенство  $h^2 + h(z_1 + z_2) + (z_1 + z_2)^2 = 0$ , из которого вытекает соотношение

$$1 + \frac{h}{z_1 + z_2} + \left( \frac{h}{z_1 + z_2} \right)^2 = 0. \quad (8.3.7)$$

Докажем, что последнее равенство не выполнено ни при каких  $h, z_1, z_2, z_1 + z_2 \neq 0$ .

Действительно, с одной стороны  $Tr(1 + \frac{h}{z_1 + z_2} + (\frac{h}{z_1 + z_2})^2) = Tr(1) = 1$ . С другой стороны, если равенство (8.3.7) выполнено, то  $Tr(1 + \frac{h}{z_1 + z_2} + (\frac{h}{z_1 + z_2})^2) = Tr(0) = 0$ . Полученное противоречие доказывает, что в коде Препарата  $P_m$  не существует пар векторов  $(\varphi_X, \varphi_Y), (\varphi_{X'}, \varphi_{Y'})$  таких, что  $wt(\varphi_X + \varphi_{X'}) = wt(\varphi_Y + \varphi_{Y'}) = 2$ , что завершает доказательство п.(а) теоремы в случае  $\sum_{x \in X} x = 0$ .

Сведем теперь случай  $S = \sum_{x \in X} x \neq 0$  к предыдущему.

Положим  $\hat{X} = X \cup \{S\}$ ,  $\hat{Y} = Y \cup \{S\}$ ,  $\hat{X}' = X' \cup \{S\}$  и  $\hat{Y}' = Y' \cup \{S\}$ . Очевидно,  $Z = \hat{X} \triangle \hat{X}'$ ,  $Z' = \hat{Y} \triangle \hat{Y}'$  и, следовательно,  $wt(\varphi_{\hat{Y}} + \varphi_{\hat{Y}'}) = 2$ , если  $wt(\varphi_Y + \varphi_{Y'}) = 2$ , и  $wt(\varphi_{\hat{X}} + \varphi_{\hat{X}'}) = 2$ , если  $wt(\varphi_X + \varphi_{X'}) = 2$ .

Очевидно, соотношение (8.3.6) для множеств  $\hat{X}, \hat{Y}, \hat{X}', \hat{Y}'$  выполнено тогда и только тогда, когда оно выполнено для множеств  $X, Y, X', Y'$ . Множество  $\hat{X}$  подобрано так, что  $\sum_{x \in \hat{X}} x = 0$ , что сводит рассматриваемых случай  $\sum_{x \in X} x \neq 0$  к предыдущему. Таким образом, доказательство п.(а) теоремы завершено. Заметим, что при этом условие (i) определения 8.3.1 было использовано только при доказательстве случая  $Y = Y'$ .

Подсчитаем теперь число векторов  $(\varphi_X, \varphi_Y)$  кода  $P_m$ .

Индексируем координаты вектора  $\mathbf{x} = (x_{\alpha_1}, \dots, x_{\alpha_{2^m}}) \in \mathbb{F}_2^{2^m}$  элементами  $\alpha_j$  поля  $\mathbb{F}_{2^m} = \{\alpha_1, \dots, \alpha_{2^m}\}$ . Обозначим через  $X(\mathbf{x}) = \{\alpha_j | x_{\alpha_j} = 1\}$  индексов тех координат вектора  $\mathbf{x}$ , которые равны 1.

Очевидно, соответствие  $\mathbf{x} \leftrightarrow X(\mathbf{x})$  является взаимно однозначным. Пусть вектор  $\mathbf{x} = \mathbf{x}(X)$  соответствует множеству  $X$  в этом соответствии. Как нетрудно увидеть, выражения  $\sum_{\alpha \in \mathbb{F}_{2^m}} \varphi_X(\alpha)$ ,  $\sum_{\alpha \in X} \alpha$ ,  $\sum_{\alpha \in X} \alpha^3$  в определении 8.3.1 можно представить в следующем виде

$$\sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha}, \sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha} \alpha, \sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha} \alpha^3, \quad (8.3.8)$$

соответственно.

Зафиксируем множество  $X$  в определении 8.3.1. Покажем, что множество  $Y$ , удовлетворяющее пп. (i)-(iii) этого определения, можно выбрать  $2^{2^m-2m-1}$  способами.

Действительно, размерность пространства решений невырожденной однородной системы линейных уравнений

$$\sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha} = 0, \sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha} \alpha = 0, \sum_{\alpha \in \mathbb{F}_{2^m}} x_{\alpha} \alpha^3 = 0 \quad (8.3.9)$$

равна  $2^m - 2m - 1$ . Поэтому число различных множеств  $Y$  при фиксированном  $X$  равно указанному числу. (Упражнение)

С другой стороны число различных множеств  $X$  с четным числом элементов, очевидно, равно  $2^{2^m-1}$ . Это доказывает пункт (b) утверждения теоремы.  $\square$

**Следствие 8.3.1** Код  $P'_m$  длины  $n = 2^{m+1} - 1$ , где  $m$  — нечетное число, образованный всеми векторами кода  $P_m$  с одной выколотой координатой (произвольно какой) является нелинейным двоичным кодом с кодовым расстоянием 5 и числом элементов  $2^{n-2m-2}$ .

**Доказательство.** Упражнение.

Следует сказать, что код  $P'_m$  обладает многими замечательными свойствами. В частности, что весьма существенно, он имеет число элементов в два раза большее, чем число элементов двоичного БЧХ-кода (см. 5.2.3) с тем же кодовым расстоянием и той же длиной.

Следует сказать, что распределение расстояний между парами векторов кода  $P_m$  не очень трудно вычислить непосредственно, исходя из его определения 8.3.1. Этого мы здесь делать не будем.

Заметим только, что распределение взаимных расстояний кода Препараты является в некотором смысле двойственным к распределению взаимных расстояний кода Кердока, хотя оба кода являются нелинейными и для них соотношение МакВильямс конечно неприменимо. Вместе с тем можно непосредственно проверить, что взаимные расстояния этих кодов удовлетворяют соотношению МакВильямс (9.0.5), в котором  $\mathfrak{K}$  — спектр взаимных расстояний кода Кердока и  $\mathfrak{K}^\perp$  — спектр взаимных расстояний кода Препараты. Это другое отличительное свойство кода  $P_m$ .

Причина этого довольно долго была не понята. Затем было установлено, что коды Кердока и Препараты можно рассматривать как проекции линейных кодов  $\mathfrak{K}$  и  $\mathfrak{K}^\perp$  над кольцом  $\mathbf{Z}_4 = \mathbf{Z}/4\mathbf{Z}$  вычетов по модулю 4 в кольцо  $\mathbf{Z}_2$  с помощью, так называемого, отображения Грея (см., например, [4]). Оказалось, что код  $\mathfrak{K}$  и  $\mathfrak{K}^\perp$  являются двойственными в кольце  $\mathbf{Z}_4$  один к другому. Для них нетрудно вывести соотношение МакВильямс вида (9.0.5), что и объясняет двойственность их спектров.

Таким образом, чтобы вычислить распределение взаимных расстояний в коде Препарата можно воспользоваться соотношением МакВильямс и известным из теоремы 8.2.1. (Упражнение)

Следует также сказать, что укороченный код Препарата длины  $2^{m+1} - 2$  путем перестановки его координат примерно также как это было сделано для кода Кердока А.А. Нечаевым [27] может быть превращен в циклический код.

Также как и код Кердока код Препарата широко используется для построения комбинаторных конструкций (см. [77]).

## 8.4 Циклический линейный код, порождаемый булевыми функциями ранга 2

**Теорема 8.4.1** Пусть  $m = 2t - 1$  — нечетное число.

Линейный антиподальный двоичный код  $\mathfrak{K}_m$  длины  $n = 2^m$ , образованный векторами вида

$$\Upsilon = \overline{Tr(\mathbf{x}^3 + b\mathbf{x} + \varepsilon)}, \quad a, b \in \mathbb{F}_{2^m}, \quad \varepsilon \in \mathbb{F}_2, \quad (8.4.1)$$

- i. Код  $\mathfrak{K}_m$  имеет размерность  $2m+1$  и кодовое расстояние равно  $d = 2^{m-1} - 2^{\frac{1}{2}(m+1)} = \frac{1}{2}(n - \sqrt{2n})$ .
- ii. Код  $\mathfrak{K}_m$  лежит на границе (2.0.34) Теоремы 2.0.8, т.е. он имеет максимально возможное число элементов среди всех антиподальных кодов с кодовым расстоянием  $d = \frac{1}{2}(n - \sqrt{2n})$ .
- iii. Число векторов кода  $\mathfrak{K}_m$  веса 0,  $\frac{1}{2}(n \pm \sqrt{2n})$  и  $\frac{n}{2}$  приведено в следующей таблице

Таблица 2.

Вес вектора $\Upsilon \in \mathfrak{K}_m$	0	$\frac{1}{2}(n - \sqrt{2n})$	$\frac{n}{2}$	$\frac{1}{2}(n + \sqrt{2n})$	$n$
Число векторов $\Upsilon$ с заданным весом	1	$\frac{1}{2}n(n-1)$	$n^2+n-2$	$\frac{1}{2}n(n-1)$	1

1 **Доказательство.** Утверждение теоремы о размерности кода  $\mathfrak{K}_m$  очевидно.

Для доказательства утверждения о кодовом расстоянии воспользуемся леммой 8.1.2 (соотношение (8.1.3)) и очевидным соотношением  $(\Upsilon, \Upsilon') = n - 2d(\Upsilon, \Upsilon')$ .

Справедливость утверждения п. ii. теоремы проверяется непосредственно.

Утверждение п. iii. теоремы вытекает из утверждений леммы 8.1.2.  $\square$

Мы индексировали координаты вектора  $\overline{Tr(\mathbf{x}^3 + b\mathbf{x} + \varepsilon)}$  с помощью элементов поля  $\mathbb{F}_{2^m}$ , записанных в некотором порядке:  $\mathbb{F}_{2^m} = \{\alpha_1, \alpha_1, \dots, \alpha_{2^m}\}$ ,  $\alpha_{2^m} = 0$ . Далее упорядочим ненулевые элементы поля  $\mathbb{F}_{2^m}$  с помощью его первообразного элемента  $\theta$ , а именно, положим  $\alpha_j = \theta^{j-1}$ ,  $j = 1, \dots, 2^m - 1$ , и будем рассматривать последовательности  $\overline{Tr(f(\mathbf{x}))}'$ ,  $f(\mathbf{x}) = \mathbf{x}^3 + b\mathbf{x} + \varepsilon$  с одной выколотой координатой, номер которой равен 0  $\in \mathbb{F}_{2^m}$ . Таким образом,

$$\overline{Tr(\mathbf{x}^3 + b\mathbf{x} + \varepsilon)}' = (Tr(f(\theta^0)), Tr(f(\theta^1)), \dots, Tr(f(\theta^{2^m-2}))). \quad (8.4.2)$$

Непосредственно из теоремы 8.4.1 вытекает

**Следствие 8.4.1** Код  $\mathfrak{K}'_m$  длины  $n = 2^m - 1$ ,  $m = 2t - 1 > 1$ , образованный всеми последовательностями вида (8.4.2), является двоичным циклическим кодом размерности  $2m + 1$  с кодовым расстоянием  $d = \frac{1}{2}(n - \sqrt{2n}) - 1$ .

## 8.5 Авто и взаимная корреляция последовательностей

Пусть  $\mathbf{x} = (x_0, x_1, \dots, x_{n-1})$ ,  $\mathbf{y} = (y_0, y_1, \dots, y_{n-1})$  — векторы с координатами из поля комплексных чисел  $\mathbb{C}$ , т.е.  $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$ .

### Определение 8.5.1 Функция

$$T_{\mathbf{x}, \mathbf{y}}(j) = \Re \{x_0 \bar{y}_j + x_1 \bar{y}_{j+1} + \cdots + x_{n-1} \bar{y}_{n-1+j}\}, \quad (8.5.1)$$

где индексы у  $y_{j+k}$  рассматриваются по  $\text{mod } n$ ,  $\Re\{x\}$  — действительная часть комплексного числа  $x$  и  $\bar{y}_k$  — число, комплексно-сопряженное с  $y_k$ , называется взаимно корреляционной функцией последовательностей  $\mathbf{x}$  и  $\mathbf{y}$ .

Если  $\mathbf{x} = \mathbf{y}$ , то функция  $T_{\mathbf{x}}(j) = T_{\mathbf{x}, \mathbf{x}}(j)$  называется автокорреляционной функцией последовательности  $\mathbf{x}$ . Очевидно,  $T_{\mathbf{x}}(0) = |x_0|^2 + \cdots + |x_{n-1}|^2 = |\mathbf{x}|^2$ .

**Замечание 8.5.1** Иногда вместо функции  $T_{\mathbf{x}, \mathbf{y}}(j)$  в качестве взаимно корреляционной функции рассматривают функцию

$$\tilde{T}_{\mathbf{x}, \mathbf{y}}(j) = |x_0 \bar{y}_j + x_1 \bar{y}_{j+1} + \cdots + x_{n-1} \bar{y}_{n-1+j}|. \quad (8.5.2)$$

Далее мы будем рассматривать в качестве взаимно корреляционной функции только функцию  $T_{\mathbf{x}, \mathbf{y}}(j)$ . Вместе с тем значительное число работ посвящено изучению именно функции  $\tilde{T}_{\mathbf{x}, \mathbf{y}}(j)$ .

**Пример 8.5.1** Рассмотрим последовательность

$$\mathbf{x} = (1, 1, \exp -\frac{2\pi i}{3}, \exp \frac{2\pi i}{3}, \exp \frac{2\pi i}{3}, \exp -\frac{2\pi i}{3}, 1) \quad (8.5.3)$$

длины 7, координатами которой являются корни 3-ей степени из 1. График функции  $T_{\mathbf{x}}(j)$  имеет следующий вид

Рис. 1

Отметим, что функция  $T_{\mathbf{x}}(j)$  имеет "высокий" пик при  $j \equiv 0 \text{ mod } 7$  и принимает "малые" отрицательные значения при  $j \not\equiv 0 \text{ mod } 7$ . Это свойство при их техническом использовании обеспечивает хорошую различимость последовательности  $\mathbf{x}$  от ее циклических сдвигов.

Часто предполагается, что  $|\mathbf{y}| = |\mathbf{x}| = n$ , т.е. полагается, что векторы  $\mathbf{x}, \mathbf{y}$  лежат на унитарной сфере  $U^{n-1}$  радиуса  $\sqrt{n}$ .

Как видно из (8.5.1) функция  $T_{\mathbf{x}, \mathbf{y}}(j)$  равна действительной части обычного скалярного произведения в унитарном пространстве  $\mathbb{C}^n$  векторов  $\mathbf{x}$  и  $\mathbf{y}^{(j)}$  (циклический сдвиг вектора  $\mathbf{y}$  на  $j$  разрядов).

Отсюда вытекает, что если  $|\mathbf{y}| = |\mathbf{x}| = n$ , то число  $T_{\mathbf{x}, \mathbf{y}}(j)$  может быть выражено через евклидово расстояние  $\lambda_{\mathbf{C}}(\mathbf{x}, \mathbf{y})$  (см. раздел 1.2.1) между векторами  $\mathbf{x}$  и  $\mathbf{y}^{(j)}$  следующим образом (см. (1.2.6)).

$$T_{\mathbf{x}, \mathbf{y}}(j) = n(1 - \frac{1}{2}\lambda_{\mathbf{C}}^2(\mathbf{x}, \mathbf{y}^{(j)})) \quad (8.5.4)$$

Обычно, но не всегда, в качестве координат  $\mathbf{x}$  и  $\mathbf{y}$  рассматриваются последовательности, у которых координатами являются корни  $m$ -ой степени из 1, т.е.  $x_j = \exp \frac{2\pi i a_j}{m}$ ,  $i = \sqrt{-1}$ , где  $a_i$ ,  $0 \leq a_i < m$ , — целое число.

Мы далее ограничимся рассмотрением только случая  $m = p$ , где  $p$  — простое число, в котором координатами  $\mathbf{x}$  и  $\mathbf{y}$  служат числа  $\exp \frac{2\pi i a_j}{p}$ . Последовательность  $\mathbf{x}$  в этом

случае определяется  $p$ -ичной последовательностью  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_p^n$ . В случае  $p = 2$ , в котором  $x_j = (-1)^{a_j}$ , последовательность  $\mathbf{x}$  также как и последовательность  $\mathbf{a}$  мы будем называть двоичной.

Пусть  $\mathbf{a} = (a_0, \dots, a_{n-1}) \in \mathbb{F}_p^n$  — вектор в пространстве  $\mathbb{F}_p^n$ . Функция  $f: \mathbf{a} \rightarrow \hat{\mathbf{a}} = \frac{1}{\sqrt{n}}(\exp \frac{2\pi i a_0}{p}, \dots, \exp \frac{2\pi i a_{n-1}}{p})$  переводит элементы пространства  $\mathbb{F}_p^n$  в точки единичной унитарной сферы  $U^{n-1}$ .

Пространство  $\mathbb{F}_p^n$  снабжено метрикой Хемминга  $d$ , а пространство  $U^{n-1}$ , в которое погружается пространство  $\mathbb{F}_p^n$  с помощью отображения  $f$ , — евклидовой метрикой  $\lambda_{\mathcal{C}}(\mathbf{x}, \mathbf{y})$ . Как видно из определения этих метрик при  $p \gg 2$  они слабо связаны между собой. Например, векторы  $\mathbf{a}_0 = (0, \dots, 0)$  и  $\mathbf{a}_1 = (1, \dots, 1)$  в метрике Хемминга  $d$  максимально далеко расположены один от другого, а в метрике  $\lambda_{\mathcal{C}}$  образы этих векторов  $\hat{\mathbf{a}}_0$  и  $\hat{\mathbf{a}}_1$  лежат достаточно близко один к другому. Вместе с тем при  $p = 2$  метрики  $d$  и  $\lambda_{\mathcal{C}}(\mathbf{x}, \mathbf{y})$  эквивалентны, т.е. существует монотонная функция  $\rho(x)$  такая, что  $\rho(\lambda_{\mathcal{C}}(\hat{\mathbf{a}}, \hat{\mathbf{b}})) = d(\mathbf{a}, \mathbf{b})$ . (Упражнение: выписать в явном виде функцию  $\rho(x)$ )

Пусть  $W = \{\mathbf{a}_1, \dots, \mathbf{a}_M\} \subset \mathbb{F}_p^n$  код (произвольное подмножество) в пространстве  $\mathbb{F}_p^n$ , в который входят только векторы обладающие свойством  $\mathbf{a}_s^{(j)} \neq \mathbf{a}_s$ ,  $j = 1, \dots, n-1$ , (ациклические векторы), и  $\widehat{W} = \{\hat{\mathbf{a}}_1, \dots, \hat{\mathbf{a}}_M\} \subset U^{n-1}$  — образ  $W$  при отображении  $f$ . Положим

$$\tau(\widehat{W}) = \max_{\substack{\mathbf{x}, \mathbf{y} \in \widehat{W}, 0 \leq t < n \\ \text{и } t > 0, \text{ если } \mathbf{x} = \mathbf{y}}} T_{\mathbf{x}, \mathbf{y}}(j). \quad (8.5.5)$$

Величина  $\tau(\widehat{W})$  называется *взаимной корреляцией кода*  $\widehat{W}$ .

Пусть  $W^{(c)}$  — код, образованный всеми циклическими сдвигами векторов кода  $W$ . Как нетрудно увидеть, величина  $\tau(\widehat{W})$  совпадает с величиной

$$\eta(\widehat{W}^{(c)}) = \max_{\mathbf{x}, \mathbf{y} \in \widehat{W}^{(c)}, \mathbf{x} \neq \mathbf{y}} \Re(\hat{\mathbf{x}}, \hat{\mathbf{y}}). \quad (8.5.6)$$

Отметим, что из соотношения (8.5.6) следует, что  $\eta(\widehat{W}^{(c)}) = 1 - \frac{1}{2}\lambda_{\mathcal{C}}^2(\widehat{W}^{(c)})$ , где  $\lambda_{\mathcal{C}}(\widehat{W}^{(c)})$  — кодовое расстояние в метрике  $\lambda_{\mathcal{C}}$  кода  $\widehat{W}^{(c)}$ , т.е. взаимная корреляция кода  $\widehat{W}$  полностью определяется кодовым расстоянием в метрике  $\lambda_{\mathcal{C}}$  кода  $\widehat{W}^{(c)}$ . Очевидно, чем больше кодовое расстояние  $\lambda_{\mathcal{C}}(\widehat{W}^{(c)})$ , тем меньше взаимная корреляция  $\tau(\widehat{W})$ .

Множества  $\widehat{W}$ , для которых величина  $\tau(\widehat{W})$  принимает значение близкое к минимально возможному находят применение в радиотехнике. Они используются для повышения разрешающей способности радиолокационных измерений, для разделения радиосигналов по форме и времени в широкополосных многоканальных системах связи, телеметрии и адресных системах.

Это замечание показывает, что изучение циклических кодов в метрике  $\lambda_{\mathcal{C}}$  имеет в технике связи существенные практическое значение.

**Пример 8.5.2** Пусть  $\xi$  — порождающий элемент мультипликативной группы поля  $\mathbb{F}_p$  ( $p$  — простое число) и  $\mathbf{a} = (\xi^0, \xi^1, \dots, \xi^{p-2}) \in \mathbb{F}_p^{p-1}$ . Последовательность  $\hat{\mathbf{a}} =$



$\frac{1}{\sqrt{p-1}}(\exp \frac{2\pi i a_0}{p}, \exp \frac{2\pi i a_1}{p}, \dots, \exp \frac{2\pi i a_{p-2}}{p})$ , где  $a_j = \xi^j$ , имеет следующую автокорреляционную функцию:

$$T_{\mathbf{x}}(j) = \begin{cases} 1, & \text{если } j \equiv 0 \pmod{n}, \\ -\frac{1}{p-1}, & \text{если } j \not\equiv 0 \pmod{n}. \end{cases} \quad (8.5.7)$$

Доказательство справедливости соотношения (8.5.7) предоставляется читателю (Упражнение).

Далее в этом разделе мы приведем примеры последовательностей  $\mathbf{x} \in \{1, -1\}^{n_j}$  с беспредельно возрастающими длинами  $n_j$ ,  $j = 1, 2, \dots$ , для которых  $T_{\mathbf{x}}(j) = -1$  при  $j \not\equiv 0 \pmod{n}$ . Для этих последовательностей  $\tau(\{\mathbf{x}\}) = \max_{1 \leq k \leq n_j}(\mathbf{x}, \mathbf{x}^{(k)}) = -1$ , что является минимально возможным значением этой величины. (Упражнение)

### Последовательности, получаемые с помощью символов Лежандра

Пусть  $\mathbb{F}_q$  — конечное поле с  $q = p^l$  элементами и  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$  — его мультипликативная группа. Как хорошо известно, группа  $\mathbb{F}_q^*$  является циклической, т.е. в ней содержится элемент  $\xi$  (не один), который ее порождает. Этот элемент называется примитивным или порождающим элементом мультипликативной группы поля. Таким образом,  $\mathbb{F}_q^* = \{\xi^j | j = 0, \dots, p-2\}$ .

Пусть  $m|p-1$ . Мы обозначаем через  $\psi(x)$  гомоморфизм группы  $\mathbb{F}_q^*$  в группу корней  $m$ -ой степени из 1. Этот гомоморфизм называется  $m$ -значным мультипликативным характером группы

$\mathbb{F}_q^*$ . Другими словами,  $\psi(x)$  — функция со значениями в подгруппе порядка  $m$  группы  $\Phi = \{\exp \frac{2\pi i a}{p-1} | a = 0, \dots, p-2\}$ , которая обладает следующим основным свойством

$$\psi(x \cdot y) = \psi(x) \cdot \psi(y) \quad \text{для всех } x, y \in \mathbb{F}_q^*. \quad (8.5.8)$$

Множество всех гомоморфизмов  $\psi(x)$ , очевидно, образует группу, групповой операцией в которой является поточечное умножение гомоморфизмов. Стандартное обозначение для этой группы:

$$\text{Hom}(\mathbb{F}_q^*, \mathbb{C}^*).$$

Элементарные свойства характеров изложены почти во всех книгах по теории чисел или в начальных курсах алгебры (см., например, [11]). Автор предлагает для первоначального изучения книгу [1], (Виноградов) и особенно рекомендует решить хотя бы некоторые задачи, приведенные в ней.

На элементе  $x = 0$  функция  $\psi(x)$  не определена, т.к. 0 не принадлежит мультипликативной группе поля  $\mathbb{F}_q$ . Обычно полагают, что  $\psi(0) = 0$ . Вместе с тем далее мы будем определять значение функции  $\psi(x)$  в нуле каждый раз особо указываемым образом.

Как нетрудно установить, функция  $\psi(x)$ ,  $x \in \mathbb{F}_q^*$ , имеет следующий явный вид

$$\psi(x) = \exp \frac{2\pi i t \text{ind } x}{m}, \quad (t, m) = 1, \quad (8.5.9)$$

где функция  $\text{ind}_\xi x = \text{ind } x$  принимает значение  $y$ ,  $0 \leq y \leq p-2$ , если  $x = \xi^y$ . Функцию  $\text{ind}_\xi x$  обычно называют индексом или дискретным логарифмом по основанию  $\xi$  элемента (вычета)  $x$ .

Если  $q$  — нечетное число и  $m = 2$ , то в этом случае характер  $\psi(x)$  принимает только действительные значения  $\pm 1$ . Его принято называть символом Лежандра и обозначать через  $\left(\frac{x}{p}\right)$ .

Заметим, что с некоторой условностью в обозначениях можно показать, что

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}. \quad (8.5.10)$$

Условность заключается в том, что в левой части равенства (8.5.10) стоит действительное число (1 или  $-1$ ), в то время как в его правой части стоит элемент поля  $\mathbb{F}_q$  также равный 1 или  $-1$ . Этой условностью мы будем пренебрегать, ибо всегда из контекста будет ясно с какими элементами в данном месте мы имеем дело — действительными числами или элементами поля  $\mathbb{F}_q$ . Помимо (8.5.10) имеется также много других способов вычисления символа Лежандра (см., например, [1]).

Мы несколько расширим область определения функции  $\left(\frac{x}{p}\right)$  символ Лежандра. А именно, положим  $\left(\frac{0}{p}\right) = 1$ . Так определенную функцию будем обозначать через  $\left(\frac{x}{p}\right)_b$ .

Рассмотрим двоичную последовательность  $\mathbf{x} \in \{1, -1\}^p$

$$\mathbf{x} = \left( \left(\frac{0}{p}\right)_b, \left(\frac{1}{p}\right)_b, \left(\frac{2}{p}\right)_b, \dots, \left(\frac{p-1}{p}\right)_b \right). \quad (8.5.11)$$

Очевидно, сдвиг  $\mathbf{x}^{(j)}$  последовательности  $\mathbf{x}$  на  $j$  разрядов вправо имеет вид

$$\mathbf{x}^{(j)} = \left( \left(\frac{j}{p}\right)_b, \left(\frac{j+1}{p}\right)_b, \left(\frac{j+2}{p}\right)_b, \dots, \left(\frac{j+p-1}{p}\right)_b \right). \quad (8.5.12)$$

**Лемма 8.5.1** *Имеет место равенство*

$$S = \sum_{x \in \mathbb{F}_q} \left( \frac{x(x+a)}{p} \right) = -1, \text{ если } a \neq 0. \quad (8.5.13)$$

Напомним, что в левой части (8.5.13) мы полагаем, что  $\left(\frac{y}{p}\right) = 0$ , если  $y = 0$ .

**Доказательство леммы.** Очевидно, (в частности, это следует из соотношения (8.5.10)) что  $\left(\frac{x}{p}\right) = \left(\frac{x^{-1}}{p}\right)$ ,  $x \in \mathbb{F}_p^*$ . Поэтому

$$S = \sum_{x \in \mathbb{F}_q} \left( \frac{x^{-1}(x+a)}{p} \right) = \sum_{x \in \mathbb{F}_q} \left( \frac{(1 + \frac{a}{x})}{p} \right) = \sum_{y \in \mathbb{F}_q, y \neq 0} \left( \frac{1+y}{p} \right) = -1. \quad (8.5.14)$$

□

**Теорема 8.5.1** *Если  $p = 4t - 1$ , то для последовательности  $\mathbf{x}$ , определенной соотношением (8.5.11), выполнено*

$$T_{\mathbf{x}}(j) = \begin{cases} p, & \text{если } j \equiv 0 \pmod{p}, \\ -1, & \text{если } j \not\equiv 0 \pmod{p}. \end{cases} \quad (8.5.15)$$

**Доказательство.** Как следует из определения последовательности  $\mathbf{x}$

$$T_{\mathbf{x}}(j) = (\mathbf{x}, \mathbf{x}^{(j)}) = \sum_{x \in \mathbb{F}_q} \left( \frac{x(x+j)}{p} \right) + \left( \frac{j}{p} \right) + \left( \frac{-j}{p} \right). \quad (8.5.16)$$

Так как  $\left( \frac{-1}{p} \right) = -1$ , если  $p = 4t - 1$ , то  $\left( \frac{j}{p} \right) + \left( \frac{-j}{p} \right) = 0$ . Отсюда и из соотношения (8.5.16) и леммы 8.5.1 следует утверждение теоремы.  $\square$

Заметим, что если  $p = 4t + 1$ , то  $\left( \frac{j}{p} \right) = \left( \frac{-j}{p} \right)$ , и, как следует из (8.5.16), выполнено соотношение

$$T_{\mathbf{x}}(j) = \begin{cases} p, & \text{если } j \equiv 0 \pmod{p}, \\ 2 \left( \frac{j}{p} \right) - 1, & \text{если } j \not\equiv 0 \pmod{p}. \end{cases} \quad (8.5.17)$$

При  $p = 4t - 1$ , как следует из теоремы 8.6.4, двоичный код, порожденный всеми циклическими сдвигами последовательности  $\mathbf{x}$  к которым добавлена последовательность  $(-1, -1, \dots, -1)$ , имеет кодовое расстояние Хемминга равно  $\frac{p+1}{2}$  (проверить) и число элементов  $p + 1$ . Число элементов этого кода лежит на границе Плоткина (2.0.11), т.е. он является кодом с максимальным числом элементов.

## Рекуррентные последовательности максимального периода

Если в предыдущем разделе для построения последовательности  $\mathbf{x}$  использовались свойства аддитивной группы поля  $\mathbb{F}_p$ , в то время как в настоящем разделе для построения последовательностей  $\mathbf{x}$  с "хорошими" корреляционными свойствами мы будем использовать свойства мультипликативной группы поля  $\mathbb{F}_q$ ,  $q = p^l$ , которая является циклической и имеет порядок  $q - 1$ .

Пусть  $Tr(x) : \mathbb{F}_q \rightarrow \mathbb{F}_p$ , — линейная над  $\mathbb{F}_p$  функция "след", определенная соотношением (6.1.4), в котором положено  $r = p$ . Мы рассматриваем последовательность

$$\mathbf{a} = (Tr(a\theta^0), Tr(a\theta^1), Tr(a\theta^2), \dots, Tr(a\theta^{q-2})), \quad a \in \mathbb{F}_q \setminus \{0\}, \quad (8.5.18)$$

порожденную первообразным элементом  $\theta$  мультипликативной группы поля  $\mathbb{F}_q$  и коэффициентом  $a$ .

Если элемент  $a$  заставить пробегать все элементы поля  $\mathbb{F}_q$ , то множество получаемых при этом последовательностей вида (8.5.18), как нетрудно увидеть, является  $p$ -значным линейным над  $\mathbb{F}_p$  кодом  $\mathfrak{K}_\theta$ , размерность которого равна  $l$ . Более того, код  $\mathfrak{K}_\theta$  является циклическим в виду того, что циклический сдвиг  $\mathbf{a}^{(j)} = (Tr(a\theta^j), Tr(a\theta^{j+1}), \dots, Tr(a\theta^{j+q-2})) = (Tr(a'\theta^0), Tr(a'\theta^1), Tr(a'\theta^2), \dots, Tr(a'\theta^{q-2}))$  вектора  $\mathbf{a}$  на  $j$  разрядов порождается коэффициентом  $a' = \theta^j a$ .

Как следует из теоремы 5.1.2 и леммы 5.1.3 последовательность  $\mathbf{a}$  является рекуррентной последовательностью с аннулирующим (проверочным) многочленом  $g(x) = x^l f(x^{-1}) = x^l + g_{l-1}x^{l-1} + \dots + g_1x + g_0$ , где  $f(x)$  — минимальный многочлен элемента  $\theta$ .

Таким образом, последовательность  $\mathbf{a} = (a_0, a_1, \dots, a_{q-1})$ , определенная соотношением (8.5.18), может быть представлена в виде

$$a_{j+l} = -(a_{j+l-1}g_1 + \dots + a_{j-1}g_{l-1} + a_jg_l), \quad j = 0, \dots, q-2, \quad (8.5.19)$$

т.е. она является линейной рекуррентной последовательностью.

Последнее свойство позволяет порождать знаки последовательности  $\mathbf{a}$  с помощью, так называемого, регистра сдвига, состоящего из  $l$  ячеек памяти с линейной обратной связью. Происходит это следующим образом.

Пусть  $\bar{a}^{(t)} = (a_{t+l-1}, a_{t+l-2}, \dots, a_t)$  — заполнение регистра в момент времени  $t$ . В момент времени  $t+1$  заполнение регистра будет следующим:  $\bar{a}^{(t+1)} = (a_{t+l}, a_{t+l-2}, \dots, a_{t+1})$ , где  $a_{t+l} = -(a_{t+l-1}g_1 + \dots + a_{t-1}g_{l-1} + a_t g_l)$ ,  $t = 0, \dots, q-2$ , т.е. следующее состояние регистра образуется с помощью сдвига его содержимого на один разряд вправо и заполнением освободившейся ячейки памяти значением линейной функции  $L(\mathbf{x}) = -(x_{l-1}g_1 + \dots + x_1g_{l-1} + x_0g_l)$  в точке  $\bar{a}^{(t)}$ .

Рис.

Мы будем рассматривать последовательность

$$\hat{\mathbf{a}} = \left( \exp \frac{2\pi i \operatorname{Tr}(a\theta^0)}{p}, \exp \frac{2\pi i \operatorname{Tr}(a\theta^1)}{p}, \dots, \exp \frac{2\pi i \operatorname{Tr}(a\theta^{q-2})}{p} \right) \quad (8.5.20)$$

и изучать ее автокорреляционную функцию  $T_{\hat{\mathbf{a}}}(j)$ .

**Теорема 8.5.2** Автокорреляционная функция  $T_{\hat{\mathbf{a}}}(j)$  последовательности  $\hat{\mathbf{a}}$  имеет вид

$$T_{\hat{\mathbf{a}}}(j) = \begin{cases} q-1, & \text{если } j \equiv 0 \pmod{q-1}, \\ -1, & \text{если } j \not\equiv 0 \pmod{q-1}. \end{cases} \quad (8.5.21)$$

**Доказательство.** Очевидно,

$$T_{\hat{\mathbf{a}}}(j) = \sum_{s=0}^{q-2} \exp \frac{2\pi i (\operatorname{Tr}(a\theta^s) - \operatorname{Tr}(a\theta^{s+j}))}{p} = \sum_{s=0}^{q-2} \exp \frac{2\pi i \operatorname{Tr}(a'\theta^s)}{p}, \quad (8.5.22)$$

где  $a' = a(1 - \theta^j) \neq 0$ , если  $j \not\equiv 0 \pmod{q-1}$ . Таким образом, для доказательства теоремы достаточно показать, что последняя сумма в (8.5.22) равна  $-1$ , если  $a' \neq 0$ .

Для любого  $\alpha \in \mathbb{F}_p$  и  $a' \neq 0$  число решений уравнения

$$\operatorname{Tr}(a'x) = 0, \quad (8.5.23)$$

принадлежащих полю  $\mathbb{F}_q$ , очевидно, равно  $\frac{q}{p}$ . Действительно, при  $a' \neq 0$   $\operatorname{Tr}(a'x)$  — ненулевая линейная функция над  $\mathbb{F}_p$ . Поэтому множество  $L$  решений уравнения (8.5.23) является подпространством, размерность которого над  $\mathbb{F}_p$ , очевидно, равна  $l-1$ . Следовательно,  $|L| = \frac{q}{p} = p^{l-1}$ .

Так как функция  $\operatorname{Tr}(a'x)$  принимает значения из поля  $\mathbb{F}_p$ , то она принимает и ненулевые значения. Каждое ненулевое значение функция  $\operatorname{Tr}(a'x)$  принимает одинаковое число раз, ибо  $\operatorname{Tr}(a'\alpha x) = \alpha \operatorname{Tr}(a'x)$ ,  $\alpha \in \mathbb{F}_p$ . Отсюда непосредственно вытекает, что уравнение  $\operatorname{Tr}(a'x) = \alpha$  для любого  $\alpha \in \mathbb{F}_p$  имеет  $p^{l-1}$  решений.

Значения функции  $\theta^s$ ,  $s = 0, \dots, q-2$ , пробегает все ненулевые значения из поля  $\mathbb{F}_q$ . Следовательно, из вышесказанного вытекает, что функция  $\operatorname{Tr}(a'\theta^s)$ ,  $s = 0, \dots, q-2$ , принимает  $p^{l-1}$  раз значение  $\alpha$ , если  $\alpha \neq 0$ , и принимает  $p^{l-1} - 1$  раз значение  $0$ .

Отсюда и из очевидного равенства

$$\sum_{\alpha=0}^{p-1} \exp \frac{2\pi i \alpha}{p} = 0 \quad (8.5.24)$$

следует второе соотношение в (8.5.21). Справедливость первого соотношения в (8.5.21) очевидна.  $\square$

Из теоремы 8.4.1 и того неоднократно упоминаемого факта, что  $d(\mathbf{x}, \mathbf{y}) = \frac{1}{2}(n - (\hat{\mathbf{x}}, \hat{\mathbf{y}}))$ , непосредственно следует

**Теорема 8.5.3** Пусть  $m = 2t - 1$  — нечетное число,  $\theta$  — первообразный элемент мультипликативной группы поля  $\mathbb{F}_q$ ,  $q = 2^m$ .

Рассмотрим линейный двоичный циклический код  $R_m^{(c)}$  длины  $n = 2^m - 1$  и размерности  $2t$ , образованный векторами вида

$$\Theta(a, b) = (Tr(a\theta^3 + b\theta), Tr(a\theta^{3 \cdot 2} + b\theta^2), \dots, Tr(a\theta^{3 \cdot (2^m-1)} + b\theta^{2^m-1})), \quad a, b \in \mathbb{F}_{2^m}, \quad \varepsilon \in \mathbb{F}_2, \quad (8.5.25)$$

и код  $R_m$ ,  $|R_m| = 2^m + 1 = \frac{1}{2^m-1}(|R_m^{(c)}| - 1)$ , образованный представителями циклов ненулевых элементов кода  $R_m$ .

Тогда

$$\tau(R_m) = \eta(R_m^{(c)}) = 2^{\frac{m+1}{2}} - 1. \quad (8.5.26)$$

## 8.6 Коды с кодовым расстоянием 5 или 6

Сначала естественно рассмотреть свойства некоторых  $p$ -значных БЧХ-коды с кодовым расстоянием 2 длин  $p^l - 1$ ,  $p^l$  и  $p^l + 1$ .

**Определение 8.6.1** [Квазисовершенный код] Код  $\mathfrak{K} \subset \mathbb{F}_q^n$  называется квазисовершенным, если для некоторого  $t$  шары радиуса  $t$  с центрами в кодовых точках не пересекаются, а шары радиуса  $t + 1$  содержат все векторы пространства  $\mathbb{F}_q^n$ .

Несколько иначе тоже самое можно сказать и следующим образом.

Положим

$$d(\mathbf{a}, \mathfrak{K}) = \min_{\mathbf{x} \in \mathfrak{K}} d(\mathbf{a}, \mathbf{x}). \quad (8.6.1)$$

Число  $d(\mathbf{a}, \mathfrak{K})$  называется расстоянием между вектором  $\mathbf{a}$  и кодом  $\mathfrak{K}$ .

Код  $\mathfrak{K} \subset \mathbb{F}_q^n$  называется квазисовершенным, если

$d(\mathfrak{K}) \geq 2t + 1$ , и любой вектор  $\mathbf{x} \in \mathbb{F}_q^n$  находится на расстоянии не более чем  $t + 1$  от кода  $\mathfrak{K}$ .

**Теорема 8.6.1** Линейный над полем  $\mathbb{F}_q$  код  $\mathfrak{K}$  с кодовым расстоянием  $d \geq 2t + 1$  и размерностью  $k$  является квазисовершенным тогда и только тогда, когда его проверочная  $n \times k$ -матрица (матрица с  $n$  столбцами и  $k$  строками)  $B$  обладает следующим свойством.

Любой вектор-столбец  $\mathbf{a}^T$  "высоты"  $k$  с координатами из поля  $\mathbb{F}_q$  может быть представлен как сумма с коэффициентами из  $\mathbb{F}_q^n$  не более чем из  $t + 1$  столбцов проверочной матрицы  $B$ .

**Доказательство.** Так как размерность пространства, натянутого на столбцы матрицы равна  $k$  (код имеет размерность  $k$ ), то для любого  $\mathbf{a} \in \mathbb{F}_q^k$  найдется вектор  $\mathbf{x} \in \mathbb{F}_q^k$  такой, что  $\mathbf{a}^T = B\mathbf{x}^T$ . Если код  $\mathfrak{K}$  — квазисовершенный, то для  $\mathbf{x} \in \mathbb{F}_q^k$  найдется вектор  $\mathbf{y}$  веса не более, чем  $t + 1$  такой, что  $\mathbf{x} + \mathbf{y} \in \mathfrak{K}$ .

Отсюда следует, что  $\mathbf{a}^T = B\mathbf{x}^T = -B\mathbf{y}^T$ , т.е.  $\mathbf{a}^T$  — сумма не более, чем  $t+1$  столбцов матрицы  $B$ .

Если некоторый вектор  $\mathbf{a}^T$  нельзя представить в виде суммы не более, чем  $t+1$  столбцов матрицы  $B$ , то, как нетрудно установить, вектор  $\mathbf{x}$ , определяемый равенством  $\mathbf{a}^T = B\mathbf{x}^T$ , находится от кода  $\mathcal{K}$  на расстоянии более  $t+1$ , т.е. код  $\mathcal{K}$  не является квазисовершенным.  $\square$

### 8.6.1 БЧХ-коды

Мы сначала рассматриваем  $p$ -значные БЧХ-коды длины  $q$ , определяемые проверочной матрицей вида (5.0.1), у которых параметр  $d$  принимает значение 5, т.е. БЧХ-коды с гарантированным кодовым расстоянием 5.

В рассматриваемом случае, как следует из теоремы 8.6.1, дело сводится к доказательству разрешимости при всех  $\alpha_j$ ,  $j = 0, 1, 2, 3$  (в этом случае код квазисовершенный) или неразрешимости при некоторых  $\alpha_j$ ,  $j = 0, 1, 2, 3$  (в этом случае код не является квазисовершенным) следующей системы уравнений

$$z_1x_1^j + z_2x_2^j + z_3x_3^j = \alpha_j, \quad j = 0, 1, 2, 3, \quad z_1, z_2, z_3, \alpha_0 \in \mathbb{F}_p, \quad x_1, x_2, x_3 \in \mathbb{F}_q, \quad (8.6.2)$$

где  $\alpha_j$ ,  $j = 1, 2, 3$ , — фиксированные элементы поля  $\mathbb{F}_q$ .

Пусть  $p > 3$ . Укажем значения элементов  $\alpha_j$ , для которых система (8.6.2) не имеет решений, а именно положим  $\alpha_j = z_0x_0^j$ ,  $z_0 \in \mathbb{F}_p \setminus \{0\}$ ,  $j = 0, 1, 2$ , и  $\alpha_3 = z'_0x_0^3$ , где  $x_0$  — фиксированный ненулевой элемент поля  $\mathbb{F}_q$  и  $z'_0 \neq z_0$ ,  $z'_0 \neq 0$ .

Заметим, что если  $x_0 \notin \{x_1, x_2, x_3\}$  и  $|\{x_1, x_2, x_3\}| = 3$ , то система относительно неизвестных  $z_1, z_2, z_3$  однородных линейных уравнений (8.6.2) при фиксированных  $z_j$  и  $z'_3$  не имеет ненулевых решений, ибо в этом случае матрица  $\|x_i^j\|_{i,j=0,\dots,3}$  ее коэффициентов невырождена (ее определитель является определителем Вандермонда).

Если же, например,  $x_0 = x_1$  и  $|\{x_1, x_2, x_3\}| = 3$ , то система, состоящая из первых трех уравнений в (8.6.2) относительно неизвестных  $z_1 - z_0, z_2, z_3$ , имеет только нулевое решение  $z_1 - z_0 = 0, z_2 = 0, z_3 = 0$  в  $\mathbb{F}_p$ , ибо матрица  $\|x_i^j\|_{i,j=0,1,2}$  ее коэффициентов невырождена. Это нулевое решение не является решением полной системы (8.6.2).

Если  $|\{x_1, x_2, x_3\}| < 3$ , то, очевидно, уравнение (8.6.2) не имеет решений при указанных значениях  $\alpha_j$ .

Таким образом, система (8.6.2) не имеет решений при указанных значениях  $\alpha_j$ , т.е. рассматриваемый БЧХ-код, исправляющий две ошибки, не является квазисовершенным при  $p > 3$ .

### 8.6.2 Троичный БЧХ-код, исправляющий две ошибки

**Теорема 8.6.2** *Троичный БЧХ-код  $BCH_{3,q}(n, 5)$  (см. теорему 5.2.1) длины  $n = 3^l - 1$ , исправляющий две ошибки, является квазисовершенным.*

**Доказательство.** Проверочная матрица  $B$  кода  $BCH_{3,q}(n, 5)$  имеет вид

$$B = \begin{pmatrix} \theta_1^0 & \theta_2^0 & \cdots & \theta_n^0 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \theta_1^2 & \theta_2^2 & \cdots & \theta_n^2 \end{pmatrix}, \quad (8.6.3)$$

где  $\{\theta_1, \theta_2, \dots, \theta_n\} = \mathbb{F}_q \setminus \{0\}$ . Заметим, что матрица  $B$  не содержит строку вида  $\theta_1^3, \theta_2^3, \dots, \theta_n^3$ , которая обязательно должна присутствовать, если значность кода более, чем 3.

Из теоремы 8.6.1 следует, что для доказательства данной теоремы достаточно показать, что система

$$\begin{aligned} z_1 + z_2 + z_3 &= \alpha_0 \\ z_1x_1 + z_2x_2 + z_3x_3 &= \alpha_1, \text{ где } z_1, z_2, z_3 \in \mathbb{F}_3, x_1, x_2, x_3 \in \mathbb{F}_q, \\ z_1x_1^2 + z_2x_2^2 + z_3x_3^2 &= \alpha_2 \end{aligned} \quad (8.6.4)$$

при любых  $\alpha_1, \alpha_3 \in \mathbb{F}_q$  и  $\alpha_0 \in \mathbb{F}_3$  имеет решение в поле  $\mathbb{F}_q$ . Докажем это.

Если  $(\alpha_0, \alpha_1, \alpha_2) \neq (0, 0, 0)$ , то, очевидно,

без ограничения общности, заменив  $\alpha_j$  на  $\frac{\alpha_j}{z_1}$ , мы можем полагать, что  $z_1 = 1$ . Положим  $x_1 = -z_2x_2 - z_3x_3, z_2 = z_3 = 1$ . В этом случае система 8.6.4 при  $x_2 \neq 0$  примет вид

$$(1 + y)^2 + 1 + y^2 = -y^2 - y - 1 = \frac{\alpha_2}{x_2}, \quad (8.6.5)$$

где  $y = \frac{x_3}{x_2}$ . Если  $\alpha_2 \neq 0$ , то не трудно показать, что при некотором значении  $x_2 \in \mathbb{F}_q \setminus \{0\}$  уравнение (8.6.5) имеет решение. (Упражнение.) Если же  $\alpha_2 = 0$ , то решением уравнения (8.6.5) является  $y = 1$ .  $\square$

### 8.6.3 Трои́чный код работы [26], исправляющий две ошибки

Другим интересным примером квазисовершенного кода является троичный код  $C_l$ , описанный в работе [26].

Пусть  $\mathbb{F}_q, q = 3^l$ , — конечное поле характеристики 3. Мы будем обозначать через  $G_l$  подгруппу порядка  $n = \frac{q+1}{2}$  мультипликативной группы  $\mathbb{F}_{q^2}^*$  поля  $\mathbb{F}_q$ . Элементами группы  $G_l$ , очевидно, являются все корни уравнения  $x^n - 1 = 0$ . Пусть  $\xi$  — порождающий элемент группы  $G_l$ .

Мы будем отдельно рассматривать два случая  $l = 2r$  и  $l = 2r + 1$  — четные и нечетные значения  $l$ . Обозначим через  $C_{2r}$  линейный троичный код длины  $n$  с проверочной матрицей

$$B_{2r} = (\xi_1, \xi_2, \dots, \xi_n), \quad (8.6.6)$$

где  $\xi_j = \xi^j$ .

Через  $C_{2r+1}$  мы обозначаем троичный код длины  $n$  с проверочной матрицей

$$B_{2r+1} = (\xi_1, \xi_2, \dots, \xi_n), \quad (8.6.7)$$

где  $\xi_j = \xi^j, i = 0, \dots, \frac{n}{2} - 1, \xi_j = \theta \xi^j, j = \frac{n}{2}, \dots, n - 1$ , и  $\theta$  — порождающий элемент подгруппы порядка 4 мультипликативной группы поля  $\mathbb{F}_{q^2}^*$ , или, по другому,  $\theta$  — корень уравнения  $x^4 - 1 = 0$ , такой, что  $\theta^2 = -1$ .

**Теорема 8.6.3** Код  $C_l$ ,  $l \geq 1$  является квазисовершенным линейным трочичным кодом, исправляющим две ошибки. При четном  $l$  код  $C_l$  является циклическим.

**Доказательство.** Сначала покажем, что кодовое расстояние кода  $C_l$  не меньше пяти, а именно покажем, что равенство

$$\sum_{i=0}^3 x_i \xi_{s_i} = 0, \quad x_i \in \mathbb{F}_3, \quad s_0 < s_1 < s_2 < s_3 \quad (8.6.8)$$

возможно только при  $x_0 = \dots = x_3 = 0$ .

Для этого возведем равенство (8.6.8) в степень  $2, 3^l, 3^{l+1}$ . В результате с учетом соотношения  $\xi_i^{3^l} = \xi_i^{-1}$  получим следующую систему линейных уравнений относительно неизвестных  $x_i$

$$\sum_{i=0}^3 x_i \xi_{s_i} = \sum_{i=0}^3 x_i \xi_{s_i}^3 = \sum_{i=0}^3 x_i \xi_{s_i}^{-1} = \sum_{i=0}^3 x_i \xi_{s_i}^{-3} = 0. \quad (8.6.9)$$

Определитель

$$\Delta = \begin{vmatrix} \xi_{s_0} & \xi_{s_1} & \xi_{s_2} & \xi_{s_3} \\ \xi_{s_0}^3 & \xi_{s_1}^3 & \xi_{s_2}^3 & \xi_{s_3}^3 \\ \xi_{s_0}^{-1} & \xi_{s_1}^{-1} & \xi_{s_2}^{-1} & \xi_{s_3}^{-1} \\ \xi_{s_0}^{-3} & \xi_{s_1}^{-3} & \xi_{s_2}^{-3} & \xi_{s_3}^{-3} \end{vmatrix} = (\xi_{s_0} \xi_{s_1} \xi_{s_2} \xi_{s_3})^{-3} \begin{vmatrix} \xi_{s_0}^2 & \xi_{s_1}^2 & \xi_{s_2}^2 & \xi_{s_3}^2 \\ \xi_{s_0}^6 & \xi_{s_1}^6 & \xi_{s_2}^6 & \xi_{s_3}^6 \\ \xi_{s_0}^4 & \xi_{s_1}^4 & \xi_{s_2}^4 & \xi_{s_3}^4 \\ \xi_{s_0}^0 & \xi_{s_1}^0 & \xi_{s_2}^0 & \xi_{s_3}^0 \end{vmatrix} \quad (8.6.10)$$

матрицы из коэффициентов этой системы кратен определителю Вандермонда — последнему определителю в (8.6.10). Определитель

Вандермонда отличен от 0 тогда и только тогда, когда все элементы  $\xi_{s_0}^2, \xi_{s_1}^2, \xi_{s_2}^2, \xi_{s_3}^2$  попарно различны. Как нетрудно проверить (Упражнение), элементы  $\xi_j$  определены так, что это свойство действительно выполнено. Это доказывает утверждение теоремы о кодовом расстоянии кода  $C_l$ .

Для доказательства квазисовершенности кода  $C_l$  достаточно показать, что для любого  $\alpha \in \mathbb{F}_{q^2}$ ,  $\alpha \neq 0$ , найдутся такие элементы  $\xi_{s_1}, \xi_{s_2}, \xi_{s_3}$  и элементы  $x_1, x_2, x_3 \in \mathbb{F}_3$ , что  $\alpha = x_1 \xi_{s_1} + x_2 \xi_{s_2} + x_3 \xi_{s_3}$ .

В виду того, что множество элементов  $\{\pm \xi_j | j = 1, \dots, n\}$  совпадает с множеством  $\Pi$  корней уравнения  $x^{3^{l+1}} - 1 = 0$ , достаточно показать разрешимость уравнения

$$\pi_1 + \pi_2 + \pi_3 = \alpha, \quad \pi_1, \pi_2, \pi_3 \in \Pi. \quad (8.6.11)$$

Заметим, что любой ненулевой элемент  $\alpha$  может быть представлен в виде  $\alpha = \pi \cdot \beta$ , где  $\pi \in \Pi$  и  $\beta$  — один из корней из корней уравнения  $y^{2(3^l-1)} - 1 = 0$ . таким образом, достаточно доказать разрешимость относительно  $\pi_1, \pi_2, \pi_3$  уравнения

$$\pi_1 + \pi_2 + \pi_3 = \beta, \quad \pi_1, \pi_2, \pi_3 \in \Pi, \quad (8.6.12)$$

где  $\beta$  — корень одного из уравнений  $y^{3^l-1} - 1 = 0$  или  $y^{3^l-1} + 1 = 0$ .

Доказательство разрешимости уравнения (8.6.12) является достаточно сложным и мы его приводить не будем. Полное доказательство, использующее, так называемую, оценку А.Вейля (см. теорему 9.2.1, в которой вместо аддитивного характера  $\chi$  нужно взять квадратичный характер мультипликативной группы поля  $\mathbb{F}_q$ ), имеется в работе [26]. Вместе



с тем читатель, возможно, сможет самостоятельно найти доказательство разрешимости уравнения (8.6.12) без использования оценки А.Вейля.

То, что при четном  $l$  код  $C_l$  — циклическим, является очевидным.  $\square$

(Упражнение. Предложить конструкцию циклического кода  $C_l$  при нечетном  $l$ )

## 8.6.4 Коды Геворкяна

Рассмотрим в несколько усовершенствованном виде конструкцию, предложенную в 1975 г. Д.Н. Геворкяном, троичного кода  $C_l^G$  длины  $n = \frac{3^l-1}{2}$  (на единицу меньше, чем у кода  $C_l$ ), исправляющего две ошибки, с тем же числом  $2l$  проверок что и у кода  $C_l$ , и четверичного длины  $n' = \frac{4^l-1}{3}$  также исправляющего две ошибки с числом проверок  $2l$ . Предположительно эти коды являются квазисовершенным, но доказательство этого факта автору не известно.

### Троичные коды

Мы будем обозначать через  $H_l$  подгруппу порядка  $n = \frac{3^l-1}{2}$  мультипликативной группы  $\mathbb{F}_{3^l}^*$  поля  $\mathbb{F}_{3^l}$  и через  $J_l$  — подгруппу порядка  $n' = \frac{4^l-1}{3}$  мультипликативной группы  $\mathbb{F}_{4^l}^*$  поля  $\mathbb{F}_{4^l}$ . Их элементами, очевидно, являются все корни уравнений  $x^n - 1 = 0$  и  $x^{n'} - 1 = 0$ . Пусть  $\xi$  — порождающий элемент группы  $H_l$  и  $\theta$  — порождающий элемент группы  $J_l$ .

В случае нечетного  $l$  (в этом случае длина  $n$  кода  $C_l^G$  является нечетным числом) в качестве проверочной матрицы троичного кода  $C_l^G$  мы возьмем матрицу

$$B_l^G = \begin{pmatrix} \xi & \xi^2 & \cdots & \xi^n \\ \xi^{-1} & \xi^{-2} & \cdots & \xi^{-n} \end{pmatrix}. \quad (8.6.13)$$

Заметим, что оригинальная конструкция Д.Н. Геворкяна матрицы  $B_l^G$  немного другая — его конструкция не обеспечивает цикличность кода  $C_l^G$ .

**Теорема 8.6.4** *При нечетном  $l \geq 1$  код  $C_l^G$  является линейным циклическим троичным кодом, исправляющим две ошибки.*

**Доказательство.** Цикличность кода  $C_l^G$  очевидна.

Покажем, что любые четыре различных столбца матрицы  $B_l^G$  являются линейно-независимыми. Действительно, предположим, что

$$\begin{aligned} \sum_{i=0}^3 x_i \xi^{s_i} &= 0, \\ \sum_{i=0}^3 x_i \xi^{-s_i} &= 0, \quad x_i \in \mathbb{F}_3, \quad s_0 < s_1 < s_2 < s_3. \end{aligned} \quad (8.6.14)$$

Возведем каждое из равенств в (8.6.14) в степень 3. В результате получим систему из четырех однородных линейных уравнений относительно неизвестных  $x_0, x_1, x_2, x_3$

$$\begin{aligned}
\sum_{i=0}^3 x_i \xi^{s_i} = 0, \quad \sum_{i=0}^3 x_i \xi^{3s_i} = 0, \\
\sum_{i=0}^3 x_i \xi^{-s_i} = 0, \quad \sum_{i=0}^3 x_i \xi^{-3s_i} = 0, \quad x_i \in \mathbb{F}_3, \quad s_0 < s_1 < s_2 < s_3.
\end{aligned} \tag{8.6.15}$$

Определитель

$$\Delta' = \begin{vmatrix} \xi^{s_0} & \xi^{s_1} & \xi^{s_2} & \xi^{s_3} \\ \xi^{3s_0} & \xi^{3s_1} & \xi^{3s_2} & \xi^{3s_3} \\ \xi^{-s_0} & \xi^{-s_1} & \xi^{-s_2} & \xi^{-s_3} \\ \xi^{-3s_0} & \xi^{-3s_1} & \xi^{-3s_2} & \xi^{-3s_3} \end{vmatrix} = (\xi^{s_0} \xi^{s_1} \xi^{s_2} \xi^{s_3})^{-3} \begin{vmatrix} \xi^{2s_0} & \xi^{2s_1} & \xi^{2s_2} & \xi^{2s_3} \\ \xi^{6s_0} & \xi^{6s_1} & \xi^{6s_2} & \xi^{6s_3} \\ \xi^{4s_0} & \xi^{4s_1} & \xi^{4s_2} & \xi^{4s_3} \\ \xi^0 & \xi^0 & \xi^0 & \xi^0 \end{vmatrix} \tag{8.6.16}$$

матрицы из коэффициентов этой системы кратен определителю Вандермонда — последнему определителю в (8.6.16). Этот определитель Вандермонда отличен от 0, ибо все элементы  $\xi^{2s_0}, \xi^{2s_1}, \xi^{2s_2}, \xi^{2s_3}$  попарно различны в виду того, что при нечетном  $l$  порядок группы  $H_l$  взаимно прост с числом 2.

Таким образом, система (8.6.16) имеет полный ранг и, следовательно, она не имеет ненулевых решений. Это доказывает утверждение теоремы о кодовом расстоянии кода  $C_l^G$ .  $\square$

Если  $l$  — нечетное число, то конструкцию матрицы  $B_l^G$  надо немного видоизменить. Например, можно использовать матрицу подобную матрице  $B_{2r+1}$  из раздела 8.6.3. В оригинальной работе Д.Н. Геворкяна используется матрица

$$B_l^G = \begin{pmatrix} \gamma & \gamma^2 & \cdots & \gamma^n \\ \gamma^{-1} & \gamma^{-2} & \cdots & \gamma^{-n} \end{pmatrix}, \tag{8.6.17}$$

где  $\gamma$  — порождающий элемент мультипликативной группы поля  $\mathbb{F}_{3^l}$ . В этом случае  $C_l$  — троичный код с кодовым расстоянием, по меньшей мере, 5, который не является циклическим. (Упражнение)

### Четверичные коды

Пусть  $\vartheta$  — порождающий элемент мультипликативной группы поля  $\mathbb{F}_{4^l}$ ,  $n = \frac{4^l-1}{3}$  и

$$B_l^G = \begin{pmatrix} \vartheta & \vartheta^2 & \cdots & \vartheta^n \\ \vartheta^{-1 \cdot 2} & \vartheta^{-2 \cdot 2} & \cdots & \vartheta^{-n \cdot 2} \end{pmatrix}, \tag{8.6.18}$$

— порождающая матрица четверичного кода  $C_l^G$ .

**Теорема 8.6.5** Код  $C_l^G$  является линейным четверичным кодом длины  $n = \frac{4^l-1}{3}$  и размерности над  $\mathbb{F}_4$  равной  $\log_4(3n-1)$ , исправляющим две ошибки.

**Доказательство** сводится к доказательству невырожденности однородной системы линейных уравнений относительно неизвестных  $x_0, x_1, x_2, x_3$

$$\begin{aligned} \sum_{i=0}^3 x_i \vartheta^{s_i} = 0, \quad \sum_{i=0}^3 x_i \vartheta^{4s_i} = 0, \\ \sum_{i=0}^3 x_i \vartheta^{-s_i} = 0, \quad \sum_{i=0}^3 x_i \vartheta^{-4s_i} = 0, \quad x_i \in \mathbb{F}_4, \quad s_0 < s_1 < s_2 < s_3. \end{aligned} \quad (8.6.19)$$

Это свойство доказывается почти также как и в доказательстве теоремы 8.6.4.  $\square$

Следует отметить, что коды теоремы 8.6.5 не являются циклическими. (Упражнение. Видоизменить матрицу (8.6.19) так, чтобы код  $C_l^G$  был циклическим) Возможно, они являются квазисовершенными, но, как уже отмечалось, доказательство этого неизвестно. (Упражнение. Изучить коды, двойственные к  $C_l^G$ )

### Двоичные коды

Пусть  $\zeta$  — порождающий элемент мультипликативной группы поля  $\mathbb{F}_{2^l}$ ,  $n = 2^l - 1$  и

$$B_l^G = \begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^n \\ \zeta^{1 \cdot 3} & \zeta^{2 \cdot 3} & \cdots & \zeta^{n \cdot 3} \end{pmatrix}, \quad (8.6.20)$$

— порождающая матрица двоичного БЧХ-кода  $\mathfrak{K}_l$ . Код  $\mathfrak{K}_l$  исправляет две ошибки (теорема 5.2.2) и имеет размерность  $2l$  (теорема 5.2.3).

**Теорема 8.6.6** *Код  $\mathfrak{K}_l$  является линейным циклическим квазисовершенным кодом длины  $n = 2^l - 1$ , исправляющим две ошибки.*

**Доказательство.** Из теоремы 8.6.1 вытекает, что достаточно доказать разрешимость системы уравнений

$$\sum_{i=1}^3 y_i = \alpha, \quad \sum_{i=1}^3 y_i^3 = \beta, \quad y_i \in \mathbb{F}_{2^l} \quad (8.6.21)$$

при любых  $\alpha, \beta \in \mathbb{F}_{2^l}$ . Положим  $z_i = y_i + \alpha$ ,  $i=1,2,3$ . В результате получим (упражнение), что система (8.6.23) имеет решение тогда и только тогда, когда их имеет система

$$\sum_{i=1}^3 z_i = 0, \quad \sum_{i=1}^3 z_i^3 = \gamma, \quad z_i \in \mathbb{F}_{2^l}, \quad \gamma = \alpha^3 + \beta. \quad (8.6.22)$$

Полагая  $z_3 = z_1 + z_2$ , получаем систему

$$z_1 z_2 (z_1 + z_2) = \gamma. \quad (8.6.23)$$

Положим  $x = \frac{z_1}{z_2}$ ,  $z_2 \neq 0$ . В этом случае для разрешимости системы достаточно установить разрешимость в поле  $\mathbb{F}_{2^l}$  уравнения

$$x^2 + x + \frac{\gamma}{z_2^3} = 0. \quad (8.6.24)$$

при некотором  $z_2 \in \mathbb{F}_q^*$ .

Для того, чтобы уравнение было разрешимо должно найтись такое  $z_2$ , что  $Tr(\frac{\gamma}{z_2^3}) = 0$ . (см. Приложение I). Это свойство при  $l > 2$  непосредственно вытекает из следствия 8.1.1.  $\square$

Проверочная матрица двоичного кода Гоппы  $\mathfrak{K}_G$  длины  $n = 2^l$ , исправляющие две ошибки, имеют вид

$$B_l = \left( \frac{1}{\vartheta - a_1}, \frac{1}{\vartheta - a_1}, \dots, \frac{1}{\vartheta - a_{2^l-1}} \right), \quad (8.6.25)$$

где  $\vartheta$  — корень неприводимого многочлена  $x^2 + ax + b$ ,  $a, b \in \mathbb{F}_{2^l}$  и  $\{a_0, a_1, \dots, a_{2^l-1}\} = \mathbb{F}_{2^l}$  (см.

см. раздел 5.3.3 и теорему 5.3.2).

Используя оценку А.Вейля, нетрудно доказать следующую теорему. (Упражнение)

**Теорема 8.6.7** *Двоичный код Гоппы  $\mathfrak{K}_G$  длины  $n = 2^l$ , исправляющие две ошибки, является квазисовершенным.*

## Глава 9

# Весовой спектр линейного кода

Пусть  $\mathcal{K} \in \mathbb{F}_q^n$  — линейный код. Обозначим через  $\eta_j = \eta_j(\mathcal{K})$ ,  $j = 0, \dots, n$ , — число векторов в коде  $\mathcal{K}$  веса  $j$ . Очевидно,  $\eta_0 = 1$  и  $\eta_j = 0$ , если  $j = 1, \dots, d-1$ , где  $d$  — кодовое расстояние кода  $\mathcal{K}$ . Вектор  $\eta(\mathcal{K}) = (\eta_0, \dots, \eta_n)$  называется спектром кода  $\mathcal{K}$ .

Вместе с кодом  $\mathcal{K}$  рассмотрим код  $\mathcal{K}^\perp$ , двойственный к нему (см. раздел 1.1.3), и его спектр  $\eta(\mathcal{K}^\perp)$ .

Вообще говоря, спектр  $\eta(\mathcal{K})$  не определяет линейный код  $\mathcal{K}$ : различные в том или ином смысле (уточнять не будем) коды могут иметь один и тот же спектр. Вместе с тем, как мы увидим далее, спектр  $\eta(\mathcal{K})$  полностью определяется спектром двойственного кода  $\eta(\mathcal{K}^\perp)$  и наоборот. Это утверждение достаточно давно известно в теории кодирования под названием соотношение МакВильямс.

Это соотношение обычно формулируется в терминах нумератора  $W_{\mathcal{K}}(x)$  весов кода  $\mathcal{K}$ . Нумератор определяется следующим образом.

$$W_{\mathcal{K}}(x, y) = \sum_{j=0}^n \eta_j x^j y^{n-j}, \quad (9.0.1)$$

где  $x, y$  — формальные переменные. Если обозначить через  $w(\mathbf{a})$  вес Хемминга вектора  $\mathbf{a} \in \mathbb{F}_q^n$ , то последнее соотношение, очевидно, можно записать в виде

$$W_{\mathcal{K}}(x, y) = \sum_{\mathbf{a} \in \mathcal{K}} x^{w(\mathbf{a})} y^{n-w(\mathbf{a})}. \quad (9.0.2)$$

Функция

$$\psi_{\mathcal{K}}(\mathbf{a}) = \begin{cases} 1, & \text{если } \mathbf{a} \in \mathcal{K}, \\ 0, & \text{если } \mathbf{a} \notin \mathcal{K}. \end{cases} \quad (9.0.3)$$

называется характеристической функцией кода  $\mathcal{K}$ .

С помощью функции  $\psi_{\mathcal{K}}(\mathbf{x})$  соотношение (9.0.2) можно, очевидно, записать в виде

$$W_{\mathcal{K}}(x, y) = \sum_{\mathbf{a} \in \mathbb{F}_q^n} \psi_{\mathcal{K}}(\mathbf{a}) x^{w(\mathbf{a})} y^{n-w(\mathbf{a})}. \quad (9.0.4)$$

Как мы увидим далее, характеристическая функция  $\psi_{\mathcal{K}}(\mathbf{x})$  достаточно просто может быть представлена через спектр кода  $\mathcal{K}^\perp$ . Поэтому равенство 9.0.4 после некоторых преобразований превращается в соотношение, которое носит название соотношения МакВильямс. Оно связывает спектр кода  $\mathcal{K}$  со спектром кода  $\mathcal{K}^\perp$ . Перед выводом соотношения

МакВильямс получим явное представление характеристической функции  $\psi_{\mathfrak{K}}(\mathbf{x})$  через параметры кода  $\mathfrak{K}^\perp$ .

Во-первых, заметим, что

**Теорема 9.0.8 (Соотношение МакВильямс)** *Имеет место соотношение*

$$\begin{aligned} W_{\mathfrak{K}}(x, y) &= \frac{1}{|\mathfrak{K}^\perp|} W_{\mathfrak{K}^\perp}(y - x, y + (q - 1)x) = \\ &= \frac{1}{|\mathfrak{K}^\perp|} \sum_{s=0}^n \nu_s (y - x)^s (y + (q - 1)x)^{n-s}, \end{aligned} \quad (9.0.5)$$

где  $\nu_s$  — число векторов веса  $s$  в коде  $\mathfrak{K}^\perp$ .

Перед доказательством теоремы докажем лемму.

**Лемма 9.0.1** *Пусть  $l(\mathbf{x})$  — ненулевая линейная над  $\mathbb{F}_p$  функция, отображающая элементы поля  $\mathbb{F}_q$  в элементы поля  $\mathbb{F}_p$ .*

*Тогда характеристической функцией  $\psi_{\mathfrak{K}}(\mathbf{x})$  кода  $\mathfrak{K}$  может быть представлена в виде*

$$\psi_{\mathfrak{K}}(\mathbf{x}) = \frac{1}{|\mathfrak{K}^\perp|} \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \exp\left(\frac{2\pi i l(\langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right), \quad \mathbf{x} \in \mathbb{F}_q^n. \quad (9.0.6)$$

**Доказательство.** Как следует из определения двойственного кода вектор  $\mathbf{x}$  принадлежит коду  $\mathfrak{K}$  тогда и только тогда, когда  $\langle \mathbf{x}, \mathbf{y} \rangle = 0$  для всех  $\mathbf{y} \in \mathfrak{K}^\perp$ , где  $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \dots + x_n y_n$  — скалярное произведение в поле  $\mathbb{F}_q$ . Поэтому, если  $\mathbf{x} \notin \mathfrak{K}$ , то существует такое  $\mathbf{y}_0 \in \mathfrak{K}^\perp$ , что  $\langle \mathbf{x}, \mathbf{y}_0 \rangle \neq 0$ . Отметим, что для любого  $b \in \mathbb{F}_q$  элемент  $b\mathbf{y}_0$  также принадлежит коду  $\mathfrak{K}^\perp$ . Отсюда для любого  $b \in \mathbb{F}_q$  следует, что

$$\begin{aligned} \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \exp\left(\frac{2\pi i l(\langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right) &= \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \exp\left(\frac{2\pi i l(\langle \mathbf{x}, \mathbf{y} + b\mathbf{y}_0 \rangle)}{p}\right) \\ &= \exp\left(\frac{2\pi i l(b\langle \mathbf{x}, \mathbf{y}_0 \rangle)}{p}\right) \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \exp\left(\frac{2\pi i l(a\langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right). \end{aligned} \quad (9.0.7)$$

$l(\cdot)$  — ненулевая линейная функция и  $\langle \mathbf{x}, \mathbf{y}_0 \rangle \neq 0$ , поэтому существует такое  $b_0 \in \mathbb{F}_q$ , что  $l(b_0 \langle \mathbf{x}, \mathbf{y}_0 \rangle) \neq 0$ . Отсюда следует, что множитель  $\exp\left(\frac{2\pi i l(b_0 \langle \mathbf{x}, \mathbf{y}_0 \rangle)}{p}\right)$  в правой части (9.0.7) отличен от 1. Следовательно,  $\psi_{\mathfrak{K}}(\mathbf{x}) = \exp\left(\frac{2\pi i l(b_0 \langle \mathbf{x}, \mathbf{y}_0 \rangle)}{p}\right) \psi_{\mathfrak{K}}(\mathbf{x})$ . Это возможно, только при  $\psi_{\mathfrak{K}}(\mathbf{x}) = 0$ .

Если  $\mathbf{x} \in \mathfrak{K}$ , то, очевидно,  $\psi_{\mathfrak{K}}(\mathbf{x}) = 1$ .  $\square$

**Следствие 9.0.1** *Если  $\mathbb{F}_q$  — простое поле, т.е.  $q = p$ , тогда характеристической функцией  $\psi_{\mathfrak{K}}(\mathbf{x})$  кода  $\mathfrak{K}$  может быть представлена в виде*

$$\psi_{\mathfrak{K}}(\mathbf{x}) = \frac{1}{|\mathfrak{K}^\perp|} \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \exp\left(\frac{2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}{p}\right), \quad \mathbf{x} \in \mathbb{F}_q^n. \quad \square \quad (9.0.8)$$

### Доказательство теоремы 9.0.8.

Подставим в соотношение (9.0.4) выражение (9.0.6) для характеристической функции  $\psi_{\mathfrak{K}}(\mathbf{x})$ . В результате получим

$$W_{\mathfrak{K}}(x, y) = \frac{1}{|\mathfrak{K}^\perp|} \sum_{\mathbf{y} \in \mathfrak{K}^\perp} \sum_{\mathbf{x} \in \mathbb{F}_q^n} x^{w(\mathbf{x})} y^{n-w(\mathbf{x})} \exp\left(\frac{2\pi i l(\langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right). \quad (9.0.9)$$

Как следует из определения,  $w(\mathbf{x}) = w(x_1) + \dots + w(x_n)$ ,  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ , где  $w(x) = \begin{cases} 1, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0 \end{cases}$ . Поэтому

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} x^{w(\mathbf{x})} y^{n-w(\mathbf{x})} \exp\left(\frac{2\pi i l(\langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right) = \prod_{s=1}^n \sum_{x_s \in \mathbb{F}_q} x^{w(x_s)} y^{1-w(x_s)} \exp\left(\frac{2\pi i l(x_s y_s)}{p}\right). \quad (9.0.10)$$

Как легко установить,

$$\sum_{x_s \in \mathbb{F}_q} x^{w(x_s)} y^{1-w(x_s)} \exp\left(\frac{2\pi i l(x_s y_s)}{p}\right) = \begin{cases} (y - x), & \text{если } y_s \neq 0, \\ y + (q-1)x, & \text{если } y_s = 0 \end{cases}. \quad (9.0.11)$$

Следовательно, при  $a \neq 0$

$$\sum_{\mathbf{x} \in \mathbb{F}_q^n} x^{w(\mathbf{x})} \exp\left(\frac{2\pi i l(a \langle \mathbf{x}, \mathbf{y} \rangle)}{p}\right) = ((1-x))^{w(\mathbf{y})} (1 + (q-1)x)^{n-w(\mathbf{y})}. \quad (9.0.12)$$

Возвращаясь теперь к соотношению (9.0.9), получим равенство МакВильямс (9.0.5).

□

**Лемма 9.0.2** Пусть  $l(\mathbf{x})$  — произвольная ненулевая линейная функция, отображающая аддитивную группу поля  $\mathbb{F}_q$  в аддитивную группу поля  $\mathbb{F}_p$ .

## 9.1 Спектр линейного кода и многочлены Кравчука

### 9.1.1 Соотношение МакВильямс для весовой функции линейного кода

Многочлены Кравчука были определены в разделе 3 (см. равенство (3.2.13)). Они играют весьма существенную роль в теории кодирования. В настоящем разделе мы изучаем соотношения, которые с помощью многочленов Кравчука и им подобным выражают спектр линейного кода  $\mathfrak{K}$  через спектр кода  $\mathfrak{K}^\perp$ , двойственного к нему.

Сначала отметим, что если приравнять коэффициенты при  $x^s y^{n-s}$  в левой и правой частях соотношения МакВильямс (9.0.5), то мы, как нетрудно установить, при  $q = p$  получим

$$\eta_w = \frac{1}{|\mathfrak{K}^\perp|} \sum_{s=0}^n P_w(s) \nu_s, \quad (9.1.1)$$

где многочлен Кравчука  $P_w(s) = K_w^{(p,n)}(x)$  определен равенством (3.2.13). Обратно, если для спектров  $\eta(\mathfrak{K})$  и  $\eta(\mathfrak{K}^\perp) = (\nu_0, \dots, \nu_n)$  выполнено соотношение (4.1.1), то нумератор  $W(x, y)$  спектра  $\eta(\mathfrak{K})$  может быть представлен в виде (9.0.5).

Как представляется автору, соотношение (4.1.1) играет в теории кодирования фундаментальную роль. Это происходит по следующим двум причинам.

Во-первых, равенство (4.1.1) с помощью теории характеров, изложенной в разделе 3, можно довольно просто обобщить в нескольких направлениях.

Во-вторых, равенство (4.1.1) позволяет вывести новые соотношения между спектрами кодов  $\mathfrak{K}$  и  $\mathfrak{K}^\perp$ , которые позволяют в некоторых случаях получить явные асимптотические выражения элементов спектра кода  $\mathfrak{K}$ . Об этом подробно написано в разделе 9.1.3.

Соотношение МакВильямс оставляет меньше простора для обобщений и исследований спектра кода.

Как уже было отмечено, (см. раздел 3.2.3, главы 3) функция  $wt(\mathbf{x})$  является центральной относительно мономиальной группы  $H \subset \text{Aut}(\mathbb{F}_p^n)$ . Напомним, что  $H$  действует на элементарной абелевой группе  $\mathbb{F}_p^n$  посредством умножения ее элементов на мономиальные матрицы. Классы сопряженных элементов группы  $\mathbb{F}_p^n$  относительно мономиальной группы  $H$  ее автоморфизмов образованы векторами из  $\mathbb{F}_p^n$  определенного веса.

Несколько иначе об этом можно сказать следующим образом. Аддитивная группа  $\mathbb{F}_q^n$  относительно действия  $H$  разбивается на  $n+1$  орбит  $A_0, \dots, A_n$ . Орбита  $A_w$  состоит из векторов  $\mathbf{x} \in \mathbb{F}_p^n$  веса  $w$ . Функция  $wt(\mathbf{x})$  на каждой орбите  $A_w$  принимает одно и то же значение —  $w$ .

Соотношение (9.1.1) может быть выведено следующим образом. Очевидно

$$\eta_w = \sum_{wt(\mathbf{x})=w} \psi_{\mathfrak{K}}(\mathbf{x}), \quad (9.1.2)$$

где  $\psi_{\mathfrak{K}}(\mathbf{x})$  — характеристическая функция кода  $\mathfrak{K}$  и суммирование в сумме  $\sum_{wt(\mathbf{x})=w}$  производится по всем векторам  $\mathbf{x}$  из  $\mathbb{F}_p^n$ , вес которых равен  $w$ .

С другой стороны, как легко увидеть, значение функции

$$\Phi_w(\mathbf{y}) = \sum_{wt(\mathbf{x})=w} \exp\left(\frac{2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}{p}\right) \quad (9.1.3)$$

определяется только значением  $wt(\mathbf{y}) = s$ , т.е.  $\Phi_{\mathbf{x}}(\mathbf{y})$  — центральная функция как по  $\mathbf{y}$  относительно действия мономиальной группы  $H$ . (Упражнение)

$$\Phi_H(\mathfrak{x}, \varpi) = S_H(s)P_H(s, w) = \tilde{S}_{\tilde{H}}(w)\tilde{P}_{\tilde{H}}(w, s), \text{ если } \mathfrak{x} \in A_s, \varpi \in \tilde{A}_w, \quad (9.1.4)$$

Заметим, что функция  $\Phi_w(\mathbf{x})$  совпадает с функцией  $Y_w(\mathfrak{y}) = \sum_{\varpi \in \tilde{A}_w} \varpi(\mathfrak{y})$ , где  $\mathfrak{y} = \mathbf{y}$  (см. 3.1.17), поэтому

$$\Phi_w(\mathbf{x}) = P_H(s, w) = P_w(s), \quad (9.1.5)$$

если  $wt(\mathbf{x}) = s$  (см. (3.1.18)).

Отсюда, используя представление (9.0.6) характеристической функции  $\psi_{\mathfrak{K}}(\mathbf{x})$ , и соотношения (9.1.2) и (9.1.5), получим равенство (9.1.1), из которого, как было отмечено выше, вытекает соотношение МакВильямс (9.0.5).



### 9.1.2 Соотношение МакВильямс для полной весовой функции линейного кода

Вышеприведенные рассуждения относительно вывода соотношения (9.1.1) могут быть легко перенесены на функции, которые являются центральными относительно действия на группе  $\mathbb{F}_p^n$  той или иной подгруппе ее группы автоморфизмов. Далее речь пойдет о симметрической группе в качестве группы  $H$  (см. главу 3, раздел "Симметрическая группа в качестве группы  $H$  и полная весовая функция").

Рассмотрим функцию  $c_k(\mathbf{x})$ , равную числу координат у вектора  $\mathbf{x}$ , принимающих значение  $k \in \mathbb{F}_p$ . Вектор  $\mathbf{c}(\mathbf{x}) = (c_0(\mathbf{x}), \dots, c_{p-1}(\mathbf{x}))$  называется композицией вектора  $\mathbf{x}$  или полным весом вектора  $\mathbf{x}$ .

Очевидно, композиция  $\mathbf{c}(\mathbf{x})$  является центральной функцией относительно действия на группе  $\mathbb{F}_p^n$  симметрической группы  $S_n$ , элементы которой переставляют координаты векторов из  $\mathbb{F}_p^n$ .

Обозначим через  $\kappa_{\mathbf{c}} = \kappa_{\mathbf{c}}(\mathcal{K})$  — число векторов  $\mathbf{x}$  кода  $\mathcal{K}$ , у которых композиция  $\mathbf{c}(\mathbf{x})$  равна  $\mathbf{c}$ . Множество векторов

$$\kappa = \kappa(\mathcal{K}) = \{\kappa_{\mathbf{c}}(\mathcal{K}) \mid \mathbf{c} = (c_0, \dots, c_{p-1}) \text{ пробегает все векторы такие, что } c_0 + \dots + c_{p-1} = n\} \quad (9.1.6)$$

называется композиционным спектром или полным спектром кода  $\mathcal{K}$ .

Как следует из соотношения 9.0.8,

$$\kappa_{\mathbf{c}} = \sum_{\mathbf{c}(\mathbf{x})=\mathbf{c}} \psi_{\mathcal{K}}(\mathbf{x}) = \frac{1}{|\mathcal{K}^\perp|} \sum_{\mathbf{y} \in K^\perp} \sum_{\mathbf{c}(\mathbf{x})=\mathbf{c}} \exp\left(\frac{2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}{p}\right), \quad (9.1.7)$$

где  $\psi_{\mathcal{K}}(\mathbf{x})$  — характеристическая функция кода  $\mathcal{K}$  и суммирование в сумме  $\sum_{\mathbf{c}(\mathbf{x})=\mathbf{c}}$  производится по всем  $\mathbf{x} \in \mathbb{F}_p^n$  таким, что  $\mathbf{c}(\mathbf{x}) = \mathbf{c}$ .

Предположим, что  $c_k(\mathbf{y}) = w_k$ ,  $k = 0, \dots, p-1$ ,  $w_0 + \dots + w_{p-1} = n$  и  $\mathbf{w} = (w_0, \dots, w_{p-1})$ . Легко увидеть, что

$$\Phi_{\mathbf{c}}(\mathbf{y}) = \sum_{\mathbf{c}(\mathbf{x})=\mathbf{c}} \exp\left(\frac{2\pi i \langle \mathbf{x}, \mathbf{y} \rangle}{p}\right), \quad (9.1.8)$$

функция определяется только значением функции  $\mathbf{c}(\mathbf{y}) = \mathbf{w}$ , т.е.  $\Phi_{\mathbf{c}}(\mathbf{y}) = \Phi_{\mathbf{c}}(\mathbf{y}')$ , если  $\mathbf{c}(\mathbf{y}) = \mathbf{c}(\mathbf{y}')$ .

Пусть  $\mathbf{c}(\mathbf{y}) = \mathbf{w}$ . Используя элементарные комбинаторные соображения, связанные с размещением  $p$  различных чисел (предметов)  $0, \dots, p-1$  каждый в числе  $c_0, \dots, c_{p-1}$  по  $p$  ящиков, каждый объемом  $w_0, \dots, w_{p-1}$ , получим

$$\Phi_{\mathbf{c}}(\mathbf{y}) := p_{\mathbf{c}}(\mathbf{w}) = \widetilde{\sum} \binom{w_0}{c_{0,0}, \dots, c_{0,p-1}} \cdots \binom{w_{p-1}}{c_{p-1,0}, \dots, c_{p-1,p-1}} \exp\left(\frac{2\pi i \sum_{t=0}^{p-1} t c_{t,s}}{p}\right), \quad (9.1.9)$$

где  $c_{t,s}$  — число символов равных  $t$  в векторе  $\mathbf{x}$  попавших на символ  $s$  в векторе  $\mathbf{y}$ . Суммирование в сумме  $\widetilde{\sum}$  производится по всем векторам  $\mathbf{c}^{(j)} = (c_{j,0}, \dots, c_{j,p-1})$ ,  $j = 0, \dots, p-1$ , таким, что  $\sum_{s=0}^{p-1} c_{j,s} = c_j$ ,  $j = 0, \dots, p-1$ , и  $\sum_{t=0}^{p-1} c_{t,s} = w_s$ ,  $s = 0, \dots, p-1$ .

Пусть  $z_0, \dots, z_m$  — формальные переменные. Непосредственно видно, что

$$p_{\mathbf{c}}(\mathbf{w}) = \text{coeff}_{z_0^{c_0} \dots z_{p-1}^{c_{p-1}}} \prod_{j=0}^l \left( \sum_{s=0}^m \exp \left( \frac{2\pi i s}{p} \right) z_s \right)^{w_j}. \quad (9.1.10)$$

Соотношение (9.1.9) позволяют записать равенство (9.1.7) в виде

$$\kappa_{\mathbf{c}} = \sum_{\mathbf{w}} p_{\mathbf{c}}(\mathbf{w}) \nu_{\mathbf{w}}(\mathfrak{K}^\perp), \quad (9.1.11)$$

где  $\nu_{\mathbf{w}}(\mathfrak{K}^\perp)$  — число векторов в коде  $\mathfrak{K}^\perp$ , у которых полный вес равен  $\mathbf{w}$ .

Если воспользоваться соотношением (9.1.10), то равенство (9.1.11) можно представить в виде

$$\begin{aligned} \sum_{\mathbf{c}} \kappa_{\mathbf{c}}(\mathfrak{K}) z_0^{c_0} z_1^{c_1} \dots z_{p-1}^{c_{p-1}} = \\ \frac{1}{|\mathfrak{K}^\perp|} \sum_{\mathbf{w}} \nu_{\mathbf{w}}(\mathfrak{K}^\perp) \prod_{j=0}^{p-1} \left( z_0 + \exp \left( \frac{2\pi i j}{p} \right) z_1 + \dots + \exp \left( \frac{2\pi i (p-1)j}{p} \right) z_{p-1} \right)^{w_j}, \end{aligned} \quad (9.1.12)$$

где суммирование в суммах  $\sum_{\mathbf{c}}$  и  $\sum_{\mathbf{w}}$  производится по всем векторам  $\mathbf{c} = (c_0, \dots, c_{p-1})$  и  $\mathbf{w} = (w_0, \dots, w_{p-1})$  таким, что  $c_0 + \dots + c_{p-1} = w_0 + \dots + w_{p-1} = n$ .

Заметим, что функцию  $p_{\mathbf{c}}(\mathbf{w})$ , определенная соотношением (9.1.9), можно рассматривать как многочлен от целочисленных переменных  $w_0, \dots, w_{p-1}$ , связанных соотношением  $w_0 + \dots + w_{p-1} = n$ . Таким образом  $p_{\mathbf{c}}(\mathbf{w})$  — многочлен от  $p-1$  целочисленных независимых переменных. Как легко установить, многочлен  $p_{\mathbf{c}}(\mathbf{w})$  при  $p=2$  является многочленом Кравчука (см. равенство (3.2.13)).

Как следует из теоремы 3.1.1 многочлены  $p_{\mathbf{c}}(\mathbf{w})$  являются ортогональными с весами  $C_{\mathbf{w}} = \binom{n}{w_0, \dots, w_{p-1}}$ , т.е.

$$\frac{1}{p^n} \sum_{\mathbf{w}} C_{\mathbf{w}} p_{\mathbf{c}}(\mathbf{w}) p_{\mathbf{c}'}(\mathbf{w}) = \begin{cases} 0, & \text{если } \mathbf{c} \neq \mathbf{c}', \\ C_{\mathbf{c}}, & \text{если } \mathbf{c} = \mathbf{c}'. \end{cases} \quad (9.1.13)$$

### 9.1.3 Использование соотношения МакВильямс для вычисления спектра кода.

Пусть  $\mathfrak{K}$  — линейный над конечным полем  $\mathbb{F}_p$  ( $p$  — простое число) код длины  $n$  и размерности  $k$ . Как и ранее, мы обозначаем через  $\eta_s = \eta_s(\mathfrak{K})$  число элементов кода  $\mathfrak{K}$ , вес которых равен  $s$ . Вектор  $\boldsymbol{\eta}(\mathfrak{K}) = (\eta_0, \eta_1, \dots, \eta_n)$  называется спектром кода  $\mathfrak{K}$ , а функция

$$W_{\mathfrak{K}}(x, y) = \sum_{j=0}^n \eta_j x^j y^{n-j} = \sum_{\mathbf{a} \in \mathfrak{K}} x^{wt(\mathbf{a})} y^{n-wt(\mathbf{a})}, \quad (9.1.14)$$

где  $wt(\mathbf{x})$  — вес вектора  $\mathbf{x}$ , — нумератором кода  $\mathfrak{K}$ . (см. также раздел 9)

Через  $\mathfrak{K}^\perp$  мы обозначаем код ортогональный в пространстве  $\mathbb{F}_p^n$  к коду  $\mathfrak{K}$ . Код  $\mathfrak{K}^\perp$  состоит из всех векторов  $\mathbf{b} \in \mathbb{F}_p^n$ , для которых  $(\mathbf{b}, \mathbf{a}) = 0$  при всех  $\mathbf{a} \in \mathfrak{K}$ , где  $(\mathbf{b}, \mathbf{a}) = \sum_{j=1}^n a_j b_j$  — скалярное произведение в пространстве  $\mathbb{F}_p^n$ .

Как показано в разделе 9 спектры  $\boldsymbol{\eta}(\mathfrak{K})$  и  $\boldsymbol{\eta}(\mathfrak{K}^\perp) = (\nu_0, \nu_1, \dots, \nu_n)$  связаны, так называемым, соотношением МакВильямса (9.0.5).

Для вычисления спектра  $\boldsymbol{\eta}(\mathfrak{K})$  кода  $\mathfrak{K}$  равенство (9.0.5) можно использовать следующим образом. Предположим, что нам известна некая информация о спектре кода  $\mathfrak{K}^\perp$ . В этом случае можно получить определенную информацию и о спектре кода  $\mathfrak{K}$ .

В качестве примера рассмотрим двоичный код  $\mathfrak{K} = R_{m-2}$  Рида-Маллера  $m-2$ -порядка, длины  $n = 2^m$  и размерности  $k = 2^m - m - 1$ . Проверочная матрица этого кода имеет вид

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_{1,1} & a_{1,2} & \cdots & a_{1,2^m-1} & a_{1,2^m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,2^m-1} & a_{2,2^m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,2^m-1} & a_{m,2^m} \end{pmatrix}, \quad a_{i,j} \in \mathbb{F}_2, \quad (9.1.15)$$

где все вектор-столбцы  $\begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{m,j} \end{pmatrix}$ ,  $j = 1, \dots, 2^m$ , с координатами из  $\mathbb{F}_2$  различны. Заме-

тим, что коды Рида-Маллера будут подробно изучаться далее в главе 7.

Как легко видеть, любые три столбца матрицы  $B$  являются линейно-независимыми над полем  $\mathbb{F}_2$ . Кроме того, сумма любых трех столбцов матрицы  $B$  является одним из ее столбцов. Поэтому код  $\mathfrak{K} = R_{m-2}$  содержит вектор веса 4. Следовательно, в соответствии с теоремой 1.1.1 кодовое расстояние кода  $R_{m-1}$  равно 4.

С другой стороны, очевидно, спектр линейного кода  $R_{m-2}^\perp = R_1$  размерности  $m+1$ , который представляет собой пространство, натянутое на строки матрицы  $B$ , имеет вид

$$\boldsymbol{\eta}(R_{m-2}^\perp) = (1, 0, \dots, 0, 2(n-1), 0, \dots, 0, 1), \quad (9.1.16)$$

где координата со значением  $2(n-1)$  имеет номер  $\frac{n}{2} = 2^{m-1}$ . (Упражнение)

Таким образом, соотношение МакВильямса (9.0.5) для кода  $R_{m-2}$  примет вид

$$W_{R_{m-2}}(x, y) = \frac{1}{2n} ((x+y)^n + 2(n-1)(x+y)^{n/2}(y-x)^{n/2} + (y-x)^n) \quad (9.1.17)$$

Приравнивая коэффициенты при  $x^w y^{n-w}$  в левой и правой частях равенства (14.3.11), получим

$$\eta_w = \frac{1}{2n} \left( \binom{n}{w} (K_w^{(2,n)}(0) + K_w^{(2,n)}(n)) + 2(n-1) K_w^{(2,n)}\left(\frac{n}{2}\right) \right), \quad (9.1.18)$$

где  $K_w^{(2,n)}(c) = \text{coeff}_{x^c y^{n-c}} (y-x)^w (x+y)^{n-w}$  — многочлен Кравчука (см. (3.2.13) и (3.2.15)). Заметим, что  $K_w^{(2,n)}(0) = \binom{n}{w}$  и  $K_w^{(2,n)}(n) = (-1)^w \binom{n}{w}$ . Так как  $(y-x)^{\frac{n}{2}} (y+x)^{\frac{n}{2}} = (y^2 - x^2)^{\frac{n}{2}}$ , то  $K_w^{(2,n)}(\frac{n}{2}) = 0$  при нечетных значениях  $w$  и  $K_{2t}^{(2,n)}(\frac{n}{2}) = (-1)^t \binom{n/2}{t}$  при четных значениях  $w = 2t$ . Отсюда следует

$$\eta_w = \begin{cases} 0, & \text{если } w \text{ — нечетное число} \\ \frac{1}{n} \left( \binom{n}{2t} + (-1)^t (n-1) \binom{n/2}{t} \right), & \text{если } w = 2t \end{cases}. \quad (9.1.19)$$

Таким образом, мы вычислили спектр кода  $R_{m-2}$ , исходя из известного спектра двойственного к  $R_{m-2}$  кода  $R_{\perp m-2} = R_1$ .

Заметим, что из соотношений (9.1.19) вытекает, что  $\eta_0 = 1$ ,  $\eta_1 = \eta_2 = \eta_3 = 0$  и

$$\eta_4 = \frac{1}{n} \left( \binom{n}{4} + 2(n-1) \binom{\frac{n}{2}}{2} \right). \quad (9.1.20)$$

Соотношение (9.1.20) имеет интересную комбинаторную трактовку, а именно, векторы кода  $R_{m-2}$  веса 4 являются векторами инцидентности, так называемой, системы Штейнера.

Пусть  $X$  — конечное множество с  $n$  элементами. Набор  $S(t, w, n) = \{B_1, \dots, B_N\}$   $w$ -подмножеств (блоков)  $B_j$  множества  $X$  называется системой Штейнера, если любое  $t$ -подмножество множества  $X$  содержится ровно в одном блоке набора  $S(t, w, n)$ . Это понятие является частным случаем понятия комбинаторной тактической конфигурации. Общеизвестная система троек Штейнера в наших обозначениях является системой  $S(2, 3, n)$ .

Если в качестве набора  $\{B_1, \dots, B_N\}$  взять четырехэлементные подмножества  $B_j$  множества  $X = \{1, \dots, 2^m\}$ , у которых вектором инцидентности является один из векторов веса 4 кода  $R_{m-2}$ , то мы получим систему Штейнера  $S(3, 4, n)$ , у которой  $N = \eta_4$ . (Упражнение) Это утверждение является частным случаем теоремы Ассмуса-Меттсона [48].

Соотношение (9.1.20) можно представить в виде

$$\eta_4 = \begin{cases} 0, & \text{если } w \text{ — нечетное число,} \\ \frac{1}{n} \binom{n}{w} (1 + \epsilon_{4,n}), & \text{если } w \text{ — четное число,} \end{cases} \quad (9.1.21)$$

где  $\epsilon_{4,n} \sim \frac{1}{n}$ ,  $n \rightarrow \infty$ . (Упражнение. Доказать асимптотическое равенство, аналогичное (9.1.21), для соотношения (9.1.19).)

В общем случае из соотношения МакВильямс (9.0.8) вытекает равенство (4.1.1). Это соотношение позволяет с помощью многочленов Кравчука  $K_w^{(p,n)}(x)$  представить спектр кода  $\mathfrak{K}$  через спектр кода, двойственного к нему. Получаемые при этом явные выражения для  $\eta_w$  являются весьма громоздкими. Более того, если спектр кода  $\mathfrak{K}^\perp$  известен не точно, например, для его элементов известны только асимптотические выражения, то соотношение (4.1.1), по существу, не позволяет вычислить даже приближенно величину  $\eta_w$  из-за того, что значение многочлена Кравчука в точке  $x$  трудно представить в виде простого и явного асимптотического выражения.

Вместе с тем, соотношение (4.1.1) подходит для вычисления спектра кода  $\mathfrak{K}$  с помощью ЭВМ для кодов, для которых точно известен спектр его двойственного кода  $\mathfrak{K}^\perp$ .

Получить нетривиальные асимптотические оценки для величин  $|K_w^{(p,n)}(x)|$  весьма непросто. Они известны в случае  $x = 0$   $x = n$ :  $K_w^{(p,n)}(0) = \binom{n}{w} (p-1)^w$  и  $K_w^{(p,n)}(n) = \binom{n}{w} (-1)^w$ . Также достаточно просто получить асимптотические оценки  $|K_w^{(p,n)}(x)|$  в случае  $x = \frac{(p-1)n}{p} (1 + \epsilon)$ ,  $n \rightarrow \infty$ .

Из этих оценок вытекает, что если  $|K_w^{(p)}(x)| \ll K_w^{(p)}(0) = (p-1)^j \binom{n}{w}$  и код не содержит ненулевых векторов маленького и очень большого веса (спектр сосредоточен около  $\frac{(p-1)n}{p}$ ), то определяющими членами в правой части суммы (4.1.1) являются первый и последний (при  $w = 0$  и  $w = n$ ). В этом случае можно ожидать, что

$$\eta_w \approx \frac{1}{|\mathfrak{K}^\perp|} \binom{n}{w} ((p-1)^w + (-1)^w \nu_n), \quad (9.1.22)$$

где  $\nu_n$  — число векторов максимального веса  $n$  в коде  $\mathfrak{K}^\perp$ , в виду того, что сумма всех остальных членов суммы в (4.1.1) будет предположительно малой по сравнению с крайними членами.

Строго доказать соотношение, подобное (9.1.22), весьма непросто. Это сделано только для некоторых кодов  $\mathfrak{K}$  специального вида. В частности, в работе [36] строго доказано соотношение подобное (9.1.22) для величин  $\eta_w$  двоичного кода Боуза-Чоудхури-Хоквингема длины  $n = 2^m - 1$  в случае  $n \rightarrow \infty$  и числе исправляемых ошибок  $t = o(\sqrt{n})$ . Этот результат получен с использованием глубокой и нетривиальной оценки А. Вейля сумм с характеристиками. А именно, с помощью оценки А. Вейля получена оценка  $\sum_{s=1}^{n-1} \nu_s K_s^{(2,n)}(x) \ll \binom{n}{j}$ , из которой следует соотношение (9.1.22).

В последующих разделах мы покажем как можно получать асимптотические выражения для элементов  $\eta_w$  спектра кода  $\mathfrak{K}$ , не вычисляя явно значений многочлена Кравчука. Это позволит нам, в частности, вывести достаточно простыми методами указанный выше результат о спектре БЧХ-кода.

#### 9.1.4 Функция типа $\chi^2$ для элементов спектра кода $\mathfrak{K}$ .

Мы рассматриваем квадрат взвешенного среднего отклонения числа элементов спектра кода  $\mathfrak{K}$  от биномиального распределения. Говоря более точно, мы для линейного над  $\mathbb{F}_p$  кода  $\mathfrak{K}$  длины  $n$  рассматриваем функцию

$$\Xi(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|} \sum_{w=1}^n \frac{(\eta_w - \omega(w)|\mathfrak{K}|)^2}{\omega(w)}, \quad (9.1.23)$$

где  $\omega(w) = \omega_p(w) := \frac{(p-1)^w \binom{n}{w}}{p^n}$ . Число  $\omega(w)$  можно трактовать как долю векторов веса  $w$  в всем пространстве  $\mathbb{F}_p^n$ . Заметим, что функция  $\omega(w)$  имеет колоколообразный график, принимая наибольшие значения, которые приблизительно равны  $\frac{C}{\sqrt{n}}$ , при  $w \sim \frac{(p-1)n}{p}$ . При  $w$  таких, что  $|w - \frac{(p-1)n}{p}| \geq c \cdot n$ ,  $c > 0$ , значение функции  $\omega(w)$  экспоненциально от  $n$  число раз меньше, чем  $\omega(\frac{(p-1)n}{p})$ .

Функция  $\Xi(\mathfrak{K})$  представляет собой нормированный средний квадрат отклонения элементов  $\eta_w$  спектра кода  $\mathfrak{K}$  от ожидаемого значения —  $\omega(w)|\mathfrak{K}|$ .

Выбор нормировки (иначе — весовой функции  $\frac{1}{\omega(w)}$ ) представляется естественным: вклад "типичных" элементов (элементов  $\eta_w$  со значениями  $w$  около  $\frac{p-1}{p}n$ ) делится на большое число  $\omega(w) = (p-1)^w \binom{n}{w} p^{-n}$ , а вклад "не типичных" элементов  $\eta_w$ , т.е. с "маленькими" или "очень большими" значениями  $w$ , — на относительно небольшое число  $\omega(w)$ .

Естественно полагать, что модуль отклонения  $|\eta_w - \omega(w)|\mathfrak{K}|$  имеет порядок  $\sqrt{\omega(w)|\mathfrak{K}|} \approx \sqrt{\eta_w}$ , поэтому сумма в (9.1.23) предположительно по порядку равна  $n$  при больших  $k$  и  $n - k$ . Это утверждение строго не доказано.

Функцию  $\Xi(\mathfrak{K})$  можно выразить через нормированную сумму квадратов элементов  $\nu$  спектра двойственного кода  $\mathfrak{K}^\perp$  (Теорема 9.1.1). Это в некоторых случаях позволяет находить асимптотические выражения для элементов спектра кода  $\mathfrak{K}$ .

В следующем разделе рассматриваются тождества, которые связывают функцию  $\Xi(\mathfrak{K})$  с некоторыми функциями от спектра кода  $\mathfrak{K}^\perp$ .

### 9.1.5 Выражение функции $\Xi(\mathfrak{K})$ через спектр двойственного кода.

**Теорема 9.1.1** Пусть  $P(x)$  — произвольный многочлен степени  $\leq n$  с коэффициентами из поля действительных чисел и

$$P(x) = \sum_{t=0}^n \alpha_t K_t^{(p,n)}(x) \quad (9.1.24)$$

— его представление через базис  $\{K_t^{(p,n)}(x) | t = 0, \dots, n\}$  ортогональных многочленов Кравчука.

Тогда для элементов  $\eta_j$  спектра кода  $\mathfrak{K}$  и элементов  $\nu_j$  спектра кода  $\mathfrak{K}^\perp$  выполнено соотношение

$$\frac{1}{|\mathfrak{K}^\perp|} \sum_{t=0}^n \frac{(\nu_t - \omega(t)P(t))^2}{\omega(t)} = \frac{1}{|\mathfrak{K}|} \sum_{s=0}^n \frac{(\eta_s - \omega(s)|\mathfrak{K}|\alpha_s)^2}{\omega(s)}. \quad (9.1.25)$$

$$\text{где } \omega(j) = \frac{(p-1)^j \binom{n}{j}}{p^n}.$$

**Доказательство.** Равенство (4.1.1), меняя местами  $\mathfrak{K}$  и  $\mathfrak{K}^\perp$ , запишем в виде

$$\nu_j = \frac{1}{|\mathfrak{K}|} \sum_{x=0}^n \eta_x K_j^{(p,n)}(x). \quad (9.1.26)$$

Используя лемму 3.2.1, получим соотношение

$$K_j^{(p,n)}(s)\omega(s) = K_s^{(p,n)}(j)\omega(j). \quad (9.1.27)$$

С помощью (9.1.27) соотношение (9.1.26) представим в виде

$$\frac{\nu_j}{\omega(j)} = \frac{1}{|\mathfrak{K}|} \sum_{s=0}^n \frac{\eta_s K_s^{(p,n)}(j)}{\omega(s)}. \quad (9.1.28)$$

Из равенств (9.1.28) и (9.1.24) следует соотношение

$$\frac{\nu_j}{\omega(j)} - P(j) = \sum_{s=0}^n \left( \frac{\eta_s}{\omega(s)|\mathfrak{K}|} - \alpha_s \right) K_s^{(p,n)}(j). \quad (9.1.29)$$

Возведем обе части последнего равенства в квадрат. Затем умножим их на  $\omega(j)$  и просуммируем по  $j$  от 0 до  $n$ . Воспользовавшись соотношением ортогональности для многочленов  $K_j^{(p)}(s)$  (см. (3.2.17)), соотношением (9.1.27) в результате получим

$$\sum_{t=0}^n \frac{(\nu_j - \omega(j)P(j))^2}{\omega(j)} = \frac{p^n}{|\mathfrak{K}|^2} \sum_{s=0}^n \frac{(\eta_s - \omega(s)|\mathfrak{K}|\alpha_s)^2}{\omega(s)}, \quad (9.1.30)$$

что эквивалентно (9.1.25), ибо  $|\mathfrak{K}| \cdot |\mathfrak{K}^\perp| = p^n$ .  $\square$

Теорема 9.1.1 была впервые доказана в работе [26].

Несколько следующих следствий вытекают из теоремы 9.1.1 с помощью выбора подходящего многочлена  $P(x)$ .

**Следствие 9.1.1** *Имеет место соотношение*

$$\Xi(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|} \sum_{j=0}^n \frac{(\eta_j - \omega(j)|\mathfrak{K}|)^2}{\omega(j)} = \frac{1}{|\mathfrak{K}^\perp|} \sum_{j=1}^n \frac{\nu_j^2}{\omega(j)}, \quad (9.1.31)$$

где  $\nu_j$  — число элементов кода  $\mathfrak{K}^\perp$  веса  $j$ .

**Доказательство.** Заметим, что значения многочлена  $K_0(s) = \sum_{t=0}^n K_w^{(p,n)}(s)$  равны 0 при  $s = 1, \dots, n$  и  $K_0(0) = p^n$ . Это можно установить следующим образом.

Из равенства (3.2.15) вытекает, что  $K_0(s) = \Omega(s, 1, 1)$ , где

$$\Omega(s, x, y) = (y - x)^s (x + (p - 1)y)^{n-s} = \sum_{w=0}^n K_w^{(p,n)}(s) x^w y^{n-w}. \quad (9.1.32)$$

Заметим, что  $\nu_0 - \omega(0)K_0(0) = 0$ , ибо  $\nu_0 = 1$ .

Отсюда и равенства (9.1.25), в котором положено  $P(s) = K_0(s)$ , т.е. в (9.1.25)  $\alpha_s = 1$ ,  $s = 0, \dots, n$ , следуют требуемое соотношение (9.1.31).  $\square$

**Следствие 9.1.2** *Имеет место соотношение*

$$\Xi_1(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|} \sum_{s=0}^n \frac{\left( \eta_s - \left( 1 + \nu_n \frac{(-1)^s}{(p-1)^s} \right) \omega(s) |\mathfrak{K}| \right)^2}{\omega(s)} = \frac{1}{|\mathfrak{K}^\perp|} \sum_{t=1}^{n-1} \frac{\nu_t^2}{\omega(t)}, \quad (9.1.33)$$

где  $\nu_n$  — число элементов в коде  $\mathfrak{K}^\perp$ .

**Доказательство.** Пусть  $K_1(s) = \sum_{t=0}^n \left( -\frac{1}{p-1} \right)^t K_t^{(p,n)}(s)$ . Из очевидного соотношения  $K_1(s) = \Omega(s, 1, -\frac{1}{p-1})$  следует, что

$$K_1(s) = \begin{cases} 0, & \text{если } s = 0, \dots, n-1, \\ \frac{p^n}{(p-1)^n}, & \text{если } s = n \end{cases}. \quad (9.1.34)$$

Отсюда и из (9.1.25), в котором положено  $P(x) = K_0(x) + \nu_n K_1(x)$ , следует (9.1.33).  $\square$

**Следствие 9.1.3** *При  $p = 2$ ,  $\nu_n = 1$  равенство (9.1.33) принимает вид*

$$\Xi_1(\mathfrak{K}) = \frac{1}{|\mathfrak{K}|} \sum_{s=0}^{\lfloor \frac{n}{2} \rfloor} \frac{(\eta_{2s} - 2\omega(2s)|\mathfrak{K}|)^2}{\omega(2s)} = \frac{1}{|\mathfrak{K}^\perp|} \sum_{t=1}^{n-1} \frac{\nu_t^2}{\omega(t)}. \quad (9.1.35)$$

$\square$

Заметим, что при  $p = 2$  и  $\nu_n = 1$  код содержит векторы только четного веса и поэтому  $\nu_{2j+1} = 0$ .

**Замечание 9.1.1** *Если положить в Теореме (9.1.1)*

$$P(x) = \frac{1}{|\mathfrak{K}|} \sum_{s=0}^n \eta_s \frac{K_s^{(p,n)}(x)}{\omega(t)}, \quad (9.1.36)$$

то левая равенства (9.1.25) обратится в нуль. Следовательно,

$$(\nu_t - \omega(t)P(t))^2 = 0, \quad t = 0, \dots, n. \quad (9.1.37)$$

Последнее соотношение, с учетом соотношения (9.1.27) совпадает с соотношением (4.1.1), в котором переставлены местами  $\nu_t$  и  $\eta_s$ . Соотношение (4.1.1) является одной из форм соотношения МакВильямс.

Это показывает, что в рассматриваемом случае Теорема (9.1.1) и соотношение МакВильямс (Теорема 9.0.8) являются эквивалентными утверждениями.

### 9.1.6 Среднее функции $\Xi(\mathfrak{K})$

Вычисление значения функции  $\Xi(\mathfrak{K})$  (см. (9.1.31)) дает содержательную "глобальную" информацию о спектре  $\eta(\mathfrak{K})$  кода  $\mathfrak{K}$ , в частности, об его отклонении от биномиального закона распределения. Вместе с тем в общем случае вычислить правую или левую части соотношения (9.1.31) при больших значениях  $k = \dim \mathfrak{K}$  и  $n - k$  не представляется возможным. Это происходит потому, что в настоящее время неизвестно как по проверочной или порождающей матрицы вычислить спектр  $\eta(\mathfrak{K})$  без явного вычисления весов всех элементов  $\mathfrak{K}$  или  $\mathfrak{K}^\perp$ .

Естественно попытаться вычислить среднее значение  $M\Xi_1(\mathfrak{K})$  функции  $\Xi(\mathfrak{K})$ , взятое по всем кодам  $\mathfrak{K}$  с заданной размерностью  $k$ , и сравнить его со значением  $\Xi(\mathfrak{K})$  для конкретного кода  $\mathfrak{K}$ . Если  $M\Xi_1(\mathfrak{K}) \sim \Xi_1(\mathfrak{K}_m)$ , то можно говорить о том, что спектр  $\eta(\mathfrak{K}_m)$  является "типичным" среди всех спектров кодов заданной размерности.

Автору вычислить или оценить значение  $M_k = M\Xi(\mathfrak{K})$ ,  $k = \dim \mathfrak{K}$  не удалось, хотя он затратил на это значительные усилия. Вместе с тем эта задача по нашим представлениям не безнадежна.

### 9.1.7 Пример вычисления спектра кода $\mathfrak{K}$ с помощью функции $\Xi(\mathfrak{K})$

Для многих кодов  $\mathfrak{K}$  можно получить информацию о спектре кода  $\mathfrak{K}^\perp$ . Эту информацию можно использовать для получения асимптотических выражений для элементов спектра кода  $\mathfrak{K}$ .

Например, код  $R_1 = R_{m-2}^\perp$ , двойственный к коду  $\mathfrak{K} = R_{m-2}$ , имеет спектр  $\eta(R_{m-2}^\perp)$ , определяемым соотношением (9.1.16). Поэтому правую часть равенства (9.1.35) можно оценить сверху следующим образом:

$$\frac{1}{|R_1|} \sum_{t=1}^{n-1} \frac{\nu_t^2}{\omega(t)} < \frac{|R_1|}{\omega(\frac{n}{2})}. \quad (9.1.38)$$

С другой стороны, при любом  $s \leq \frac{n}{2}$  левую часть равенства (9.1.35) можно оценить снизу следующим образом:

$$\frac{1}{|R_{m-2}|\omega(2s)} (\eta_{2s} - 2\omega(2s)|\mathfrak{K}|)^2 < \frac{1}{|R_{m-2}|} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{(\eta_{2j} - 2\omega(2j)|R_{m-2}|)^2}{\omega(2j)}. \quad (9.1.39)$$

Отсюда с учетом соотношений (9.1.35), (9.1.39) и  $|RM_1| \cdot |R_{m-2}| = 2^n$  получим



$$(\eta_{2s} - 2\omega(2s)|R_{m-2}|) | < \sqrt{\frac{2^n \omega(2s)}{\omega(\frac{n}{2})}}. \quad (9.1.40)$$

Из оценок для биномиальных коэффициентов (Лемма 2.0.5) вытекает, что

$$\omega\left(\frac{n}{2}\right) = 2^{-n} \binom{n}{\frac{n}{2}} < \frac{1}{C_0 \sqrt{n}}, \quad (9.1.41)$$

где  $C_0$  — абсолютная постоянная, и, следовательно, правая часть (9.1.40) не превосходит  $C_1 n^{\frac{1}{4}} \binom{n}{2s}^{\frac{1}{2}}$ , где  $C_1 = \sqrt{C_0}$ .

Отсюда

$$|(\eta_{2s} - 2\omega(2s)|R_{m-2}|) | < C_1 n^{\frac{1}{4}} \sqrt{\binom{n}{2s}}. \quad (9.1.42)$$

Так как для достаточно больших  $n$   $2\omega(2s)|R_{m-2}| = \frac{\binom{n}{2s}}{n} > C_1 n^{\frac{1}{4}} \sqrt{\binom{n}{2s}}$ ,  $s = 2, \dots, \frac{n}{2} - 2$ , то оценку (8.2.1) можно записать в виде

$$\eta_{2s} = 2\omega(2s)|R_{m-2}|(1 + \epsilon_n) = \frac{\binom{n}{2s}}{n}(1 + \epsilon_n), \quad s = 2, \dots, \frac{n}{2} - 2, \quad (9.1.43)$$

где  $\epsilon_n \rightarrow 0$ , если  $n \rightarrow \infty$ .

Таким образом, мы снова получили соотношение (9.1.21), но при этом мы не вычисляли и не оценивали значения многочленов Кравчука. Это обстоятельство во многих случаях имеет принципиальное значение. Например, при получении асимптотических выражений элементов спектра для БЧХ-кодов приходится, если используется соотношение (4.1.1), оценивать значения многочленов Кравчука в точках  $x$ , отличных от  $x = \frac{n}{2}$ . Получение подобных оценок представляет значительные сложности и, кроме того, во многих случаях приводит к огрублению получаемых оценок для элементов спектра.

В следующем разделе мы с помощью Теоремы 9.1.1 получим асимптотические выражения для элементов спектра БЧХ-кодов.

## 9.2 Спектр БЧХ-кодов

В сущности, в настоящем разделе мы повторим рассуждения предыдущего раздела, использованные при получении выражения (9.1.43), но в значительно более сложном случае.

Мы будем использовать глубокий результат (оценка Вейля), полученный французским математиком А. Вейлем в 1947 г, который известен также как граница Карлица-Ушиямы. В настоящее время этот результат общеизвестен. Более подробные сведения о ней имеются, например, в книге [18].

Перед формулировкой результата А. Вейлем напомним некоторые определения. Линейная над полем  $\mathbb{F}_p$  функция след  $Tr(x)$ ,  $x \in \mathbb{F}_q$ ,  $q = p^l$ , отображающая поле  $\mathbb{F}_q$  в поле  $\mathbb{F}_p$ , была определена в главе 5 (равенство (5.1.11) при  $r = p$ ).

Функция

$$\chi(x) = \exp\left(\frac{2\pi i Tr(x)}{p}\right), \quad i = \sqrt{-1}, \quad (9.2.1)$$

называется характером аддитивной группы поля  $\mathbb{F}_q$ . Она гомоморфно отображает аддитивную группу поля  $\mathbb{F}_q$  в группу корней из 1  $p$ -ой степени, т.е.  $\chi(x+y) = \chi(x)\chi(y)$ ,  $x, y \in \mathbb{F}_q$ .

**Теорема 9.2.1 (Оценка А.Вейля)** Если  $f(x) \in \mathbb{F}_q[x]$  такой многочлен, что функция  $Tr(f(x))$  принимает, по меньшей мере, два различных значения при  $x \in \mathbb{F}_q$ , т.е.  $Tr(f(x)) \not\equiv \text{const}$ , тогда

$$T_f = \left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (r-1)q^{\frac{1}{2}}, \text{ где } r = \deg f(x). \quad (9.2.2)$$

Оценка (9.2.2) является нетривиальной, только если  $r-1 \leq \sqrt{q}$ .

Мы рассматриваем коды Рида-Соломона  $\mathfrak{K}(B_{\mathcal{A}}^{(d)})$  типа 2 длины  $q$ , т.е. коды, у которых проверочная матрица  $B = B_{\mathcal{A}}^{(d)}$  (см. (5.0.1)), определяется множеством  $\mathcal{A} = \mathbb{F}_q$ . Как обычно, код  $BCH(B_{\mathcal{A}}^{(d)}) = \mathfrak{K}(B_{\mathcal{A}}^{(d)}) \cap \mathbb{F}_p^q$  мы будем называть БЧХ-кодом над полем  $\mathbb{F}_p$  типа 2.

Код  $\mathfrak{K}^{\perp}(B_{\mathcal{A}}^{(d)})$ , двойственный к коду  $\mathfrak{K}(B_{\mathcal{A}}^{(d)})$ , очевидно, состоит из всех векторов вида

$$\mathbf{a}_f = (f(\alpha_1), \dots, f(\alpha_q)) \quad (9.2.3)$$

**Лемма 9.2.1** Подпространство пространства  $\mathbb{F}_p$ , состоящее из всех векторов вида

$$\mathbf{a}_f = (Tr(f(\alpha_1)), \dots, Tr(f(\alpha_q))), \deg f \leq d-2, \quad (9.2.4)$$

является кодом  $BCH^{\perp}(B_{\mathcal{A}}^{(d)})$ , двойственный к коду  $BCH(B_{\mathcal{A}}^{(d)})$ .

**Доказательство.** Пусть  $\omega = \{\omega_1, \dots, \omega_l\}$  — какой-либо базис поля  $\mathbb{F}_q$  над полем  $\mathbb{F}_r$ . В этом случае элемент  $\alpha \in \mathbb{F}_q$  можно представить в виде  $\alpha = \sum_{j=1}^l a_j \omega_j$ ,  $a_j \in \mathbb{F}_p$ . Вектор  $\bar{\alpha} = (a_1, \dots, a_l)$  является записью элемента  $\alpha$  поля  $\mathbb{F}_q$  в базисе  $\omega$ .

Заменим в матрице  $B_{\mathcal{A}}^{(d)}$  каждый элемент  $\alpha_i^s$  вектором-столбцом  $\bar{\alpha}_i^{sT}$ . В результате получим матрицу  $\widehat{B}_{\mathcal{A}}^{(d)}$  с элементами из поля  $\mathbb{F}_p$ . По определению код, натянутый на строки матрицы  $\widehat{B}_{\mathcal{A}}^{(d)}$ , является кодом  $BCH^{\perp}(B_{\mathcal{A}}^{(d)})$ .

Таким образом, нам надо показать, что пространство векторов  $L_d = \{\mathbf{a}_f \mid \deg f \leq d-2\}$  совпадает с пространством строк матрицы  $\widehat{B}_{\mathcal{A}}^{(d)}$ .

Пусть  $\mathbf{b} \in BCH(B_{\mathcal{A}}^{(d)})$ . Из определения функции  $Tr(x)$  следует, что  $\langle \mathbf{b}, \mathbf{a}_f \rangle = 0$  для всех  $\mathbf{a}_f \in L_d$ . Поэтому  $L_d \subseteq BCH^{\perp}(B_{\mathcal{A}}^{(d)})$ .

С другой стороны, рассмотрим  $l \times q$ -матрицу  $B_{\mathcal{A}}^{(d),s} = (\bar{a}_1^{sT}, \dots, \bar{a}_q^{sT})$ ,  $0 \leq s \leq d-2$ . Легко показать, что пространство строк матрицы  $B_{\mathcal{A}}^{(d),s}$  принадлежит пространству  $\{\mathbf{a}_f \mid f(x) = ax^s\}$ . Поэтому  $BCH^{\perp}(B_{\mathcal{A}}^{(d)}) \subseteq L_d$ , что доказывает лемму.  $\square$

**Лемма 9.2.2** Если  $\alpha_f \in BCH^{\perp}(B_{\mathcal{A}}^{(d)})$  и  $Tr(f(x)) \not\equiv \text{const}$ , то

$$\frac{p-1}{p} (q + (d-3)\sqrt{q}) \geq w(\alpha_f) \geq \frac{p-1}{p} (q - (d-3)\sqrt{q}). \quad (9.2.5)$$

**Доказательство.** Очевидно, вес  $wt(\alpha)$  вектора  $\alpha = (a_1, \dots, a_n) \in \mathbb{F}_p^n$  равен

$$wt(\alpha) = q - \sum_{s=1}^n \frac{1}{p} \left( \sum_{j=0}^{p-1} \exp \left( \frac{2\pi i j a_s}{p} \right) \right). \quad (9.2.6)$$

Отсюда следует, что

$$w(\alpha_f) = q - \frac{1}{p} \sum_{x \in \mathbb{F}_q} \sum_{j=0}^{p-1} \chi^j(f(x)) = \left( \frac{p-1}{p} q - \frac{1}{p} \sum_{j=1}^{p-1} \sum_{x \in \mathbb{F}_q} \chi^j(f(x)) \right). \quad (9.2.7)$$

Отсюда и из оценки А. Вейля (9.2.2) следуют оценки (9.2.7).  $\square$

**Теорема 9.2.2** Пусть  $p > 2$ ,  $\mathfrak{K} = BCH(B_A^{(d)})$  —  $p$ -значный БЧХ-кода длины  $q = p^l$  с гарантированным кодовым расстоянием  $d$ , определяемый проверочной матрицей  $B_A^{(d)}$ ,  $A = \mathbb{F}_q$  (см. (5.0.1)), и пусть  $r_d = 1 + l \cdot \left( d - 2 - \left\lfloor \frac{d-2}{p} \right\rfloor \right)$  — размерность кода  $BCH^\perp(B_A^{(d)})$  (см. Теорему 5.2.3).

Тогда при

$$d = \text{const}, \quad q \rightarrow \infty, \quad \text{и} \quad s > 2 \left( d - 2 - \left\lfloor \frac{d-2}{p} \right\rfloor \right) \quad (9.2.8)$$

имеет место асимптотическое представление элемента  $\eta_s = \eta_s(BCH(B_A^{(d)}))$  спектра кода  $BCH(B_A^{(d)})$

$$\eta_s = p^{-r_d} ((p-1)^s + (-1)^s(p-1)) \binom{q}{s} (1 + \varepsilon_{s,q}), \quad (9.2.9)$$

где

$$\varepsilon_{s,q} \asymp q^{-\frac{1}{4}} p^{r_d} (p-1)^{-s} \binom{q}{s}^{-\frac{1}{2}} \rightarrow 0 \quad \text{при} \quad q \rightarrow \infty. \quad (9.2.10)$$

**Доказательство.** Мы будем использовать соотношение (9.2.20) Следствия 9.1.2.

Во-первых, докажем, что в условиях теоремы  $\nu_q = p-1$ . Предположим, что  $\alpha_f \in BCH^\perp(B_A^{(d)})$  и  $Tr(f(x)) \not\equiv \text{const}$ . Тогда согласно (9.2.5)  $w(\alpha_f) < q$ . Таким образом,  $w(\alpha_f) = q$  только, если  $Tr(f(x)) \equiv \text{const} \in \mathbb{F}_p$ .

Степень ненулевого многочлена  $Tr(x)$  равна  $p^{l-1} < q$ . Поэтому он принимает ненулевое значение при

некотором  $x \in \mathbb{F}_q$ , т.е. для некоторого  $a \in \mathbb{F}_q$   $Tr(a) = b \neq 0$ ,  $b \in \mathbb{F}_p$ . Поэтому при подходящем  $c \in \mathbb{F}_p \setminus \{0\}$  и  $f(x) = a$  многочлен  $Tr(cf(x)) = cTr(f(x)) = cb$  принимает любое наперед заданное ненулевое значение. Отсюда следует, что код  $BCH^\perp(B_A^{(d)})$  содержит ровно  $p-1$  векторов  $\alpha_f$  веса  $q$ , которые определяются многочленами  $f(x)$ , имеющими вид  $f(x) = ac$ .

Так как  $|\mathfrak{K}||\mathfrak{K}^\perp| = p^q$ , то из (9.2.20) следует, что при любом  $s$

$$\left( \eta_s - \left( 1 + \nu_q \frac{(-1)^s}{(p-1)^s} \right) \omega(s) |\mathfrak{K}| \right)^2 < |\mathfrak{K}| \omega(s) \Xi_1(\mathfrak{K}) = \frac{1}{|\mathfrak{K}^\perp|^2} \binom{q}{s} \sum_{t=1}^{n-1} \frac{\nu_t^2}{\omega(t)} = R_d. \quad (9.2.11)$$

Оценим сверху правую часть  $R_d$  неравенства (8.6.11). Из Леммы 9.2.2 (равенство (9.2.5)) следует, что выполнено соотношение

$$\nu_t = 0, \text{ если } \left| t - \frac{(p-1)q}{p} \right| > \frac{p-1}{p} (d-3) \sqrt{q}. \quad (9.2.12)$$

Отсюда и из очевидного неравенства  $\sum_{t=1}^{n-1} \nu_t^2 < |\mathfrak{K}^\perp|^2$  следует, что

$$R_d \leq \frac{1}{\omega_{\min} |\mathfrak{K}^\perp|^2} \binom{q}{s} \sum_{t=1}^{n-1} \nu_t^2 < \frac{\binom{q}{s}}{\omega_{\min}}, \quad (9.2.13)$$

где  $\omega_{\min} = \min \omega(t)$  и  $\min$  берется по всем  $t$  таким, что  $\left| t - \frac{(p-1)q}{p} \right| \leq \frac{p-1}{p} (d-3) \sqrt{q}$ .

Очевидно,  $\min \omega(t)$  достигается на границе интервала  $\left[ \frac{(p-1)q}{p} - (d-3) \sqrt{q}, \frac{(p-1)q}{p} + (d-3) \sqrt{q} \right]$  изменения параметра  $t$ , т.е.

$$\omega_{\min} = \frac{1}{p^q} \min \left( (p-1)^{t_0} \binom{q}{t_0}, (p-1)^{t_1} \binom{q}{t_1} \right), \quad (9.2.14)$$

где  $t_0 = \frac{p-1}{p} (q - (d-3) \sqrt{q})$  и  $t_1 = \frac{p-1}{p} (q + (d-3) \sqrt{q})$ .

Как следует из оценок вероятностей биномиального распределения (см. Лемму 2.0.5, оценки (2.0.44)), если  $d = \text{const}$ ,  $q \rightarrow \infty$ , то

$$\omega_{\min} = \frac{1}{C_d \sqrt{q}}, \quad (9.2.15)$$

где постоянная  $C_d$  зависит от параметра  $d$ . (Упражнение)

Согласно Лемме 5.2.5 в условиях теоремы  $d = \text{const}$ ,  $q \rightarrow \infty$  размерность кода  $\mathfrak{K}^\perp$  равна  $r_d = 1 + \left( d - 2 - l \cdot \left\lfloor \frac{d-2}{p} \right\rfloor \right)$ . Поэтому

$$\omega(s) |\mathfrak{K}| = \frac{\binom{q}{s}}{p^{r_d}}. \quad (9.2.16)$$

Отсюда с учетом того, что  $\nu_q = p-1$ , из (8.6.11), (9.2.13), (9.2.16) следует оценка

$$\left| \left( \eta_s - p^{-r_d} ((p-1)^s + (-1)^s (p-1)) \binom{q}{s} \right) \right| < \sqrt{R_d} < \sqrt{C_d \sqrt{q} \binom{q}{s}} = Q_{d,s}. \quad (9.2.17)$$

Из последней оценки вытекает, что если  $p = \text{const}$ ,  $q \rightarrow \infty$ , то

$$\varepsilon_{s,q} = \frac{Q_{d,s}}{p^{-r_d} ((p-1)^s + (-1)^s (p-1)) \binom{q}{s}} \asymp q^{\frac{1}{4}} p^{r_d} (p-1)^{-s} \binom{q}{s}^{-\frac{1}{2}}, \quad p > 2, s > 1. \quad (9.2.18)$$

Если  $d = \text{const}$ , то  $r_d = 1 + l \cdot \left( d - 2 - \left\lfloor \frac{d-2}{p} \right\rfloor \right) = \text{const}'$  (см. (5.2.16)). Следовательно, при  $s > 2 \left( d - 2 - \left\lfloor \frac{d-2}{p} \right\rfloor \right)$

$$\varepsilon_{s,q} \rightarrow 0 \text{ при } q \rightarrow \infty. \quad (9.2.19)$$

Это доказывает теорему.  $\square$

Заметим, что условие теоремы  $p > 2$  необходимо только при выводе соотношения (9.2.19). В случае  $p = 2$  соотношение (9.2.19) не выполняется, если  $s > q - 2 \left( d - 2 - \left\lfloor \frac{d-2}{p} \right\rfloor \right)$ , т.е. тогда, когда  $s$  близко к числу  $q$ . Этот случай мы рассмотрим отдельно.

**Следствие 9.2.1** В условиях Теоремы 9.2.2 при  $p = 2$  имеет место асимптотическое представление элемента спектра  $\eta_s$  :

$$\eta_{2s} = 2^{-r_d} \binom{q}{2s} (1 + \varepsilon_{2s,q}) \quad \text{для всех } s \text{ таких, что } d \leq s \leq q - d, \quad (9.2.20)$$

и  $\eta_t = 0$ , для всех нечетных  $t$ ,

где  $|\varepsilon_{2s,q}| \asymp q^{\frac{1}{4}} 2^{r_d} \binom{q}{2s}^{-\frac{1}{2}}$ .

**Доказательство** повторяет доказательство Теоремы 9.2.2. Следует при этом заметить, что двоичный БЧХ-код  $BCH(B_A^{(d)})$  содержит только векторы четного веса, т.е.  $d$  — четное число. Поэтому для размерности  $r_d = 1 + l \cdot (d - 2 - \lfloor \frac{d-2}{2} \rfloor) = 1 + l \cdot \frac{d-2}{2}$  ортогонального к нему кода  $BCH^\perp(B_A^{(d)})$  (см. (5.2.16)) выполнено соотношение (9.2.19) выполнено для всех  $s$ , начиная с  $s = d$  и кончая  $s = q - d$ .  $\square$

Заметим, что Следствие 9.2.1 при  $d = \text{const}$  позволяет получить асимптотическое представление элементов спектра (9.2.20) для всех  $t$ ,  $0 < t < q$ , для которых  $\eta_t \neq 0$ . В случае же  $p > 2$  этого мы утверждать не можем. А именно, существуют значения  $t$ , в частности,  $t = d$ , для которых асимптотического представления элемента спектра  $\eta_t$  Теорема 9.2.2 не дает.

Асимптотическое представления элементов двоичного БЧХ-кода было впервые получено в работе автора [24] в 1971 г.

**Замечание 9.2.1** Распределение числа векторов веса  $s$  БЧХ-кода из Теоремы 9.2.2 при малых  $s$  заметно отличается от биномиального распределения, т.е. от распределения вида  $\eta_s \approx p^{-r_d} (p-1)^s \binom{q}{s}$ . Видимо, этот не совсем очевидный факт связан с тем, что проверочная матрица рассматриваемого БЧХ-кода содержит строку, состоящую только из единиц.

Если рассмотреть в качестве БЧХ-кода  $p$ -значный код длины  $q$  с проверочной матрицей вида (5.1.5), который не содержит векторов веса  $q$ , то, как нетрудно показать, этот код в условиях Теоремы 9.2.2 имеет распределение числа векторов веса  $s$  при достаточно больших  $s$  близкое к биномиальному:  $\eta_s \approx p^{-r_d} (p-1)^s \binom{q}{s}$ .

**Замечание 9.2.2** Теорему 9.2.2 и Следствие 9.2.1 достаточно легко обобщить на случай  $d \rightarrow \infty$  при  $q \rightarrow \infty$ . Для этого надо выяснить "взаимоотношения" параметров  $d, s, q$ , при которых  $|\varepsilon_{s,q}| \rightarrow 0$  (см. (9.2.18)) при  $q \rightarrow \infty$ . В настоящей работе мы этого делать не будем.



# Глава 10

## Схемы отношений

### 10.0.1 Введение

Схемы отношений (соответствующий английский термин — noncommutative association scheme или просто association scheme) является предметом исследований науки, которая носит название алгебраическая комбинаторика. Алгебраическая комбинаторика (см., например, [61]) помимо схем отношений включает в себя комбинаторные дизайны (combinatorial designs), а также изучает и некоторые другие математические конструкции, в частности, дистанционно-регулярные графы [61]. Без сомнения, схемы отношений являются родственной с теорией кодирования областью исследований и методы, разработанные в теории схем отношений, используются в теории кодирования. В частности, алгебры Боуза-Меснера ассоциативной схемы находят применение при одном из вариантов вывода оценок числа элементов кода с заданным кодовым расстоянием. Имеются и другие применения схем отношений в теории кодирования, о которых будет сказано ниже. Схемы отношений находят также применения в криптографии.

**Определение 10.0.1** [10] *Схема отношений  $\mathcal{S} = \mathcal{S}(X, R_0, \dots, R_m)$  (другое название — некоммутативная ассоциативная схема) на конечном множестве  $X$  с  $m+1$  классами — это разбиение множества пар  $X \times X$  на  $m+1$  подмножеств  $R_0, \dots, R_m$  (называемых отношениями), которое имеет следующие свойства:*

- i  $R_0 = \{(x, x) | x \in X\}$ .
- ii Пусть  $(x, y) \in X \times X$ . Число  $r_{i,j}(x, y)$  пар ребер  $(x, z), (z, y)$  таких, что  $(x, z) \in R_i, (z, y) \in R_j$  одинаково для всех  $(x, y) \in R_k$ , т.е. число  $r_{i,j}(x, y) = r_{i,j}^k$  определяется только отношением  $R_k$ , к которому принадлежит ребро  $(x, y)$ .
- iii Взаимное отношение  $R_j^T = \{(y, x) | (x, y) \in R_j\}$  является одним из отношений множества  $R_0, \dots, R_m$ , т.е.  $R_j^T = R_{j'}$  для некоторого  $j'$ .

Элементы множества  $X$  обычно называют вершинами, а элементы множества пар  $X \times X$  — ребрами схемы  $\mathcal{S}$ . Очень часто в качестве  $X$  рассматривается конечная группа или конечное кольцо, т.е. на множестве  $X$  определены одна или две алгебраические операции.

Если для схемы отношений  $\mathcal{S}$  в добавление к пп. i., ii., iii. выполнено свойство iv :  $r_{i,j}^k = r_{j,i}^k$ , то схема  $\mathcal{S}$  называется ассоциативной схемой.

Если для схемы отношений  $\mathcal{S}$  в добавление к пп. **i.,ii.,iii.** выполнено свойство **v** :  $R_j^T = R_j$ , т.е.  $j = j'$ , то схема  $\mathcal{S}$  называется симметричной схемой отношений.

Число  $r_{s,s}^0 = v_s$  называется валентностью отношения  $R_s$ . По определению, оно равно числу ребер  $(x, y) \in X \times X$  с фиксированной вершиной  $x \in X$ , которые принадлежат отношению  $R_s$ . Для схем отношений  $\mathcal{S}_H(\mathfrak{G})$ , которые мы будем рассматривать ниже,  $v_s$  — это также число элементов в классе сопряженных элементов  $C_s$ .

**Пример 10.0.1** Простейшей схемой отношений является схема  $\mathcal{S}$  с двумя классами  $R_0$  и  $R_1$  ( $m = 1$ ), у которой

$$R_0 = \{(a, a) | a \in X\}, \quad R_1 = \{(a, b) | a, b \in X, b \neq a\} = X \times X \setminus R_0. \quad (10.0.1)$$

**Пример 10.0.2** Наиболее известной является двоичная симметричная ассоциативная схема Хэмминга  $\mathcal{H}_2^n$  с  $m+1 = n+1$  классами отношений, у которой множеством  $X = F^n$ ,  $|F| = 2$ , является множеством всех  $n$ -мерных двоичных векторов с координатами из конечного поля  $\mathbb{F}_2$  ( $n$ -мерное двоичное пространство). Отношение (множество пар)  $R_j$  состоит из всех пар векторов  $(\mathbf{x}, \mathbf{y})$ ,  $\mathbf{x}, \mathbf{y} \in F_2^n$ , расстояние Хэмминга  $d(\mathbf{x}, \mathbf{y})$  между которыми равно  $j$ .

Если  $d(\mathbf{x}, \mathbf{y}) = k$  и  $i + j - k$  — четное неотрицательное число, то, как нетрудно вычислить (Упражнение),

$$r_{i,j}(\mathbf{x}, \mathbf{y}) = r_{i,j}^k = \binom{n-k}{r} \binom{k}{k-j+r} = \binom{n-k}{r} \binom{k}{j-r}, \quad \text{где } r = \frac{i+j-k}{2}. \quad (10.0.2)$$

Если же  $d(\mathbf{x}, \mathbf{y}) = k$  и  $i + j - k$  — нечетное или отрицательное число, то  $r_{i,j}(\mathbf{x}, \mathbf{y}) = 0$ .

Очевидно, взаимное отношение  $R_j^T$  в данном примере совпадает с отношением  $R_j$ .

Обобщением схемы отношений  $\mathcal{H}_2^n$  является схема отношений  $\mathcal{H}_q^n$ , у которой  $X = F^n$ ,  $|F| = q \geq 2$ , является  $n$ -мерным двоичным векторным пространством над конечным полем  $\mathbb{F}_q$  или некоторым кольцом с  $q$  элементами.

**Пример 10.0.3** В данном примере множество  $X = \{0, 1, \dots, 6\}$  образовано наименьшими неотрицательными вычетами по  $\text{mod } 7$ . Схема отношений  $\mathcal{S}$  имеет три класса отношений ( $m = 2$ ):

$$R_0 = \{(a, a) | a \in X\}, \quad R_+ = \{(a, b) | b - a \in \{1, 2, 4\}\}, \quad R_- = \{(a, b) | b - a \in \{3, 5, 6\}\}. \quad (10.0.3)$$

(Упражнение)

Взаимным к отношению  $R_+$  является отношение  $R_-$ , а взаимным к отношению  $R_-$  — отношение  $R_+$ , т.е. эта схема не является симметричной. (Упражнение)

Как нетрудно увидеть, к отношению  $R_+$  принадлежат все пары  $(a, b)$ , для которых  $\left(\frac{b-a}{7}\right) = 1$ , а к отношению  $R_-$  все пары, для которых  $\left(\frac{b-a}{7}\right) = -1$ , где  $\left(\frac{a}{p}\right)$ , — символ Лежандра элемента  $a$ ,  $a \neq 0$ , поля вычетов по  $\text{mod } p$ , который определяется следующим образом:  $\left(\frac{a}{p}\right) = 1$ , если в поле вычетов по  $\text{mod } p$  найдется такое  $x$ , что  $a \equiv x^2$ , и  $\left(\frac{a}{p}\right) = -1$ , если такого  $x$  не существует.

В следующих разделах мы будем изучать схемы отношений, частным случаем которых является схема отношений примера 10.0.3.



## 10.1 Построение схем отношений

Пусть  $\mathfrak{G}$  — конечная группа и  $\Gamma$  — ее точное представление в унитарном пространстве  $\mathbb{C}^f$ . Другими словами,  $\Gamma = \{\Gamma(\mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$  — множество унитарных матриц (см. раздел 1.2.2), которые являются изоморфными образами элементов группы  $\mathfrak{G}$ , так что

$$\Gamma(\mathfrak{g})\Gamma(\mathfrak{g}') = \Gamma(\mathfrak{h}), \text{ если } \mathfrak{g}\mathfrak{g}' = \mathfrak{h}. \quad (10.1.1)$$

Как известно, автоморфизм  $\sigma$  группы  $\mathfrak{G}$  это отображение  $\mathfrak{G}$  в себя, которая обладает следующим свойством

$$\mathfrak{g}^\sigma \mathfrak{g}'^\sigma = (\mathfrak{g}\mathfrak{g}')^\sigma, \quad (10.1.2)$$

где через  $\mathfrak{g}^\sigma$  обозначено действие автоморфизма  $\sigma$  на элемент  $\mathfrak{g}$ .

Очевидно, суперпозиция двух автоморфизмов снова автоморфизм группы  $\mathfrak{G}$ . Поэтому множество всех автоморфизмов  $Aut(\mathfrak{G})$  является группой, в которой групповой операцией является суперпозиция автоморфизмов.

Мы будем обозначать через  $H = \{\sigma_0, \dots, \sigma_t\}$  подгруппу группы  $Aut(\mathfrak{G})$ .

Пусть  $\mathfrak{h} \in \mathfrak{G}$ . Обозначим через  $C_{\mathfrak{h}}^H$  множество элементов группы  $\mathfrak{G}$  вида  $C_{\mathfrak{h}}^H = \{\mathfrak{h}^\sigma | \sigma \in H\}$ . Множество  $C_{\mathfrak{h}}^H$ , очевидно, является орбитой действия на  $\mathfrak{h} \in \mathfrak{G}$  элементов подгруппы  $H$  (орбитой  $H$  с представителем  $\mathfrak{h}$ ) и носит название класс сопряженных элементов относительно подгруппы  $H$  с представителем  $\mathfrak{h}$ . Отметим, что орбита  $C_{\mathfrak{e}}^H$  ( $\mathfrak{e}$  — единица группы  $\mathfrak{G}$ ) состоит из одного элемента  $\mathfrak{e}$ . Кроме того заметим, что если  $\mathfrak{h}' \notin C_{\mathfrak{h}}^H$ , то  $C_{\mathfrak{h}}^H \cap C_{\mathfrak{h}'}^H = \emptyset$ .

Таким образом, группа  $\mathfrak{G}$  разбивается на  $1 + m$  классов сопряженных элементов:

$$\mathfrak{G} = \bigcup_{j=0}^m C_j^H, \quad (10.1.3)$$

где  $C_j^H = C_{\mathfrak{h}_j}^H$ ,  $j = 0, \dots, m$ , — различные классы сопряженных элементов относительно подгруппы  $H$  и  $\mathfrak{h}_j$  — представитель  $C_j^H$ .

Индекс  $H$  в обозначении  $C_j^H$  будем опускать. Это не должно привести к недоразумениям.

### 10.1.1 Схемы отношений $\mathcal{S}_H(\mathfrak{G})$

С подгруппой  $H \subseteq Aut(\mathfrak{G})$  естественно связать схему  $\mathcal{S}_H(\mathfrak{G})$ , которая, как будет показано ниже, является схемой отношений (см. определение 10.0.1).

**Определение 10.1.1 (схемы  $\mathcal{S}_H(\mathfrak{G})$ )** .

Множество вершин  $X$  схемы  $\mathcal{S}_H(\mathfrak{G})$  образуют элементы группы  $\mathfrak{G}$ , т.е.  $X = \mathfrak{G}$ .

Множество пар  $\mathfrak{G} \times \mathfrak{G}$  разбивается на классы отношений  $R_j$ ,  $j = 0, \dots, m$  ( $\mathfrak{G} \times \mathfrak{G} = \bigcup_{j=0}^m R_j$ ) следующим образом

$$R_j = \{(\mathfrak{g}, \mathfrak{h}\mathfrak{g}) | \mathfrak{h} \in C_j, \mathfrak{g} \in \mathfrak{G}\}. \quad (10.1.4)$$

Таким образом,  $R_j$  состоит из ребер  $(\mathfrak{g}, \mathfrak{g}')$ , для которых  $\mathfrak{g}'\mathfrak{g}^{-1} \in C_j$ . Очевидно,  $|R_j| = |G||C_j|$ . Мы полагаем, что представителем класса  $R_j$  является ребро  $(\mathfrak{e}, \mathfrak{h}_j)$ , где  $\mathfrak{h}_j$  — представитель класса сопряженных элементов  $C_j$ .

Если из контекста ясно о какой группе  $\mathfrak{G}$  идет речь, используем для  $\mathcal{S}_H(\mathfrak{G})$  более короткое обозначение  $\mathcal{S}_H$ .

### Теорема 10.1.1 .

- i Схema  $\mathcal{S}_H(\mathfrak{G})$  является некоммутативной ассоциативной схемой (схемой отношений).
- ii Если ребра  $(\mathfrak{g}, \mathfrak{g}')$  и  $(\mathfrak{g}'^{-1}, \mathfrak{g}^{-1})$  всегда принадлежат одному и тому же классу отношений, то  $\mathcal{S}_H(\mathfrak{G})$  является ассоциативной схемой.
- iii Взаимное отношение  $R_j^T = R_{j'}$  схемы  $\mathcal{S}_H(\mathfrak{G})$  определяется классом сопряженных элементов  $C_{j'}$  с представителем  $\mathfrak{h}_{j'} = \mathfrak{h}_j^{-1}$ .

**Доказательство.** (п. i.) Нам нужно показать, что число  $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$  тех  $\mathfrak{h} \in \mathfrak{G}$ , для которых  $(\mathfrak{g}, \mathfrak{h}) \in R_j$ ,  $(\mathfrak{h}, \mathfrak{g}') \in R_i$  одинаково для всех  $(\mathfrak{g}, \mathfrak{g}') \in R_k$ , т.е. число  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}^k$  определяется только классом  $R_k$ , к которому принадлежит ребро  $(\mathfrak{g}, \mathfrak{g}')$ .

Если  $(\mathfrak{g}, \mathfrak{h}) \in R_j$ ,  $(\mathfrak{h}, \mathfrak{g}') \in R_i$ , то  $(\mathfrak{g}\mathfrak{h}', \mathfrak{h}\mathfrak{h}') \in R_j$ ,  $(\mathfrak{h}\mathfrak{h}', \mathfrak{g}'\mathfrak{h}') \in R_i$  при любом  $\mathfrak{h}' \in \mathfrak{G}$ . Поэтому числа  $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$  и  $r_{i,j}(\mathfrak{g}\mathfrak{h}', \mathfrak{g}'\mathfrak{h}')$  равны при любом  $\mathfrak{h}' \in \mathfrak{G}$ . Отсюда вытекает, что  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1})$ , если положить  $\mathfrak{h}' = \mathfrak{g}^{-1}$ .

Очевидно,  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{g}^\sigma, \mathfrak{g}'^\sigma)$  для любого  $\sigma \in H$ . Если  $\mathfrak{h}_k$  — представитель класса сопряженных элементов  $C_k$  и  $(\mathfrak{g}, \mathfrak{g}') \in R_k$ , то найдется такое  $\sigma \in H$ , что  $(\mathfrak{g}'\mathfrak{g}^{-1})^\sigma = \mathfrak{h}_k$ . Поэтому  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{i,j}(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1}) = r_{i,j}(\mathfrak{e}, \mathfrak{h}_k)$ , т.е. число  $r_{i,j}(\mathfrak{g}, \mathfrak{g}')$  определяется только классом отношений  $R_k$ , к которому принадлежит ребро  $(\mathfrak{g}, \mathfrak{g}')$ .

Для того, чтобы завершить доказательство п.i. достаточно показать, что каждое взаимное отношение также принадлежит схеме  $\mathcal{S}_H(\mathfrak{G})$ . Это вытекает из п.iii. леммы.

(п. ii.) Нам нужно показать, что если ребра  $(\mathfrak{g}, \mathfrak{g}')$  и  $(\mathfrak{g}'^{-1}, \mathfrak{g}^{-1})$  всегда принадлежат одному и тому же классу отношений, то  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{j,i}(\mathfrak{g}, \mathfrak{g}')$  для всех  $(\mathfrak{g}, \mathfrak{g}') \in \mathfrak{G} \times \mathfrak{G}$ .

Пусть  $(\mathfrak{e}, \mathfrak{h}) \in R_i$  и  $(\mathfrak{h}, \mathfrak{h}_k) \in R_j$ . Тогда  $(\mathfrak{e}, \mathfrak{h}_k\mathfrak{h}^{-1}) \in R_j$ . Покажем, что если выполнено условие в п. ii., то  $(\mathfrak{h}_k\mathfrak{h}^{-1}, \mathfrak{h}_k) \in R_i$ . Действительно, по условию ii. леммы, ребро  $(\mathfrak{h}_k^{-1}, (\mathfrak{h}_k\mathfrak{h}^{-1})^{-1})$  и ребро  $(\mathfrak{e}, \mathfrak{h})$  лежат в одном и том же классе отношений  $R_i$ . Отсюда следует требуемое.

Таким образом, взаимно однозначное соответствие  $\mathfrak{h} \longrightarrow \mathfrak{h}_k\mathfrak{h}^{-1}$  переставляют классы  $R_i$  и  $R_j$  во включениях  $(\mathfrak{e}, \mathfrak{h}) \in R_i$  и  $(\mathfrak{h}, \mathfrak{h}_k) \in R_j$ . Отсюда вытекает, что  $r_{i,j}(\mathfrak{g}, \mathfrak{g}') = r_{j,i}(\mathfrak{g}, \mathfrak{g}')$ .

(п. iii.) Множество  $\{(\mathfrak{h}\mathfrak{g}, \mathfrak{g}) | \mathfrak{h} \in C_j, \mathfrak{g} \in \mathfrak{G}\}$ , как нетрудно проверить, совпадает с классом отношений  $R_{j'} = \{(\mathfrak{g}, \mathfrak{h}\mathfrak{g}) | \mathfrak{g} \in C_{j'}, \mathfrak{g} \in \mathfrak{G}\}$ , определяемым классом сопряженных элементов  $C_{j'}$  с представителем  $\mathfrak{h}_{j'}^{-1}$ , где  $\mathfrak{h}_j$  — представитель класса  $C_j$ . Поэтому свойство iii. для схемы  $\mathcal{S}_H(\mathfrak{G})$  всегда выполнено.  $\square$

Упражнение. Показать, что  $\mathcal{S}_H$  является ассоциативной схемой в том случае, когда  $\mathfrak{G}$  — абелева группа, или  $H$  — группа внутренних автоморфизмов.

Упражнение. Ассоциативная схема  $\mathcal{S}_H$  является симметричной схемой отношений (ассоциативной схемой с дополнительным свойством:  $j = j'$ ), если для всех  $\mathfrak{g}, \mathfrak{g}' \in \mathfrak{G}$  элементы  $\mathfrak{g}, \mathfrak{g}^{-1}$  принадлежат одному и тому же классу сопряженных элементов группы  $\mathfrak{G}$ .

Следует отметить, что определение 10.0.1 восходит к определению работ [55], [57] и [73], в которых рассматривались ассоциативные схемы с орбитами  $R_j = \{(x^\sigma, y^\sigma) | \sigma \in \tilde{H}\}$ , играющими роль классов  $R_j$ , где  $\tilde{H}$  — группа

подстановочных автоморфизмов множества  $X$  и  $(x, y) \in X \times X$ . Наша ассоциативная схема  $\mathcal{S}_H(\mathfrak{G})$  является специальным случаем этого понятия, так как мы можем взять группу  $\mathfrak{G}$  в качестве  $X$  и полупрямое произведение  $H$  с  $\mathfrak{G}$  в качестве  $\tilde{H}$  (Замечание А. Мунемаса [68]).

Схема  $\mathcal{S}_H(\mathfrak{G})$  с абелевой группой  $\mathfrak{G}$  у которой  $H$  состоит из одного тривиального автоморфизма называют схемой Гекке (Hescke). Они были рассмотрены в работе [71].

## 10.1.2 Примеры

Предварительно рассмотрим два примера ассоциативных схем  $\mathcal{S}_H$ , изучение которых будет продолжено в разделе 10.4.1.

**Пример 10.1.1**  $\mathfrak{G} = (\mathbb{F}_p, +)$  — аддитивная группа конечного простого поля  $\mathbb{F}_p$ .

Группа  $\text{Aut}(\mathfrak{G})$  внешних автоморфизмов группы  $(\mathbb{F}_p, +)$  образована всеми отображениями  $\sigma_a : x \rightarrow ax$ ,  $a \in \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ . Очевидно,  $|\text{Aut}(\mathfrak{G})| = p - 1$ .

Подгруппа  $\Phi_d^{(p)} = \Phi_d$ ,  $d|p-1$ , группы  $\text{Aut}(\mathfrak{G})$  образованы отображениями  $\sigma_a$ , у которых  $a$  принадлежит подгруппе  $\mathbb{F}_{p,d}^*$  порядка  $d$  мультипликативной группы  $\mathbb{F}_p^*$  поля  $\mathbb{F}_p$ . Другими словами,  $\sigma_a \in \Phi_d$ , если элемент  $a$  представим в виде  $a = y^{\frac{p-1}{d}}$ ,  $y \in \mathbb{F}_p^*$ .

Представления  $\Gamma_a$  группы  $\mathfrak{G}$ , которые мы будем рассматривать в данном примере, образованы одномерными матрицами  $\|\exp\left(\frac{2\pi i ax}{p}\right)\|$ ,  $a \in \mathbb{F}_p^*$ . Таким образом, элементу  $x \in \mathbb{F}_p$  мы сопоставляем одномерную матрицу  $\Gamma_a(x) = \|\exp\left(\frac{2\pi i ax}{p}\right)\|$ .

Отметим, что групповой операцией в  $\mathbb{F}_p$  является сложение, в то время как групповой операцией в  $\Gamma_a$  является умножение матриц. Таким образом,  $\Gamma_a(x)\Gamma_a(y) = \|\exp\left(\frac{2\pi i ax}{p}\right)\| \cdot \|\exp\left(\frac{2\pi i ay}{p}\right)\| = \|\exp\left(\frac{2\pi i a(x+y)}{p}\right)\| = \Gamma_a(x+y)$  так, что отображение  $x \rightarrow \exp\left(\frac{2\pi i ax}{p}\right)$  действительно является точным представлением аддитивной группы  $\mathbb{F}_p$ . Функцию  $\exp\left(\frac{2\pi i ax}{p}\right)$  обычно называют характером группы  $\mathbb{F}_p$ .

Подгруппа автоморфизмов  $\Phi_d$  разбивает  $\mathfrak{G}$  на  $d' + 1 = 1 + \frac{p-1}{d}$  классов сопряженных элементов  $C_0, C_1, \dots, C_{d'}$ ,  $C_0 = \{0\}$ ,  $C_j = \{\tau^j x^{\frac{p-1}{d}} | x \in \mathbb{F}_p^*\}$ ,  $j = 1, \dots, d'$ ,  $dd' = p - 1$ , где  $\tau$  — первообразный элемент группы  $\mathbb{F}_p^*$ .

Классы  $R_j$  в соответствии с определением 10.1.1 имеют вид  $R_j = \{(\mathfrak{g}, \mathfrak{h} + \mathfrak{g}) | \mathfrak{h} \in C_j, \mathfrak{g} \in \mathbb{F}_p\}$ . (Напомним, что групповой операцией в данном случае в отличие от определения 10.1.1 является сложение).

Как следует из теоремы 10.1.1 (п. ii.) схема  $\mathcal{S}_{\Phi_d}$  является симметричной ассоциативной схемой тогда и только тогда, когда  $-1 \in \mathbb{F}_{p,d}^*$ . Её обычно называют циклотомической схемой на  $(\mathbb{F}_p, +)$  (см. [72], [45], стр. 66).

Если  $d = p - 1$ , то разбиение  $\mathfrak{G} \times \mathfrak{G}$  имеет вид  $\mathfrak{G} \times \mathfrak{G} = R_0 \cup R_1$ , где  $R_0 = \{(\mathfrak{g}, \mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$  и  $R_1 = \{(\mathfrak{g}, \mathfrak{h} + \mathfrak{g}) | \mathfrak{g} \in \mathbb{F}_p, \mathfrak{h} \in \mathbb{F}_p^*\}$ , ибо  $C_0 = \{0\}$ ,  $C_1 = \mathbb{F}_p^*$ . Подобную схему называют элементарной схемой отношений или схемой Хэмминга.

Если  $d = \frac{p-1}{2}$ , то  $\mathfrak{G} \times \mathfrak{G} = R_0 \cup R_+ \cup R_-$ , где  $R_0 = \{(\mathfrak{g}, \mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$  и  $R_+ = \{(\mathfrak{g}, \mathfrak{h} + \mathfrak{g}) | \mathfrak{g} \in \mathbb{F}_p, \mathfrak{h} \in \mathbb{F}_p^*, \left(\frac{\mathfrak{h}}{p}\right) = 1\}$ ,  $R_- = \{(\mathfrak{g}, \mathfrak{h} + \mathfrak{g}) | \mathfrak{g} \in \mathbb{F}_p, \mathfrak{h} \in \mathbb{F}_p^*, \left(\frac{\mathfrak{h}}{p}\right) = -1\}$ , где  $\left(\frac{\mathfrak{h}}{p}\right)$  — символ Лежандра.

В разделе 10.1.1 мы подробно рассмотрим случай, в котором  $\mathfrak{G}$  — аддитивная группа конечного поля  $\mathbb{F}_q$ ,  $q = p^l$ . При  $l > 1$  этот случай несколько сложнее, рассматриваемого случая, в частности, из-за того, что аддитивная группа простого поля  $\mathbb{F}_q$  имеет автоморфизмы, отличные от  $\sigma_a : x \rightarrow ax$ ,  $a \in \mathbb{F}_q^*$ .

**Пример 10.1.2** Пусть  $\mathfrak{G}$  — конечная группа,  $H = \text{Inn}(\mathfrak{G})$  — группа ее внутренних автоморфизмов, т.е. автоморфизмов вида  $g \rightarrow h^{-1}gh$ ,  $h \in \mathfrak{G}$ . В этом случае возникает известная схема отношений  $\mathcal{S}_H(\mathfrak{G})$  (см. [57]).

**Замечание 10.1.1** Можно установить (математический фольклор), что группа  $\mathfrak{G}$  может иметь два класса сопряженных элементов относительно группы  $\text{Aut}(\mathfrak{G})$  всех ее автоморфизмов только в том случае, когда она является элементарной абелевой группой. Все другие группы  $\mathfrak{G}$  распадаются на три или более класса сопряженных элементов. Этот не совсем очевидный факт сообщил автору Л.С. Казарин [1].

Схемы  $\mathcal{C}_H(\mathfrak{G})$ , которые имеют два класса отношений, естественно называть элементарными. Они всегда являются ассоциативными схемами. Схема  $\mathcal{C}_H(\mathfrak{G}^n)$ , построенная с помощью такой координатной схемы  $\mathcal{C}_H(\mathfrak{G})$  (см. раздел 10.2), известна [73] как ассоциативная схема Хэмминга  $\mathcal{H}_{|\mathfrak{G}|}^n$ .

Интересно отметить, что если  $\mathfrak{G} = (\mathbb{F}_{p^l}, +)$  — аддитивная группа простого поля, то существует несколько различных неизоморфных подгрупп  $H < \text{Aut}((\mathbb{F}_{p^l}, +))$ , для которых схема  $\mathcal{S}_H(\mathfrak{G})$  имеет два класса отношений.

## 10.2 Схемы отношений на $\mathfrak{G}^n$ .

Мы определили схему отношений  $\mathcal{S}_H(\mathfrak{G})$  на группе  $\mathfrak{G}$ . Теперь мы хотим определить схему отношений на группе  $\mathfrak{G}^n = \mathfrak{G} \times \dots \times \mathfrak{G}$ , используя для этого схему  $\mathcal{S}_H(\mathfrak{G})$  с  $1 + n$  отношениями  $R_j$ . Это можно сделать разными способами. Та схема  $\mathcal{S}_H(\mathfrak{G}^n)$ , которую мы определим ниже, является обобщением схемы отношений Хэмминга  $\mathcal{H}_2^n$  (см. Пример 10.0.2) и имеет родственные черты с метрикой на  $\mathfrak{G}^n$ . Сначала полезно привести некоторые наводящие соображения.

Как вводится метрика в  $n$ -мерном метрическом пространстве, например, в  $n$ -мерном евклидовом пространстве, или в  $n$ -мерном пространстве Хэмминга? Сначала мы определяем метрику  $\lambda$  одномерном координатном пространстве. Затем с помощью метрики  $\lambda$  мы определяем расстояние между векторами  $\mathbf{x} = (x_1, \dots, x_n)$  и  $\mathbf{y} = (y_1, \dots, y_n)$ , комбинируя расстояния между отдельными координатами  $\mathbf{x}$  и  $\mathbf{y}$ . Для евклидовой метрики это расстояние определяется соотношением

$$\lambda(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{j=1}^n \lambda^2(x_j, y_j)}, \quad (10.2.1)$$

а для метрики Хэмминга — с помощью соотношения

$$\lambda(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n \lambda(x_j, y_j) = d, \quad (10.2.2)$$

где в данном случае  $\lambda$  — метрика Хемминга и  $d$  — число различных координат у векторов  $\mathbf{x}$  и  $\mathbf{y}$ . Последнее соотношение в (10.2.2), в конечном итоге, и определяет схему отношений Хемминга  $\mathcal{H}_2^n: (\mathbf{x}, \mathbf{y}) \in R_d$ , если  $\lambda(\mathbf{x}, \mathbf{y}) = d$ .

Очень существенно, что любая естественная метрика на  $\mathfrak{G}^n$  инвариантна относительно одновременной перестановки координат векторов  $\mathbf{x}, \mathbf{y}$ . В конечном итоге мы хотим определить схему отношений на  $\mathfrak{G}^n$ , которая инвариантна относительно перестановки координат векторов, а затем определить на  $\mathfrak{G}^n$  с помощью этой схемы, так называемую, дистанционно-регулярную метрику, которая наследует свойство ii. в определении схемы отношений. Отметим, что как евклидова метрика, так и метрика Хемминга являются дистанционно-регулярными.

Пусть  $\mathcal{S}_H(\mathfrak{G})$  — схема с  $1+m$  отношениями  $R_j$ , определенная группой автоморфизмов  $H$ . Мы полагаем, что на  $\mathfrak{G}^n$  покоординатно независимо действуют элементы группы  $H^n$ . Таким образом, группа  $H^n$  состоит из всех отображений

$$(x_1, \dots, x_n) \rightarrow (x_1^{\sigma_1}, \dots, x_n^{\sigma_n}), \quad \sigma_j \in H. \quad (10.2.3)$$

По определению, в класс сопряженных элементов  $C_j$ , где  $\mathbf{j} = (j_1, \dots, j_n)$ ,  $j_s \in \{0, \dots, m\}$ , входят все векторы  $\mathbf{g} = (\mathbf{g}_1, \dots, \mathbf{g}_n)$ , у которых  $\mathbf{g}_s \in C_{j_s}$ .

#### Определение 10.2.1 (Определение схемы $\mathcal{S}_{H^n}(\mathfrak{G}^n)$ ) .

Множеством вершин  $X$  схемы  $\mathcal{S}_{H^n}(\mathfrak{G}^n)$  являются элементы группы  $\mathfrak{G}^n$ .

Множество  $\mathfrak{G}^n \times \mathfrak{G}^n$  разбивается на  $(1+m)^n$  классов  $\{R_j | \mathbf{j} = (j_1, \dots, j_n); 0 \leq j_s \leq m\}$ , где  $(\mathbf{g}, \mathbf{g}') \in R_j$ , если  $\mathbf{g}'\mathbf{g}^{-1} \in C_j$ .

Схему  $\mathcal{S}_{H^n}(\mathfrak{G}^n)$  естественно назвать  $n$ -ой степенью схемы  $\mathcal{S}_H(\mathfrak{G})$ .

Из теоремы 10.1.1 непосредственно вытекает

**Теорема 10.2.1** *Схема  $\mathcal{S}_{H^n}(\mathfrak{G}^n)$  является схемой отношений.*

Композиционная схема отношений  $\mathcal{C}_H(\mathfrak{G}^n)$ , определенная ниже, получается из  $\mathcal{S}_{H^n}(\mathfrak{G}^n)$  путем объединения некоторых ее классов  $R_j$ . При  $n=1$  схемы  $\mathcal{C}_H(\mathfrak{G}^n)$  и  $\mathcal{S}_{H^n}(\mathfrak{G}^n)$  совпадают.

Число  $c_j(\mathbf{g})$  определим как число координат  $\mathbf{g}_s$  у вектора  $\mathbf{g} = (\mathbf{g}_1, \dots, \mathbf{g}_n)$  таких, что  $\mathbf{g}_s \in C_j$ . Вектор  $\mathbf{c}(\mathbf{g}) = (c_0(\mathbf{g}), \dots, c_m(\mathbf{g}))$ , где  $1+m$  — число классов сопряженных элементов в  $G$  относительно группы автоморфизмов  $H$ , назовем композицией вектора  $\mathbf{g}$ .

#### Определение 10.2.2 (Определение композиционной схемы $\mathcal{C}_H(\mathfrak{G}^n)$ ) .

Множество вершин  $X_n$  схемы  $\mathcal{C}_H(\mathfrak{G}^n)$  образуют элементы группы  $\mathfrak{G}^n$ .

Множество  $\mathfrak{G}^n \times \mathfrak{G}^n$  разбивается на классы  $\{R_{\mathbf{c}} | \mathbf{c} = (c_0, \dots, c_m); c_0 + \dots + c_n = n\}$ , где  $(\mathbf{g}, \mathbf{g}') \in R_{\mathbf{c}}$ , если  $\mathbf{c}(\mathbf{g}'\mathbf{g}^{-1}) = \mathbf{c}$ .

Таким образом, мы относим к одному классу  $R_{\mathbf{c}}$  все ребра  $(\mathbf{g}, \mathbf{g}')$  с одинаковыми композициями  $\mathbf{c}(\mathbf{g}'\mathbf{g}^{-1}) = \mathbf{c}$ . Как уже отмечалось,  $\mathcal{C}_H(\mathfrak{G}) = \mathcal{S}_H(\mathfrak{G})$ .

Схема  $\mathcal{C}_H(\mathfrak{G}^n)$  впервые была рассмотрена в работе [72]. В работе [71] (р. 1506) она введена иным по сравнению с определением 10.2.2 способом. Там же предложено называть ее расширением Дельсартра схемы  $\mathcal{C}_H(\mathfrak{G})$ .

Непосредственно доказать, что схема  $C_H(\mathfrak{G}^n)$  является схемой отношений достаточно сложно. Вместе с тем, если расширить группу автоморфизмов  $H^n$ , действующую на  $\mathfrak{G}^n$  так, чтобы классы сопряженных элементов относительно этой расширенной группы совпали с множеством векторов с фиксированной композицией  $\mathbf{c}$ , то теорема 10.1.1 позволяет непосредственно доказать требуемое свойство схемы  $C_H(\mathfrak{G}^n)$ .

### Определение 10.2.3 (Другое определение схемы $C_H(\mathfrak{G}^n)$ )

Пусть  $\tau = (i_1, \dots, i_n)$  — перестановка символов  $\{1, \dots, n\}$  и  $\sigma = (\sigma_1, \dots, \sigma_n)$  — автоморфизм (10.2.3) группы  $\mathfrak{G}^n$ . На группе  $\mathfrak{G}^n$  рассмотрим группу  $H^n \wr S_n$  автоморфизмов, образованных отображениями вида

$$(\sigma, \tau) : \mathbf{g} = (\mathbf{g}_1, \dots, \mathbf{g}_n) \rightarrow (\mathbf{g}_{i_1}^{\sigma_1}, \dots, \mathbf{g}_{i_n}^{\sigma_n}), \quad \sigma \in H^n, \tau \in S_n. \quad (10.2.4)$$

Схему отношений  $\mathcal{S}_{H^n \wr S_n}(\mathfrak{G}^n)$  определим в соответствии с определением 10.1.1.

Как нетрудно увидеть, схема отношений  $\mathcal{S}_{H^n \wr S_n}(\mathfrak{G}^n)$  совпадает с композиционной схемой отношений  $C_H(\mathfrak{G}^n)$ . Отсюда и из теоремы 10.1.1 следует

**Теорема 10.2.2** *Композиционная схема  $C_H(\mathfrak{G}^n)$  является схемой отношений.*

Пусть  $(\mathbf{g}, \mathbf{g}') \in R_{\mathbf{c}}$ . Если мы одновременно переставим координаты в паре векторов  $\mathbf{g}, \mathbf{g}' \in \mathfrak{G}^n$ , то полученная пара  $(\mathbf{h}, \mathbf{h}')$  будет также принадлежать отношению  $R_{\mathbf{c}}$ , т.е.  $C_H(\mathfrak{G}^n)$  обладает объявленным выше свойством: является схемой отношений, которая инвариантна относительно перестановки координат.

## 10.3 Алгебра Боуза-Меснера ассоциативной схемы

### 10.3.1 Некоторые сведения из теории представления конечных групп

В настоящем разделе для удобства читателя приведены начальные сведения по теории представления конечных групп, которыми мы будем пользоваться в последующих разделах. Доступное и систематическое изложение рассматриваемой теории имеется в [14] (существует более доступный ее репринт 2003 г.) и также во многих других книгах.

Мы будем рассматривать линейные представления  $\Gamma = \Gamma(\mathfrak{G})$  конечной группы  $\mathfrak{G}$  на  $f$ -мерном унитарном или евклидовом пространстве. Это означает, что задан гомоморфизм  $\varphi$  группы  $\mathfrak{G}$  в группу  $\Gamma(\mathfrak{G}) = \{\Gamma(\mathbf{g}) | \mathbf{g} \in \mathfrak{G}\}$  унитарных или ортогональных  $f \times f$ -матриц такой, что выполнены следующие соотношения

$$\varphi : \mathbf{g} \rightarrow \Gamma(\mathbf{g}) \text{ и } \Gamma(\mathbf{g})\Gamma(\mathbf{h}) = \Gamma(\mathbf{gh}) \text{ для всех } \mathbf{g}, \mathbf{h} \in \mathfrak{G}. \quad (10.3.1)$$

Представление  $\Gamma(\mathfrak{G})$  называется неприводимым, если не существует инвариантного относительно  $\Gamma(\mathfrak{G})$  подпространства  $L$  пространства  $C^f$  или  $R^f$  такого, что  $L \neq C^f$  и  $L \neq \{0\}$ . Таким образом, не существует собственного подпространства  $L$  такого, что

$L\Gamma(\mathfrak{g}) = L$  для всех  $\mathfrak{g} \in \mathfrak{G}$ . Если такое подпространство  $L$  размерности  $f'$ ,  $0 < f' < f$ , существует, то каждая унитарная матрица  $\Gamma(\mathfrak{g})$  в некотором базисе пространства  $\mathbf{C}^f$  может быть представлена в виде

$$\Gamma(\mathfrak{g}) = \begin{pmatrix} \Gamma_1(\mathfrak{g}) & 0 \\ 0 & \Gamma_2(\mathfrak{g}) \end{pmatrix}, \quad (10.3.2)$$

где  $\Gamma_1(\mathfrak{g})$  —  $f' \times f'$ –матрица, а  $\Gamma_2(\mathfrak{g})$  —  $(f - f') \times (f - f')$ –матрица. В этом случае пространство  $\mathbf{C}^f$  представляется в виде прямой суммы  $\mathbf{C}^f = L \oplus L'$ ,  $\dim L' = f - f'$ . инвариантных подпространств. В свою очередь, в этом случае говорят, что  $\Gamma$  — приводимое представление.

Пусть  $u(\mathfrak{x})$  — комплексно-значная функция, определенные на всех элементах группы  $\mathfrak{G}$ . Скалярным произведением функций  $u(\mathfrak{x})$  и  $u'(\mathfrak{x})$  мы называем число

$$\langle u(\mathfrak{x}), u'(\mathfrak{x}) \rangle = \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{g} \in \mathfrak{G}} \overline{u(\mathfrak{g})} u'(\mathfrak{g}). \quad (10.3.3)$$

Следующий факт является очень важным. Пусть  $\Gamma(\mathfrak{g}) = \|\gamma_{i,j}(\mathfrak{g})\|_{i,j=1,\dots,f}$  — матрица неприводимого представления  $\Gamma$ , отвечающая элементу  $\mathfrak{g}$ . Тогда

$$\langle \gamma_{i,j}(\mathfrak{g}), \gamma_{i',j'}(\mathfrak{g}) \rangle = \begin{cases} \frac{1}{f}, & \text{если } i, j = i', j'; \\ 0, & \text{если } i, j \neq i', j'. \end{cases} \quad (10.3.4)$$

Соотношение (10.3.4) называется соотношением ортогональности матричных элементов неприводимого представления  $\Gamma$ .

Известно, что для конечной группы  $\mathfrak{G}$  имеется  $1 + m$  различных (неэквивалентных) неприводимых представления, где  $1 + m$  — число классов сопряженных элементов группы  $\mathfrak{G}$  относительно группы ее внутренних автоморфизмов  $\text{Inn}(\mathfrak{G})$ . Эти представления мы будем обозначать символом  $\Gamma^k(\mathfrak{G})$ ,  $k = 0, \dots, m$ . Представление  $\Gamma^k(\mathfrak{G})$  действует на унитарном  $\mathbf{C}^{f_k}$  или ортогональном пространстве  $R^{f_k}$  размерности  $f_k$ . Числа  $f_k$  делят порядок  $|\mathfrak{G}|$  группы  $\mathfrak{G}$ . Также известно, что

$$f_0^2 + f_1^2 + \dots + f_m^2 = |\mathfrak{G}|. \quad (10.3.5)$$

В добавление к соотношению (10.3.4) выполнено равенство

$$\langle \gamma_{i,j}^k(\mathfrak{x}), \gamma_{i',j'}^s(\mathfrak{x}) \rangle = \begin{cases} 0, & \text{если } k \neq s; \\ \langle \gamma_{i,j}^k(\mathfrak{x}g), \gamma_{i',j'}^k(\mathfrak{x}) \rangle, & \text{если } k = s, \text{ т.е. в этом случае} \\ & \text{действует соотношение (10.3.4).} \end{cases} \quad (10.3.6)$$

Символом  $\text{tr } A$  мы обозначаем след матрицы  $A$ , т.е. сумму ее диагональных элементов. Если  $A = \Gamma(\mathfrak{g})$ , то число  $\text{tr } \Gamma(\mathfrak{g})$  называется характером элемента  $\mathfrak{g}$  в представлении  $\Gamma$  и обозначается символом  $\chi_\Gamma(\mathfrak{g})$ . Если  $\Gamma = \Gamma^k(\mathfrak{G})$ , то характер матрицы  $\text{tr } \Gamma^k(\mathfrak{g})$  обозначается символом  $\chi_k(\mathfrak{g})$ .

**Лемма 10.3.1** *Имеет место равенство*

$$\langle \chi_k(\mathfrak{x}), \chi_s(\mathfrak{g}'\mathfrak{x}) \rangle = \begin{cases} 0, & \text{если } k \neq s; \\ \frac{\chi_k(\mathfrak{g}')}{f_k}, & \text{если } k = s. \end{cases} \quad (10.3.7)$$

В частности, если  $k = s$  и  $\mathfrak{g}' = \mathfrak{e}$  (единица группы  $\mathfrak{G}$ ), то

$$\langle \chi_k(\mathfrak{x}), \chi_k(\mathfrak{x}) \rangle = 1. \quad (10.3.8)$$

**Доказательство.** Так как  $\Gamma^s(\mathfrak{g}'\mathfrak{g}) = \Gamma^s(\mathfrak{g}')\Gamma^s(\mathfrak{g})$ , то

$$\chi_s(\mathfrak{g}'\mathfrak{g}) = \text{tr } \Gamma^s(\mathfrak{g}'\mathfrak{g}) = \sum_{j=1}^{f_s} \sum_{i=1}^{f_s} \gamma_{i,j}^s(\mathfrak{g}') \gamma_{j,i}^s(\mathfrak{g}). \quad (10.3.9)$$

Отсюда и (10.3.6) следует, что если  $k \neq s$ , то  $\langle \text{tr } \Gamma^k(\mathfrak{g}), \text{tr } \Gamma^s(\mathfrak{g}'\mathfrak{g}) \rangle = 0$ . Если же  $k = s$ , то из соотношений (10.3.4) и (10.3.9) вытекает

$$\begin{aligned} \langle \chi_k(\mathfrak{x}), \chi_s(\mathfrak{g}'\mathfrak{x}) \rangle &= \langle \text{tr } \Gamma^k(\mathfrak{x}), \text{tr } \Gamma^k(\mathfrak{g}'\mathfrak{x}) \rangle = \\ &= \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{g} \in \mathfrak{G}} \left( \sum_{i=1}^{f_k} \gamma_{i,j}^k(\mathfrak{g}') \gamma_{j,i}^k(\mathfrak{g}) \right) \left( \sum_{i=1}^{f_k} \overline{\gamma_{i,i}^k(\mathfrak{g})} \right) = \frac{\text{tr } \Gamma^k(\mathfrak{g}')}{f_k} = \frac{\chi_k(\mathfrak{g}')}{f_k}. \end{aligned} \quad (10.3.10)$$

□

**Лемма 10.3.2** Если  $A \in GL(f, \mathbf{C})$  —  $f \times f$ -матрица и  $\Gamma(\mathfrak{G})$  — неприводимое представление группы  $\mathfrak{G}$ , тогда

$$\frac{1}{|\mathfrak{G}|} \sum_{v \in \Gamma(\mathfrak{G})} v A v^{-1} = \frac{\text{tr } A}{f} I_f. \quad (10.3.11)$$

Лемма является следствием известной леммы Шура (см. [15], стр. 377).

### 10.3.2 Базисы алгебры Боуза-Меснера

Пусть  $X = \{1, \dots, n\}$  — конечное множество. Матрицей  $A_i = \|a_{k,s}^i\|_{k,s \in X}$ ,  $i = 0, \dots, m$ , инцидентности отношения  $R_i$  схемы отношений  $\mathcal{S} = \mathcal{S}(X, R_0, \dots, R_m)$  называется  $|X| \times |X|$ -матрица, у которой  $a_{k,s}^i = 1$ , если  $(k, s) \in R_i$ , и  $a_{k,s}^i = 0$ , если  $(k, s) \notin R_i$ .

Легко проверить, свойство п. ii. определения 10.0.1 эквивалентно выполнению следующих соотношений

$$A_i A_j = \sum_{t=0}^m r_{i,j}^t A_t, \quad (10.3.12)$$

где  $r_{i,j}^t$  — целые неотрицательные числа. Вычислить числа в общем случае весьма нетривиально. Мы это сделаем для некоторых схем отношений  $\mathcal{S}_H(\mathfrak{G})$ .

Далее мы будем, не оговаривая это особо, рассматривать только случай при котором схема  $\mathcal{S}$  является ассоциативной схемой, т.е. случай при котором  $r_{i,j}^t = r_{j,i}^t$ . В этом случае  $A_i A_j = A_j A_i$  для всех  $i, j$ , т.е. матрицы  $A_i$  и  $A_j$  являются перестановочными. Более того, матрицы  $A_j$ , очевидно, являются симметрическими, ибо по определению  $A_j^T = A_{j'} = A_j$ .

В настоящем разделе мы вместо определения 10.0.1 будем использовать в качестве исходной точки наших исследований соотношение (10.3.12). Определение 10.0.1 нам понадобилось только для того, чтобы обосновать справедливость равенства (10.3.12).

Из соотношения (10.3.12) вытекает, что произведение  $A_i A_j$  выражается как сумма с целыми коэффициентами базовых матриц  $A_t$ . Отсюда следует, что множество матриц  $\mathfrak{A} = \{c_0 A_0 + \dots + c_m A_m \mid c_i \in \mathbf{C}\}$  замкнуто относительно сложения и умножения, т.е.  $\mathfrak{A}$  является алгеброй. Эта алгебра носит название алгебры Боуза-Меснера (Bouse-Mesner



algebra) или алгебры матриц инцидентности. Эта алгебра в рассматриваемом нами случае является коммутативной.

Так как матрицы  $A_j$ , очевидно, являются линейно-независимыми, то одним из ее базисов  $\mathfrak{B}$  алгебры  $\mathfrak{A}$ , рассматриваемой как линейное пространство над  $\mathbf{C}$ , является множество всех ее  $|X| \times |X|$ -матриц инцидентности:  $\mathfrak{B} = \{A_0, A_1, \dots, A_m\}$ ,  $A_0 = I$ , где  $I$  — единичная матрица (матрица отвечающая соотношению  $R_0$ ).

Заметим, что

$$A_0 + A_1 + \dots + A_m = J, \quad (10.3.13)$$

где  $J$  —  $|X| \times |X|$ -матрица, у которой все элементы равны 1.

Алгебра Боуза-Меснера является полупростой. Это, в частности, означает, что существуют базис  $\mathfrak{B}' = \{E_0, E_1, \dots, E_m\}$  алгебры  $\mathfrak{A}$ , состоящий из  $|X| \times |X|$ -матриц  $E_k$ , такой, что

i.

$$E_k E_s = \begin{cases} 0, & \text{если } k \neq s, \\ E_k, & \text{если } s = k \end{cases}. \quad (10.3.14)$$

Матрицы  $E_k$  являются идемпотентами, т.е. для них справедливо соотношение  $E_k^2 = E_k$ , из которого, в частности, вытекает, что все собственные значения каждой матрицы  $E_k$  равны 0 или 1.

ii. Пусть  $V_A$  — подпространство пространства  $\mathbf{C}^{|X|}$  (на этом пространстве действуют элементы алгебры  $\mathfrak{A}$ ), порожденное всеми собственными векторами матрицы  $A \in \mathfrak{A}$  с собственным значением равным 1. Очевидно,  $V_{AA'} = V_A \cap V_{A'}$ .

Как вытекает из определения матриц  $E_k$  пространство  $V_{E_k}$  обладает следующим свойством:

$$V_{E_k} \cap V_A = \{0\}, \text{ либо } V_{E_k} \cap V_A = V_{E_k} \text{ для каждой матрицы } A \in \mathfrak{A}. \quad (10.3.15)$$

То же самое можно сказать и несколько иначе: матрица  $E_k$  — неприводима, если для любой матрицы  $A \in \mathfrak{A}$  либо  $AE_k = 0$ , либо  $AE_k = E_k$ .

Отметим, что вектор  $\mathbf{a}E_k$ ,  $\mathbf{a} \in \mathbf{C}^{|X|}$ , обычно называют проекцией вектора  $\mathbf{a}$  на подпространство  $V_{E_k}$ , а  $E_k$  — оператором проектирования.

**Замечание 10.3.1** Алгебра  $\mathfrak{A}$  — коммутативна. Поэтому, как хорошо известно [22], существует невырожденная матрица  $C$  с действительными элементами такая, что для любой матрицы  $A \in \mathfrak{A}$  матрица  $C^{-1}AC$  является диагональной, т.е. в некотором базисе пространства  $\mathbf{C}^{|X|}$  все матрицы из  $\mathfrak{A}$  являются диагональными.

Ранг матриц  $E_k$  будем обозначать через  $t_k$ . Очевидно, что  $t_0 + \dots + t_m = |X|$ .

Отметим, что явное вычисление матриц  $E_k$  является достаточно нетривиальной задачей.

Так как  $\mathfrak{B}$  и  $\mathfrak{B}'$  базисы алгебры  $\mathfrak{A}$  и  $A_k \in \mathfrak{A}$ , то

$$A_k = P_k(0)E_0 + P_k(1)E_1 + \cdots + P_k(m)E_m, \quad k = 0, \dots, m \quad (10.3.16)$$

и

$$E_k = Q_k(0)A_0 + Q_k(1)A_1 + \cdots + Q_k(m)A_m, \quad k = 0, \dots, m, \quad (10.3.17)$$

где  $P_j(k), Q_j(k) \in \mathbf{C}$  — коэффициенты, которые, как следует из замечания, являются действительными числами. Понятно, что матрица  $P = \|P_j(k)\|_{j,k=0,\dots,m}$  является матрицей перехода от базиса  $\mathfrak{B}'$  к базису  $\mathfrak{B}$ . Далее для некоторых схем отношений  $\mathcal{S}_H(\mathfrak{G})$  мы вычислим элементы матрицы  $P$ .

Предварительно рассмотрим некоторые общие свойства чисел  $P_j(k)$  и  $Q_j(k)$ .

**Лемма 10.3.3** *Функции  $P_j(k)$  являются ортогональными с весами  $t_k$ :*

$$\sum_{k=0}^m t_k P_j(k) P_s(k) = \begin{cases} 0, & j \neq s; \\ v_s |X|, & j = s. \end{cases} \quad (10.3.18)$$

**Доказательство.** С одной стороны из свойства **i**. (соотношение (10.3.14)) и соотношения (10.3.16) вытекает, что

$$A_j A_s = P_j(0)P_s(0)E_0 + P_j(1)P_s(1)E_1 + \cdots + \bar{P}_j(m)P_s(m)E_m \quad (10.3.19)$$

С другой стороны из соотношения (10.3.12) получаем, что

$$\text{tr } A_j A_s = \text{tr} \left( \sum_{t=0}^m r_{j,s}^t A_t \right) = r_{j,s}^0 \text{tr } A_0 = |X| r_{j,s}^0, \quad (10.3.20)$$

ибо  $\text{tr } A_s = 0, s \neq 0$ , в виду того, что все диагональные элемента матрицы  $A_s, s \neq 0$ , по определению схемы отношений равны 0. Очевидно из определения схемы отношений следует, что  $r_{j,s}^0 = 0$ , если  $s \neq j$ , и  $r_{j,s}^0 = v_s$ , если  $s = j$ .  $\square$

Напомним, что число  $v_s$  называется валентностью отношения  $R_s$ . По определению, оно равно числу ребер  $(x, y) \in X \times X$  с фиксированной вершиной  $x \in X$ , которые принадлежат отношению  $R_s$ . Для схем отношений  $\mathcal{S}_H(\mathfrak{G})$   $v_s = |C_s|$  — числу элементов в классе сопряженных элементов  $C_s$ . Поэтому данным случае последнее равенство в (10.3.18) можно записать в виде  $\sum_{k=0}^m t_k P_s j(k) P_s(k) = |C_s| |X|$ .

Рассмотрим  $m+1 \times m+1$ -матрицы  $P = \|P_s(k)\|_{s,k=0,\dots,m}$ ,  $Q = \|Q_s(k)\|_{s,k=0,\dots,m}$  и  $T = \text{diag}(t_0, \dots, t_m)$ ,  $V = \text{diag}(v_0, \dots, v_m)$ . Очевидно, утверждение леммы 10.3.3 коротко можно записать в виде

$$P^T \cdot T \cdot P = |X| V \quad (10.3.21)$$

Кроме того, из соотношений (3.1.7), (10.3.17) и из леммы 10.3.3 вытекает (Упражнение)

$$Q = |X| P^{-1} = V^{-1} \cdot P^T \cdot T \quad (10.3.22)$$

Отсюда, в частности, следует, что

$$t_s P_k(s) = v_k Q_s(k) \quad s, k = 0, \dots, m. \quad (10.3.23)$$

**Следствие 10.3.1 (Из леммы 10.3.3)**

$$\sum_{k=0}^m v_k Q_j(k) Q_s(k) = \begin{cases} 0, & j \neq s; \\ t_s |X|, & j = s. \end{cases} \quad (10.3.24)$$

Рассмотрим  $m+1 \times m+1$ -матрицы  $U_k = \|r_{i,j}^k\|_{i,j=0,\dots,m}$ ,  $k = 0, \dots, m$ , где числа  $r_{i,j}^k$  — числа из определения 10.0.1. Нетрудно установить (Упражнение), что

$$v_k \sum_{j=0}^m r_{i,j}^k = v_i \sum_{j=0}^m r_{k,j}^i \quad \text{и} \quad \sum_{k=0}^m r_{i,j}^k r_{k,s}^l = \sum_{h=0}^m r_{i,h}^l r_{j,s}^h. \quad (10.3.25)$$

**Лемма 10.3.4** *Множество  $m+1 \times m+1$ -матриц  $U = \{U_k | k = 0, \dots, m\}$  с коэффициентами из кольца целых чисел являются базисом алгебры  $\mathfrak{A}'$ , которая изоморфна алгебре  $\mathfrak{A}$ .*

**Доказательство** вытекает из соотношения

$$U_i U_j = \sum_{t=0}^m r_{i,j}^t U_t, \quad (10.3.26)$$

которое является непосредственным следствием соотношения (10.3.25).  $\square$

Из этой леммы, в частности, вытекает, что собственные числа  $P_k(s)$ ,  $s = 0, \dots, m$ , матриц  $U_k$  совпадают с собственными значениями матрицы  $A_k$ . Следовательно, числа  $P_k(s)$ ,  $s = 0, \dots, m$ , являются корнями уравнения  $\det(U_k - xI_{m+1}) = 0$ .

Обычно число  $m+1$  значительно меньше числа  $|X|$ . В этом случае лемма (10.3.4) позволяет, вместо вычислений в алгебре  $\mathfrak{A}$   $|X| \times |X|$ -матриц, использовать вычисления в алгебре  $\mathfrak{A}'$   $m+1 \times m+1$ -матриц, размерность которых существенно меньше, чем  $|X| \times |X|$ . В частности, для вычисления коэффициентов  $P_k(s)$  конкретных ассоциативных схем целесообразно использовать указанное выше уравнение.

### 10.3.3 Вычисление коэффициентов $P_k(j)$ для ассоциативной схемы $\mathcal{S}_H(\mathfrak{G})$ , у которой $H = Inn(\mathfrak{G})$ . Продолжение примера 10.1.2

Мы будем элементы множества  $X$  отождествлять с элементами группы  $\mathfrak{G}$ , строки и столбцы  $|\mathfrak{G}| \times |\mathfrak{G}|$ -матрицы инцидентий  $A_k$  отношения  $R_k$  будем индексировать элементами группы  $\mathfrak{G} = \{\mathfrak{g}_1, \dots, \mathfrak{g}_N\}$ ,  $N = |\mathfrak{G}|$  так, что

$$A_k = \|a_{\mathfrak{g},\mathfrak{g}'}^k\|_{\mathfrak{g},\mathfrak{g}' \in \mathfrak{G}} \quad \text{и} \quad a_{\mathfrak{g},\mathfrak{g}'}^k = \varphi_k(\mathfrak{g}, \mathfrak{g}'), \quad (10.3.27)$$

где  $\varphi_k$  — характеристическая функция отношения  $R_k$  схемы отношений  $\mathcal{S}_H(\mathfrak{G})$ , т.е.

$$\varphi_k(\mathfrak{g}, \mathfrak{g}') = \begin{cases} 1, & \text{если } (\mathfrak{g}, \mathfrak{g}') \in R_k; \\ 0, & \text{если } (\mathfrak{g}, \mathfrak{g}') \notin R_k. \end{cases} \quad (10.3.28)$$

Умножим левую и правую части равенства (10.3.16) на матрицу  $E_s$ . В результате получим, используя соотношение (10.3.14), получим

$$A_k E_s = P_k(s) E_s. \quad (10.3.29)$$

Из этого соотношения видно, что если  $\mathbf{a} \in V_{E_s}$ , то  $\mathbf{a}$  — собственный вектор с собственным значением  $P_k(s)$  матрицы  $A_k$ . Таким образом, чтобы вычислить число  $P_k(s)$  достаточно вычислить собственное значение какого-либо ненулевого вектора  $\mathbf{a} \in V_{E_s}$ .

Пусть  $\mathbf{h}_s$  — представитель смежного класса  $C_s$  и  $\chi_j(\mathbf{r})$  — характер неприводимого представления  $\Gamma^j$  группы  $\mathfrak{G}$ . Из хорошо известного соотношения (см. [14], § 2.5)

$$\sum_{j=0}^m \bar{\chi}_j(\mathbf{h}_s) \chi_j(\mathbf{g}) = \begin{cases} 0, & \text{если } \mathbf{g} \text{ и } \mathbf{h}_s \text{ не сопряжены (находятся в} \\ & \text{различных классах сопряженных элементов);} \\ \frac{|\mathfrak{G}|}{|C_s|}, & \text{если } \mathbf{g} \text{ и } \mathbf{h}_s \text{ принадлежат одному} \\ & \text{классу сопряженных элементов } C_s. \end{cases} \quad (10.3.30)$$

и определения матрицы  $A_k$  вытекает, что

$$\varphi_k(\mathbf{g}, \mathbf{g}') = \psi_k(\mathbf{g}' \mathbf{g}^{-1}) = \frac{|C_k|}{|\mathfrak{G}|} \sum_{j=0}^m \bar{\chi}_j(\mathbf{h}_k) \chi_j(\mathbf{g}' \mathbf{g}^{-1}) = \frac{1}{|\mathfrak{G}|} \sum_{j=0}^m \sum_{h \in C_k} \bar{\chi}_j(\mathbf{h}) \chi_j(\mathbf{g}' \mathbf{g}^{-1}), \quad (10.3.31)$$

где  $\psi_k$  — характеристическая функция класса сопряженных элементов  $C_k$ .

**Теорема 10.3.1** Рассмотрим вектор  $\mathbf{a}_s(\mathbf{h}) = (\chi_s(\mathbf{h}\mathbf{g}_1), \dots, \chi_s(\mathbf{h}\mathbf{g}_N))$ ,  $N = |\mathfrak{G}|$ .

i. При любом  $\mathbf{h} \in \mathfrak{G}$  вектор  $\mathbf{a}_s(\mathbf{h})$  является собственным вектором матрицы  $A_k$  с собственным значением

$$P_s(k) = \frac{|C_k|}{f_s} \chi_s(\mathbf{h}_k^{-1}), \quad (10.3.32)$$

где  $\mathbf{h}_k$  — представитель смежного класса  $C_k$ .

ii.

$$\langle \mathbf{a}_s(\mathbf{h}), \mathbf{a}_j(\mathbf{h}') \rangle = \begin{cases} \frac{\chi_s(\mathbf{h}' \mathbf{h})}{f_s}, & \text{если } j = s; \\ 0, & \text{если } j \neq s. \end{cases} \quad (10.3.33)$$

В частности, подпространства  $V_{E_s}$ ,  $s = 0, \dots, m$ , пространства  $\mathbf{C}^{|\mathfrak{G}|}$ , натянутые на множество векторов  $\{\mathbf{a}_s(\mathbf{h}) | \mathbf{h} \in \mathfrak{G}\}$ , являются ортогональными.

**Доказательство.** Очевидно из (10.3.31) вытекает, что матрицу  $A_k$  можно представить в виде

$$A_k = \|a_{\mathbf{g}, \mathbf{g}'}^k\|_{\mathbf{g}, \mathbf{g}' \in \mathfrak{G}} = \|\psi_k(\mathbf{g}' \mathbf{g}^{-1})\|_{\mathbf{g}', \mathbf{g} \in \mathfrak{G}}. \quad (10.3.34)$$

Отсюда следует, что координата  $b_{\mathbf{g}'}$  вектора  $\mathbf{a}_s(\mathbf{h}) A_k$ , индексированная элементом  $\mathbf{g}'$ , равна  $b_{\mathbf{g}'} = \sum_{\mathbf{g} \in \mathfrak{G}} a_{\mathbf{g}, \mathbf{g}'}^k \chi_s(\mathbf{h}\mathbf{g})$ . Как следует из определения функции  $\psi_k$  (см. (10.3.31)),

$$b_{\mathbf{g}'} = \frac{|C_k|}{|\mathfrak{G}|} \sum_{\mathbf{g} \in \mathfrak{G}} \sum_{j=0}^m \bar{\chi}_j(\mathbf{h}_k) \chi_j(\mathbf{g}' \mathbf{g}^{-1}) \chi_s(\mathbf{h}\mathbf{g}). \quad (10.3.35)$$

Если положить  $\mathbf{f} = \mathbf{h}\mathbf{g}$ , то последнее равенство можно записать в виде

$$b_{\mathfrak{g}'} = |C_k| \sum_{j=0}^m \overline{\chi}_j(\mathfrak{h}_k) \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{f} \in \mathfrak{G}} \chi_j(\mathfrak{g}' \mathfrak{h} \mathfrak{f}^{-1}) \chi_s(\mathfrak{f}). \quad (10.3.36)$$

Как следует из леммы 10.3.1

$$\begin{aligned} \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{f} \in \mathfrak{G}} \chi_j(\mathfrak{g}' \mathfrak{h} \mathfrak{f}^{-1}) \chi_s(\mathfrak{f}) &= \frac{1}{|\mathfrak{G}|} \sum_{\mathfrak{f} \in \mathfrak{G}} \chi_j(\mathfrak{g}' \mathfrak{h} \mathfrak{f}) \chi_s(\mathfrak{f}^{-1}) = \\ \langle \chi_s(\mathfrak{f}), \chi_j(\mathfrak{g}' \mathfrak{h} \mathfrak{f}) \rangle &= \begin{cases} \frac{\chi_s(\mathfrak{g}' \mathfrak{h})}{f_s}, & \text{если } j = s; \\ 0, & \text{если } j \neq s. \end{cases} \end{aligned} \quad (10.3.37)$$

Как известно, и это легко установить, что  $\chi_s(\mathfrak{g}' \mathfrak{h}) = \chi_s(\mathfrak{h} \mathfrak{g}' \mathfrak{h} \mathfrak{h}^{-1}) = \chi_s(\mathfrak{h} \mathfrak{g}')$ . Это доказывает вместе с соотношениями (10.3.36) и леммой 10.3.1, что

$$b_{\mathfrak{g}'} = |C_k| \frac{\overline{\chi}_s(\mathfrak{h}_k)}{f_s} a_{\mathfrak{g}'} = \frac{|C_k|}{f_s} \chi_s(\mathfrak{h}_k^{-1}) a_{\mathfrak{g}'}, \quad (10.3.38)$$

где  $a_{\mathfrak{g}'}$  — координата вектора  $\mathbf{a}_s(\mathfrak{h})$ , индексированная элементом  $\mathfrak{g}'$ .

Как нетрудно увидеть, соотношение (10.3.38) эквивалентно утверждению п.i. теоремы 10.3.1.

Утверждение п.ii. теоремы непосредственно вытекает из леммы 10.3.1.  $\square$

Предположительно, размерность подпространства пространства  $\mathbf{C}^{|\mathfrak{G}|}$ , натянутого на множество векторов  $\mathbf{a}_s(\mathfrak{h})$ ,  $\mathfrak{h} \in \mathfrak{G}$ , равна  $|C_s|$ .

#### 10.3.4 $\mathfrak{G}$ — группа $(\mathbb{F}_p, +)$ . Продолжение примера 10.1.1

В рассматриваемом случае все неприводимые представления  $\Gamma_a$ ,  $a \in \mathbb{F}_p$ , группы  $\mathfrak{G}$  являются, как известно, одномерными и имеют вид, приведенный в примере 10.1.1. Соответственно, характер  $\chi_a(x)$  представления  $\Gamma_a$  имеет вид

$$\chi_a(x) = \exp\left(\frac{2\pi i a x}{p}\right), \quad x \in \mathbb{F}_p. \quad (10.3.39)$$

Напомним, что подгруппа автоморфизмов  $\Phi_d$  разбивает группу  $\mathfrak{G}$  на  $d' + 1 = 1 + \frac{p-1}{d}$  классов сопряженных элементов  $C_0, C_1, \dots, C_{d'}$ ,  $C_0 = \{0\}$ ,  $C_j = \{\tau^j x^{\frac{p-1}{d}} | x \in \mathbb{F}_p^*\}$ ,  $j = 1, \dots, d'$ ,  $dd' = p - 1$ , где  $\tau$  — первообразный элемент группы  $\mathbb{F}_p^*$ .

Заметим, что соотношение (10.3.31) уже не работает, так как все автоморфизмы группы  $\mathbb{F}_p$  являются внешними. Вместе с тем явный вид характеристической функции  $\psi_k(x - y)$ ,  $k \neq 0$ , класса  $C_k$  сопряженных относительно  $\Phi_d$  легко выписать с учетом того, что групповой операцией в группе  $\mathbb{F}_p$  является сложение: (Упражнение)

$$\psi_k(x) = \frac{1}{|C_k|p} \sum_{a, z \in \mathbb{F}_p} \exp\left(\frac{2\pi i a(x - \tau^k z^{\frac{p-1}{d}})}{p}\right) = \frac{1}{p} \sum_{a \in \mathbb{F}_p} \exp\left(\frac{2\pi i a x}{p}\right) \vartheta_k(-a), \quad (10.3.40)$$

где

$$\vartheta_k(b) = \frac{1}{|C_k|} \sum_{z \in \mathbb{F}_p} \exp\left(\frac{2\pi i b \tau^k z^{\frac{p-1}{d}}}{p}\right), \quad k = 0, \dots, d - 1. \quad (10.3.41)$$

Таким образом,  $A_k = \|a_{x,y}\|_{x,y \in \mathbb{F}_p} = \|\psi_k(y-x)\|_{x,y \in \mathbb{F}_p}$ .

**Теорема 10.3.2** *Вектор*

$$\mathbf{a}_k(b) = (\vartheta_k(a_1b), \dots, \vartheta_k(a_pb)), \text{ где } \{a_1, \dots, a_p\} = \mathbb{F}_p, \quad (10.3.42)$$

является собственным вектором матрицы  $A_k$  с собственным значением  $|C_k| = d$ .

**Доказательство.** Координата  $\alpha_y$ , индексированная элементом  $y \in \mathbb{F}_p$ , вектора  $\mathbf{a}(b)A_k = \mathbf{a}(b)\|\psi_k(y-x)\|$  имеет вид

$$\begin{aligned} \alpha_y &= \sum_{x \in \mathbb{F}_p} \vartheta_k(xb)\psi_k(y-x) = \\ &= \frac{1}{p} \sum_{x \in \mathbb{F}_p} \sum_{a \in \mathbb{F}_p} \exp\left(\frac{2\pi i a(y-x)}{p}\right) \vartheta_k(-a)\vartheta_k(xb). \end{aligned} \quad (10.3.43)$$

Как нетрудно установить (Упражнение), что

$$\frac{1}{p} \sum_{x \in \mathbb{F}_p} \exp\left(\frac{-2\pi i ax}{p}\right) \vartheta_k(bx) = \begin{cases} \exp\left(\frac{-2\pi i ax}{p}\right), & \text{если уравнение } a = b\tau^k z^{\frac{p-1}{d}} \text{ разрешимо;} \\ 0, & \text{в противном случае.} \end{cases} \quad (10.3.44)$$

Отсюда и (10.3.43) вытекает, что

$$\alpha_y = |C_k|\beta_y, \quad (10.3.45)$$

где  $\beta_y$  — координата вектора  $\mathbf{a}(b)$ , индексированная элементом  $y \in \mathbb{F}_p$ . Теорем доказана.  $\square$

Отметим, что вектор  $\mathbf{a}_k(b)$  и  $\mathbf{a}_s(b')$ ,  $b, b' \neq 0$ , (при одном и том же значении параметра  $d$ ) может быть получен из другого перестановкой координат. Это следует из того, что два множества  $\{a_1b\tau^k, \dots, a_pb\tau^k\}$  и  $\{a_1b'\tau^s, \dots, a_pb'\tau^s\}$  совпадают. Кроме того, очевидно, что  $\vartheta_k(a) = \vartheta_k(ay^{\frac{p-1}{d}})$  для любого  $y \neq 0$ , т.е.  $\vartheta_k(a) = \vartheta_k(b)$ , если  $a$  и  $b$  принадлежат одному и тому же классу сопряженных элементов.

Упражнение.

1. Вычислить векторы  $\mathbf{a}_k(b)$  для  $d = p-1$  и  $\frac{p-1}{2}$ .
2. Вычислить коэффициенты  $p_{i,j}^k$  в соотношении (10.3.20).

### 10.3.5 Схемы отношений Хемминга

Схемы отношений Хемминга  $\mathcal{H}_q^n$ , по-видимому, самый простой тип ассоциативных схем. Эти схемы тесно связаны с теорией кодирования. Некоторые сведения об этом имеются в разделе 10.4.6. Следует также отметить обширную обзорную статью [73], в которой подробно прослеживаются связи схем отношений Хемминга и теории кодирования. В частности, в этой статье дан вывод оценки линейного программирования, основанный на некоторых свойствах схем отношений, который несколько отличается от вывода этой оценки в разделе 4.2.1.

В примере 10.0.2 приведено определение схем отношений Хемминга. Заметим, что хорошо известно, что коэффициентами  $P_k(x)$  в соотношениях (10.3.16) и (10.3.17) являются ортогональные многочлены Кравчука (см. равенство (3.2.13)). В разделе 3 изучены некоторые свойства этих многочленов.

## 10.4 Метрики на схеме отношений $C_H(\mathfrak{G})$

Метрику  $\lambda(\mathfrak{g}, \mathfrak{g}')$  назовем центральной метрикой относительно схемы отношений  $C_H(\mathfrak{G}^n)$ , если  $\lambda(\mathfrak{g}, \mathfrak{g}') = \lambda(\mathfrak{h}, \mathfrak{h}')$  в том случае, когда  $(\mathfrak{g}, \mathfrak{g}')$  и  $(\mathfrak{h}, \mathfrak{h}')$  принадлежат одному тому же классу отношений схемы  $C_H(\mathfrak{G}^n)$ .

Несколько иначе это понятие можно определить следующим образом. Метрика  $\lambda(\mathfrak{g}, \mathfrak{g}')$  является центральной метрикой относительно схемы отношений  $C_H(\mathfrak{G}^n)$ , если  $\lambda(\mathfrak{g}, \mathfrak{g}') = \lambda(\mathfrak{h}, \mathfrak{h}')$  в том случае, когда элементы  $\mathfrak{g}'\mathfrak{g}^{-1}$  и  $\mathfrak{h}'\mathfrak{h}^{-1}$  принадлежат одному и тому же классу сопряженных элементов.

Далее на группе  $\mathfrak{G}$  мы определим метрики  $\lambda$  (вообще говоря, неХемминговые), которые являются центральными относительно отношений схемы  $C_H(\mathfrak{G}^n)$ .

В этих метриках, в отличие от метрики Хэмминга (в одномерном случае), расстояния между различными элементами  $\mathfrak{G}$ , вообще говоря, различны. Известная метрика Ли (ее определение ниже) похожа на рассматриваемые метрики  $\lambda$  в том случае, когда  $\mathfrak{G}$  — абелева группа, но совпадает с одной из них только для некоторых групп  $\mathfrak{G}$ . Это в частности происходит том случае, когда  $\mathfrak{G}$  — группа вычетов по  $\text{mod } 4$ .

Определение метрики Ли. Мы рассматриваем множество  $X = \{0, \dots, r-1\}$  как аддитивную циклическую группу, образованную неотрицательными вычетами по  $\text{mod } r$ . Расстояние Ли  $l(a, b)$  между элементами  $a, b \in X$  — это наименьший по абсолютной величине число среди вычетов  $b - a \in X$  и  $a - b \in X$ , т.е.  $l(a, b) = \min(b - a \text{ mod } r, a - b \text{ mod } r)$ . Например, если  $r = 5$ , то  $l(0, 1) = 1$  и  $l(4, 1) = 2$  и т.д.

Упражнение. Доказать, что  $l(a, b)$  — действительно метрика.

Как представляется автору, коды в пространстве с метрикой  $\lambda$  естественно использовать для исправления ошибок в дискретном  $q$ -ичном канале связи с шумом, в котором различны вероятности перехода одного символа в другой. Подобные коды лучше, чем коды в метрике Хэмминга, учитывают специфику некоторых несимметрических каналов связи. Соображения на этот счет имеются также в разделе 6.1). Ограничимся только этим общим замечанием, ибо каналы и связанные с ними метрики не являются темой для исследований настоящей работы.

**Определение 10.4.1 (Дистанационно-транзитивная метрика)** Метрика  $\lambda(\mathfrak{g}, \mathfrak{g}')$ ,  $\mathfrak{g}, \mathfrak{g}' \in \mathfrak{G}$ , называется дистанационно-транзитивной справа на группе  $\mathfrak{G}$ , если

$$\lambda(\mathfrak{g}, \mathfrak{g}') = \lambda(\mathfrak{g}\mathfrak{h}, \mathfrak{g}'\mathfrak{h}) \text{ для всех } \mathfrak{h} \in \mathfrak{G}. \quad (10.4.1)$$

Как следует из определения схемы  $C_H(\mathfrak{G})$ , центральная относительно  $C_H(\mathfrak{G})$  метрика одновременно является дистанационно-транзитивной справа метрикой. Особенно ясно это следует из определения второго абзаца этого раздела (см. начало раздела).

Отметим, что для дистанационно-транзитивной справа метрики равенство  $\lambda(\mathfrak{g}, \mathfrak{g}') = \widehat{\lambda}(\mathfrak{h}\mathfrak{g}, \mathfrak{h}\mathfrak{g}')$ , вообще говоря, может не выполняться.

**Определение 10.4.2 (Дистанационно-регулярная метрика)** Дистанационно-транзитивная справа метрика  $\lambda$  называется дистанационно-регулярной, если число  $N_{\mathfrak{g}, \mathfrak{g}'}(a, b)$  элементов  $\mathfrak{h} \in \mathfrak{G}$ , для которых  $\lambda(\mathfrak{g}, \mathfrak{h}) = a$ ,  $\lambda(\mathfrak{h}, \mathfrak{g}') = b$ , определяется только величиной  $c = \lambda(\mathfrak{g}, \mathfrak{g}')$ , т.е.  $N_{\mathfrak{g}, \mathfrak{g}'}(a, b) = N_c(a, b)$ .

Например, одномерная метрика Хэмминга, для которой  $\lambda(\mathfrak{g}, \mathfrak{g}') = 1$ , если  $\mathfrak{g} \neq \mathfrak{g}'$ , и  $\lambda(\mathfrak{g}, \mathfrak{g}) = 0$ , является, очевидно, дистанционно-регулярной.

Окружность  $\mathfrak{G}$  в евклидовой плоскости с центром в начале координат можно рассматривать как бесконечную группы, у которой групповой операцией является повороты относительно ее центра. Мы будем обозначать через  $\lambda(\mathfrak{g}, \mathfrak{g}')$ ,  $\mathfrak{g}, \mathfrak{g}' \in \mathfrak{G}$ , обычную евклидовую метрику на  $\mathfrak{G}$ . Как нетрудно установить, число  $N_{\mathfrak{g}, \mathfrak{g}'}(a, b)$  элементов  $\mathfrak{h} \in \mathfrak{G}$ , для которых  $\lambda(\mathfrak{g}, \mathfrak{h}) = a$ ,  $\lambda(\mathfrak{h}, \mathfrak{g}') = b$ , определяется только величиной  $c = \lambda(\mathfrak{g}, \mathfrak{g}')$ , т.е. метрика  $\lambda$  является дистанционно-регулярной, хотя в данном случае группа  $\mathfrak{G}$  не является конечной. Отметим, что число  $N_{\mathfrak{g}, \mathfrak{g}'}(a, b)$  может принимать одно из трех значений: 0, 1, 2.

Как следует из определения схемы  $\mathbf{C}_H(\mathfrak{G})$ , центральная относительно  $\mathbf{C}_H(\mathfrak{G})$  метрика одновременно является и дистанционно-транзитивной метрикой.

Далее будет рассмотрен один естественный класс дистанционно-регулярных метрик на конечной группы  $\mathfrak{G}$ , который включает в себя метрику Хэмминга как частный случай.

### 10.4.1 Скалярное произведение на группе

Пусть  $\Gamma = \{\Gamma(\mathfrak{g}) | \mathfrak{g} \in \mathfrak{G}\}$  — линейное представление конечной группы  $\mathfrak{G}$  на унитарном пространстве  $\mathbb{C}^f$ ,  $H$  — подгруппа группы  $\text{Aut}(\mathfrak{G})$  автоморфизмов группы  $\mathfrak{G}$  и  $\mathbf{a}$  — вектор на единичной унитарной сфере  $U^{f-1}$ . Скалярное произведение  $\langle \cdot, \cdot \rangle_{H, \mathbf{a}}$  на группе  $G$  мы определим с помощью равенства

$$\langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}} =: \langle \mathfrak{g}, \mathfrak{g}' \rangle =: \frac{1}{|H|} \sum_{\sigma \in H} (\mathbf{a} \Gamma(\mathfrak{g}^\sigma), \mathbf{a} \Gamma(\mathfrak{g}'^\sigma)) = \frac{1}{|C_j^H|} \sum_{\mathfrak{h} \in C_j^H} (\mathbf{a}, \mathbf{a} \Gamma(\mathfrak{h})), \quad (10.4.2)$$

где  $(\cdot, \cdot)$  — обычное скалярное произведение в унитарном пространстве  $U^f$  (см. (1.2.4)) и  $C_j^H$  — класс сопряженных элементов относительно подгруппы  $H$ , к которому принадлежит элемент  $\mathfrak{g}' \mathfrak{g}^{-1}$ . Отметим, что последнее равенство в (10.4.2) выполнено ввиду того, что  $\Gamma(\mathfrak{g})$  — унитарная  $f \times f$  матрица и поэтому  $(\mathbf{a} \Gamma(\mathfrak{g}^\sigma), \mathbf{a} \Gamma(\mathfrak{g}'^\sigma)) = (\mathbf{a}, \mathbf{a} \Gamma(\mathfrak{g}'^\sigma) \Gamma^{-1}(\mathfrak{g}^\sigma)) = (\mathbf{a}, \mathbf{a} \Gamma((\mathfrak{g}' \mathfrak{g}^{-1})^\sigma))$ .

Очевидно,  $\langle \mathfrak{g}, \mathfrak{g} \rangle_{H, \mathbf{a}} = 1$ .

**Замечание 10.4.1** Скалярное произведение  $\langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}}$  можно также рассматривать как обычное скалярное произведение в унитарном пространстве  $\mathbb{C}^{f(t+1)}$  вектора  $\mathbf{b}_{\mathfrak{g}} = \frac{1}{\sqrt{t+1}}(\mathbf{a} \Gamma(\mathfrak{g}^{\sigma_0}), \dots, \mathbf{a} \Gamma(\mathfrak{g}^{\sigma_t}))$ , где  $\{\sigma_0, \dots, \sigma_t\} = H$ , и вектора  $\mathbf{b}_{\mathfrak{g}'} = \frac{1}{\sqrt{t+1}}(\mathbf{a} \Gamma(\mathfrak{g}'^{\sigma_0}), \dots, \mathbf{a} \Gamma(\mathfrak{g}'^{\sigma_t}))$ , каждый из которых имеет длину 1.

Очень поучительно представить в явном виде скалярное произведение  $\langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}}$  для некоторых групп  $\mathfrak{G}$  и подгрупп  $H$  их группы автоморфизмов.

### 10.4.2 Продолжение примера 10.1.1

Для аддитивной группы  $\mathfrak{G}$  поля  $\mathbb{F}_p$ , мы, как обычно, символом  $\Phi_d$  обозначаем подгруппу  $H \subseteq \text{Aut}(\mathbb{F}_p)$ , содержащую  $d$ ,  $d|p-1$ , элементов. Мы рассматриваем одномерное представление  $\| \exp\left(\frac{2\pi i a x}{p}\right) \|$ ,  $a \in \mathbb{F}_p^*$ , группы  $\mathfrak{G}$ . В этом случае скалярное произведение



$\langle a, b \rangle_{\Phi_d, \mathbf{a}} = \langle a, b \rangle_{\Phi_d}$ ,  $a, b \in \mathbb{F}_p$ , , во-первых, не зависит от одномерного вектора  $\mathbf{a}$  длины 1 и, во-вторых, записывается в виде

$$\langle a, b \rangle_{\Phi_d} = \frac{1}{d} \sum_{x \in \mathbb{F}_{p,d}^*} \exp \left( \frac{2\pi i(b-a)x}{p} \right) = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^*} \exp \left( \frac{2\pi i(a-b)x^{\frac{p-1}{d}}}{p} \right). \quad (10.4.3)$$

В частности, если  $d = p-1$ , то

$$\langle a, b \rangle_{\Phi_{p-1}} = \begin{cases} 1, & \text{если } a = b, \\ \frac{-1}{p-1}, & \text{если } a \neq b \end{cases}. \quad (10.4.4)$$

Если же  $d = \frac{p-1}{2}$  и  $b-a \neq 0$ , то

$$\langle a, b \rangle_{\Phi_{\frac{p-1}{2}}} = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^*} \exp \left( \frac{2\pi i(b-a)x^2}{p} \right) = \frac{1}{p-1} \begin{cases} \left( \frac{b-a}{p} \right) (-1 + p^{\frac{1}{2}}), & \text{если } p = 4t+1 \\ \left( \frac{b-a}{p} \right) (-1 + ip^{\frac{1}{2}}), & \text{если } p = 4t-1 \end{cases}, \quad (10.4.5)$$

где  $i = \sqrt{-1}$ .

Соотношение (10.4.5) вытекает из хорошо известного соотношения (см., например, [28]):

$$\sum_{x \in \mathbb{F}_p} \exp \left( \frac{2\pi i x^2}{p} \right) = \begin{cases} \sqrt{p}, & \text{если } p = 4t+1 \\ i\sqrt{p}, & \text{если } p = 4t-1 \end{cases} \quad (10.4.6)$$

Левую часть (10.4.6) называют гауссовой суммой.

### 10.4.3 Продолжение примера 10.1.2

Пусть  $H = Inn(\mathfrak{G})$  — группа внутренних автоморфизмов и  $\mathbf{a} \in U^{f-1}$ .

#### Лемма 10.4.1

$$\langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}} = \frac{tr \Gamma(\mathfrak{g}' \mathfrak{g}^{-1})}{f}. \quad (10.4.7)$$

где  $\Gamma(\mathfrak{g})$  — матрица, представляющая элемент  $\mathfrak{g}$  группы  $\mathfrak{G}$ .

**Доказательство** леммы вытекает из леммы 10.3.2 и соотношения

$$\begin{aligned} \langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}} &= \frac{1}{|G|} \sum_{\mathfrak{h} \in \mathfrak{G}} (\mathbf{a} \Gamma(\mathfrak{h}) \Gamma(\mathfrak{g}) \Gamma(\mathfrak{h}^{-1}), \mathbf{a} \Gamma(\mathfrak{h}) \Gamma(\mathfrak{g}) \Gamma(\mathfrak{h}^{-1})) = \\ &= \frac{1}{|G|} (\mathbf{a}, \mathbf{a} (\sum_{\mathfrak{h} \in \mathfrak{G}} \Gamma(\mathfrak{h}) \Gamma(\mathfrak{g}' \mathfrak{g}^{-1})) \Gamma(\mathfrak{h}^{-1}))_{H, \mathbf{a}} = \frac{1}{f} tr \Gamma(\mathfrak{g}' \mathfrak{g}^{-1}) (\mathbf{a}, \mathbf{a}) = \frac{1}{f} tr \Gamma(\mathfrak{g}' \mathfrak{g}^{-1}). \end{aligned} \quad (10.4.8)$$

□

Как видно из (10.4.8), в случае  $H = Inn(\mathfrak{G})$  скалярное произведение  $\langle \mathfrak{g}, \mathfrak{g}' \rangle_{H, \mathbf{a}}$  не зависит от выбора вектора  $\mathbf{a}$  на сфере  $U^{f-1}$  и полностью определяется представлением  $\Gamma(\mathfrak{G})$  группы  $\mathfrak{G}$ .

Соотношение (10.4.8) иным способом было получено в работе [19].

### 10.4.4 Метрики на группе $\mathfrak{G}$

Определим метрику  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g}) =$  на группе  $\mathfrak{G}$  с помощью скалярного произведения (10.4.2). А именно, положим

$$\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g}) =: \{\langle \mathbf{g}', \mathbf{g}' \rangle_{H,\mathbf{a}} + \langle \mathbf{g}, \mathbf{g} \rangle_{H,\mathbf{a}} - \langle \mathbf{g}', \mathbf{g} \rangle_{H,\mathbf{a}} - \langle \mathbf{g}, \mathbf{g}' \rangle_{H,\mathbf{a}}\}^{\frac{1}{2}} = \sqrt{2 - 2\Re\langle \mathbf{g}', \mathbf{g} \rangle_{H,\mathbf{a}}}, \quad (10.4.9)$$

где  $\Re z$  — действительная часть числа  $z$ .

Отметим, что определение (10.4.9) является аналогом определения метрики  $\lambda'$  на унитарной сфере  $U^{s-1}$  в пространстве  $\mathbf{C}^s$  между векторами  $\mathbf{x}, \mathbf{y} \in U^{s-1}$ , а именно

$$\lambda'(\mathbf{x}, \mathbf{y}) = \sqrt{(\mathbf{y} - \mathbf{x}, \mathbf{y} - \mathbf{x})} = ((\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - (\mathbf{x}, \mathbf{y}) - (\mathbf{y}, \mathbf{x})) = \sqrt{2 - 2\Re(\mathbf{x}, \mathbf{y})}. \quad (10.4.10)$$

То, что  $\lambda_{H,\mathbf{a}}$  является метрикой непосредственно следует из замечания 10.4.1.

Заметим, что  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g}) = \lambda_{H,\mathbf{a}}(\mathbf{g}, \mathbf{g}')$  и  $\lambda_{H,\mathbf{a}}(\mathbf{g}, \mathbf{g}) = 0$ . Кроме того,  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g}) = \lambda_{H,\mathbf{a}}(\mathbf{h}', \mathbf{h})$ , если пары  $(\mathbf{g}', \mathbf{g}), (\mathbf{h}', \mathbf{h})$  принадлежат одному и тому же отношению схемы  $\mathcal{S}_H(\mathfrak{G})$ , т.е. метрика  $\lambda_{H,\mathbf{a}}$  является центральной функцией относительно схемы отношений  $\mathcal{S}_H(\mathfrak{G})$ .

Очевидно, из определения метрики  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  следует, что

$$\lambda_{H,\mathbf{a}}(\mathbf{g}, \mathbf{g}') = \lambda_{H,\mathbf{a}}(\mathbf{g}^\sigma, \mathbf{g}'^\sigma), \quad \sigma \in H. \quad (10.4.11)$$

Функцию  $w(\mathbf{g}) = \lambda(\mathbf{e}, \mathbf{g})$  будем называть весом элемента  $\mathbf{g}$ .

### Продолжение примеров 10.1.1 и 10.1.2

Как следует из соотношений 10.4.4 и 10.4.5

$$\lambda_{\Phi_{p-1}}(a, b) = \begin{cases} 0, & \text{если } a = b, \\ \sqrt{\frac{2p}{p-1}}, & \text{если } a \neq b \end{cases}, \quad (10.4.12)$$

если  $H = \Phi_{p-1}$ . В этом случае метрика  $\lambda_{\Phi_{p-1}}$  пропорциональна метрике Хемминга.

Если  $H = \Phi_{\frac{p-1}{2}}$  и  $p = 4t - 1$ , то

$$\lambda_{\Phi_{\frac{p-1}{2}}}(a, b) = \sqrt{\frac{2}{p-1} \left( p + \left( \frac{b-a}{p} \right) (1 - \sqrt{p}) \right)}, \quad b - a \not\equiv 0 \pmod{p}. \quad (10.4.13)$$

Если же  $p = 4t + 1$ , то выражение для  $\lambda_{\Phi_{\frac{p-1}{2}}}(a, b)$  приводить не будем. Оно похоже на (10.4.13).

Вопрос о том является ли всегда метрика  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  дистанционно-регулярной остается открытым. С одной стороны, имеются многочисленные примеры, когда метрика  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  — дистанционно-регулярна. Некоторые из них будут приведены ниже. С другой стороны не известно ни одного примера групп  $\mathfrak{G}$  и  $H$ , для которых метрика  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  не была бы дистанционно-регулярной. Автор предполагает, что  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  — всегда дистанционно-регулярна, но доказать это в общем случае он не может.

**Определение 10.4.3** Пусть  $\lambda(\mathfrak{g}', \mathfrak{g})$  — произвольная метрика на группе  $\mathfrak{G}$ , принимающая значения  $a_0 = 0, a_1, \dots, a_m$ . Схема отношений  $\mathcal{S} = \mathcal{S}(\mathfrak{G}, R_0, \dots, R_m)$  (см. определение 10.0.1) называется метрической, если  $(\mathfrak{g}', \mathfrak{g}) \in R_j$  тогда и только тогда,  $\lambda(\mathfrak{g}', \mathfrak{g}) = a_j$ .

Следует сказать, что термин "метрическая схема", введенный в книге [7], не совпадает с нашим.

Отметим, что если схема  $\mathcal{S}$  является метрической, то она является обязательно симметрической, т.е. ассоциативной схемой, у которой взаимное отношение  $R_j^T$  совпадает с исходным:  $R_j^T = R_j$ . Это следует из того, что метрика является симметрической функцией:  $\lambda(\mathfrak{g}', \mathfrak{g}) = \lambda(\mathfrak{g}, \mathfrak{g}')$  и поэтому пары  $(\mathfrak{g}', \mathfrak{g})$  и  $(\mathfrak{g}, \mathfrak{g}')$  должны принадлежать одному и тому же отношению.

Например, схема отношений Хемминга  $\mathcal{H}_q^n$  по ее определению является метрической при любом  $n$ . Схемы  $\mathcal{S}_H((\mathbb{F}_p, +))$  с  $H = \Phi_{p-1}$  и  $H = \Phi_{\frac{p-1}{2}}$ , как следует из (10.4.12) и (10.4.13), также являются метрическими.

#### Теорема 10.4.1

- i Метрика  $\lambda_{H,a}(\mathfrak{g}', \mathfrak{g})$  на  $\mathfrak{G}$  является транзитивно-инвариантной справа.
- ii Метрика  $\lambda_{H,a}(\mathfrak{g}', \mathfrak{g})$  является дистанционно-регулярной на  $\mathfrak{G}$ , а схема  $\mathcal{S}_H(\mathfrak{G})$  — метрической, если  $\lambda_{H,a}(\mathfrak{g}', \mathfrak{g}) \neq \lambda_{H,a}(\mathfrak{h}', \mathfrak{h})$  в том случае, когда  $(\mathfrak{g}', \mathfrak{g})$  и  $(\mathfrak{h}', \mathfrak{h})$  принадлежат разным классам сопряженных элементов.

**Доказательство п. i.** Ранее было отмечено, что функция  $\lambda_{H,a}(\mathfrak{g}', \mathfrak{g})$  является метрикой на  $\mathfrak{G}$ .

Матрица  $\Gamma(\mathfrak{h})$ ,  $\mathfrak{h} \in \mathfrak{G}$  является унитарной, поэтому  $(a\Gamma(\mathfrak{g})\Gamma(\mathfrak{h}), a\Gamma(\mathfrak{g}')\Gamma(\mathfrak{h})) = (a\Gamma(\mathfrak{g}), a\Gamma(\mathfrak{g}'))$ . Отсюда и из определения метрики следует, что метрика  $\lambda_{H,a}$  является транзитивно инвариантной справа. В частности,  $\lambda_{H,a}(\mathfrak{g}, \mathfrak{g}') = \lambda_{H,a}(\mathfrak{e}, \mathfrak{g}'\mathfrak{g}^{-1}) = w(\mathfrak{g}'\mathfrak{g}^{-1})$ .

Так как метрика  $\lambda_{H,a}$  является транзитивно инвариантной, для доказательства п. ii. можно положить  $\mathfrak{g}' = \mathfrak{e}$ , т.е. можно рассматривать только пары  $\mathfrak{e}, \mathfrak{g}$  в качестве  $\mathfrak{g}', \mathfrak{g}$ .

**Доказательство п. ii.** Нам достаточно показать, что для любого числа  $c$ , для которого существует пара  $(\mathfrak{g}, \mathfrak{g}')$  такая, что  $\lambda_{H,a}(\mathfrak{g}, \mathfrak{g}) = c$ , число  $N_{a,b}^c$  пар  $(\mathfrak{g}, \mathfrak{h})$  и  $(\mathfrak{h}, \mathfrak{g}')$ , для которых  $\lambda_{H,a}(\mathfrak{g}, \mathfrak{h}) = a$  и  $\lambda_{H,a}(\mathfrak{g}', \mathfrak{h}) = b$ , зависит только от числа  $c$ .

Из условия теоремы следует, числа  $a, b, c$  однозначно определяют отношения  $R_i, R_j, R_k$ , к которым принадлежит пары  $(\mathfrak{g}, \mathfrak{h})$ ,  $(\mathfrak{g}', \mathfrak{h})$  и  $(\mathfrak{g}, \mathfrak{g}')$ , соответственно. Отсюда следует, что  $N_{a,b}^c = r_{i,j}^k$ . Из этого равенства вытекает доказательство п.ii. теоремы.  $\square$

Если группа  $\mathfrak{G}$  — абелева или  $H$  — группа, образованная всеми внутренними автоморфизмами некоммутативной группы  $\mathfrak{G}$ , то

$$\lambda_{H,a}(\mathfrak{g}, \mathfrak{g}') = \lambda_{H,a}(\mathfrak{g}^{-1}, \mathfrak{g}'^{-1}). \quad (10.4.14)$$

Упражнение.

Из леммы 10.4.1 вытекает, что если  $\Gamma$  — точное неприводимое представление группы  $\mathfrak{G}$  и  $H = \text{Inn}(\mathfrak{G})$ , то

$$\lambda_{H,a}(\mathfrak{g}', \mathfrak{g}) = \lambda_{H,a}(\mathfrak{g}', \mathfrak{g}) = \sqrt{2 - \frac{2\Re \text{tr } \mathfrak{g}'\mathfrak{g}^{-1}}{f}}, \quad (10.4.15)$$

т.е.  $\lambda_{H,\mathbf{a}}$  не зависит от выбора вектора  $\mathbf{a}$  на унитарной сфере  $U^{f-1}$ .

По построению вес  $w(\mathbf{g})$  элемента  $\mathbf{g} \in \mathfrak{G}$  является функцией классов сопряженных элементов, т.е.  $w(\mathbf{g}) = w(\mathbf{g}') = w_j$ , если  $\mathbf{g}, \mathbf{g}'$  принадлежат одному и тому же классу сопряженных элементов  $C_j$ .

### 10.4.5 Метрика на группе $\mathfrak{G}^n$

Метрику  $\lambda_{H,\mathbf{a}}$  на группе  $\mathfrak{G}^n$  определим с помощью соотношения

$$\lambda_{H,\mathbf{a}}(\mathbf{g}, \mathbf{g}') = \sqrt{\sum_{j=1}^n \lambda_{H,\mathbf{a}}^2(\mathbf{g}_j, \mathbf{g}'_j)}, \quad \mathbf{g} = (\mathbf{g}_1, \dots, \mathbf{g}_n), \mathbf{g}' \in \mathfrak{G}^n. \quad (10.4.16)$$

**Замечание 10.4.2** Расстояние  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$ ,  $\mathbf{g}, \mathbf{g}' \in \mathfrak{G}^n$ , равно евклидову расстоянию между точками  $\mathbf{b}_{\mathbf{g}} = (b_{\mathbf{g}_1}, \dots, b_{\mathbf{g}_n})$  и  $\mathbf{b}_{\mathbf{g}'}$ , где  $b_{\mathbf{g}_j} = \frac{1}{\sqrt{t+1}}(\mathbf{a}\Gamma(\mathbf{g}_j^{\sigma_0}), \dots, \mathbf{a}\Gamma(\mathbf{g}_j^{\sigma_t}))$ ,  $\{\sigma_0, \dots, \sigma_t\} = H$ , расположенными на сфере  $U^{ftn-1}$  радиуса  $\sqrt{n}$  в унитарном пространстве  $\mathbb{C}^{ftn}$ . Отсюда вытекает, что  $\lambda_{H,\mathbf{a}}$  действительно является метрикой на группе  $\mathfrak{G}^n$ .

Очевидно, метрика  $\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g})$  инвариантна относительно перестановки координат векторов  $(\mathbf{g}'$  и  $\mathbf{g})$ . Поэтому она является функцией классов отношений схемы  $\mathbf{C}_H(\mathfrak{G}^n)$ , т.е.  $\lambda_{H,\mathbf{a}}(\mathbf{g}, \mathbf{g}') = \hat{\lambda}_{\mathbf{c}}$ , для всех  $(\mathbf{g}, \mathbf{g}') \in R_{\mathbf{c}}$ . В частности, для нее выполнено соотношение

$$\lambda_{H,\mathbf{a}}(\mathbf{g}', \mathbf{g}) = \sqrt{\sum_{s=1}^m c_s \lambda_s^2}, \quad \mathbf{c} = (c_0, \dots, c_m), \quad (10.4.17)$$

если  $(\mathbf{g}', \mathbf{g}) \in R_{\mathbf{c}}$  (см. раздел 10.2). Собственно говоря, схема отношений  $\mathbf{C}_H(\mathfrak{G}^n)$  была определена в разделе 10.2 так, чтобы метрика  $\lambda_{H,\mathbf{a}}$  принимала постоянное значение на ее отношениях.

Следующая теорема является аналогом теоремы 10.4.1.

**Теорема 10.4.2** (Достаточное условие дистанционной регулярности метрики  $\lambda_{H,\mathbf{a}}$ )

- i Метрика  $\lambda_{H,\mathbf{a}}$  на  $\mathfrak{G}^n$  является транзитивно-инвариантной справа.
- ii Метрика  $\lambda_{H,\mathbf{a}}$  на  $\mathfrak{G}^n$  является дистанционно-регулярной, если она принимает различные значения на разных классах отношений  $R_{\mathbf{c}}$ . Другими словами, значения весов  $w_1, \dots, w_m$  элементов из  $\mathfrak{G}$ , принадлежащих классам сопряженных элементов  $C_1, \dots, C_m$ , обладают тем свойством, что если  $(c_1, \dots, c_m) \neq (c'_1, \dots, c'_m)$ , то  $c_1 w_1 + \dots + c_m w_k \neq c'_1 w_1 + \dots + c'_m w_m$ .

**Доказательство** п. i. тривиально.

Доказательство п. ii. следует из теоремы 10.4.1.  $\square$

Из теоремы непосредственно вытекает, что метрика Хемминга является транзитивно-инвариантной.

Используя теорему 10.4.2 можно доказать, что метрика  $\lambda_{H,\mathbf{a}}$  на  $\mathbb{F}_p^n$ , где  $H = \Phi_{\frac{p-1}{2}}$  и  $p = 4t - 1$ , из раздела 10.4.4 является дистанционно-регулярна. Упражнение.

Следует отметить, что условия теорем 10.4.1 и 10.4.2, обеспечивающие дистанционно-регулярность метрик  $\lambda_{H,\mathbf{a}}$ , скорее всего, далеки от необходимых. Автору известны более сложные условия достаточности, при выполнении которых метрика  $\lambda_{H,\mathbf{a}}$  является дистанционно-регулярной.

## 10.4.6 Краткий обзор результатов по схемам отношений

Опишем в начале результаты по схемам отношений, связанные с теорией кодирования. Пусть  $\mathcal{S} = \mathcal{S}(X, R_0, \dots, R_m)$  — схема отношений,  $Y \subseteq X$  — подмножество  $X$ . Положим

$$\alpha_i = \alpha_i(Y) = |Y \times Y \cap R_i|, \quad i = 0, \dots, m. \quad (10.4.18)$$

Набор целых чисел  $\alpha_{\mathcal{S}}(Y) = (\alpha_0, \dots, \alpha_m)$  называется внутренним распределением отношений схемы  $\mathcal{S}$  в коде  $Y$ . Если  $\mathcal{S} = \mathcal{H}_q^n$  — схема отношений Хемминга, то  $\alpha_{\mathcal{S}}(Y)$  — обычное распределение расстояний в коде  $Y$  (спектр кода  $Y$ ).

Мы рассматриваем обычный линейный код  $Y = \mathcal{K}$  длины  $n$  над полем  $\mathbb{F}_q$  и двойственный к нему код  $\mathcal{K}^\perp$  (см. определение (1.1.4)). В этом случае спектры  $\nu(\mathcal{K}) = \alpha_i(\mathcal{K})$  и  $\nu(\mathcal{K}^\perp)$  кодов  $\mathcal{K}$  и  $\mathcal{K}^\perp$  связаны соотношением МакВильямс (см. теорему 9.0.8).

Посмотрим на соотношение МакВильямс с несколько более общих позиций. Во-первых, естественно сначала определить пространство  $\widetilde{\mathbb{F}}_q^n$ , двойственное к пространству  $\mathbb{F}_q^n$ . Следует отметить, что пространство  $\widetilde{\mathbb{F}}_q^n$  можно определить несколькими различными способами. Мы остановимся на следующем определении. Пространством  $\widetilde{\mathbb{F}}_q^n$  является пространство над  $\mathbb{F}_q$ , порожденное всеми отображениями (некоторыми эндоморфизмами  $\mathbb{F}_q^n$  в  $\mathbb{F}_q$ ) аддитивной группы  $\mathbb{F}_q^n$  в группу  $\mathbb{F}_p$ , которые имеют вид  $\theta_{\mathbf{a}} : \mathbf{x} = (x_1, \dots, x_n) \rightarrow \langle \mathbf{a}, \mathbf{x} \rangle$ ,  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{x} \in \mathbb{F}_q^n$ , где  $\langle \mathbf{a}, \mathbf{x} \rangle$  — скалярное произведение в поле  $\mathbb{F}_q$ .

Очевидно, в рассматриваемом случае и  $q = p$  пространство  $\widetilde{\mathbb{F}}_q^n$  изоморфно пространству всех характеров аддитивной группы  $\mathbb{F}_p^n$ . Если  $\mathcal{K}$  — подпространство пространства  $\mathbb{F}_q^n$ , то двойственным кодом  $\mathcal{K}^\perp \subseteq \widetilde{\mathbb{F}}_q^n$  является код, состоящий из всех функций  $\theta_{\mathbf{a}}(\mathbf{x}) \in \widetilde{\mathbb{F}}_q^n$ , которые отображают пространство  $\mathcal{K}$  в нуль, т.е. функций тождественно равных нулю на  $\mathcal{K}$ .

Примерно ту же схему рассуждений мы реализуем и при определении пространства  $\widetilde{\mathfrak{G}}^n$ , двойственного к пространству  $\mathfrak{G}^n$  в более общем случае. По определению, пространство  $\mathfrak{G}^n$  состоит из некоторых функций, отображающих группу  $\mathfrak{G}^n$  в группу  $\mathfrak{G}$ . Групповой операцией в  $\mathfrak{G}^n$  является поточечное умножение функций  $\theta(\mathbf{x}) \in \mathfrak{G}^n$ . Таким образом,  $\theta(\mathbf{x}) \cdot \theta'(\mathbf{x}) \in \mathfrak{G}^n$ , если  $\theta(\mathbf{x}), \theta'(\mathbf{x}) \in \mathfrak{G}^n$ .

В частности, в качестве порождающих элементов  $\widetilde{\mathfrak{G}}^n$  для некоторых групп  $\mathfrak{G}$  естественно взять множество всех эндоморфизмов группы  $\mathfrak{G}^n$  в группу  $\mathfrak{G}$  и замкнуть его с помощью групповой операции в  $\widetilde{\mathfrak{G}}^n$ . Заметим, что поточечное умножение (или поточечное сложение, если сложение является групповой операцией в  $\mathfrak{G}$ ) двух функций, каждая из которых представляет собой эндоморфизм  $\mathfrak{G}^n \rightarrow \mathfrak{G}$ , не обязательно является эндоморфизмом. Поэтому в том случае, когда  $\mathfrak{G}$  — некоммутативная группа,  $\mathfrak{G}^n$  состоит не только из эндоморфизмов, но и включает в себя некоторые другие функции. Все это имеет связи с определением двойственности схем отношений по Крейну (см. [73] и др.)

Групповым (в коммутативном случае — линейным) кодом  $\mathfrak{K}$  в пространстве  $\mathfrak{G}^n$  мы назовем любую подгруппу группы  $\mathfrak{G}^n$ . Кодом  $\tilde{\mathfrak{K}}$ , двойственным к коду  $\mathfrak{K}$ , мы назовем подгруппу в двойственном пространстве  $\tilde{\mathfrak{G}}^n$ , состоящую из функций  $\theta(\mathfrak{x}) \in \tilde{\mathfrak{G}}^n$  тождественно равных единице  $\mathfrak{e} \in \mathfrak{G}$  на коде  $\mathfrak{K}$ .

Мы рассматриваем схему отношений  $\mathcal{S}_H(\mathfrak{G}^n)$ , где  $H$  — группа автоморфизмов группы  $\mathfrak{G}^n$ . Группа  $H$  некоторым естественным образом, который в данном случае мы описывать не будем, индуцирует группу автоморфизмов  $\tilde{H}$  на двойственной группе  $\tilde{\mathfrak{G}}^n$ . В результате возникает схема отношений  $\mathcal{S}_{\tilde{H}}(\tilde{\mathfrak{G}}^n)$ , которую мы называем схемой отношений, двойственной к схеме отношений  $\mathcal{S}_H(\mathfrak{G}^n)$ .

Основной результат. Если группа  $H$  автоморфизмов схемы  $\mathcal{S}_H(\mathfrak{G}^n)$  обладает некоторыми дополнительными свойствами, которые в данном месте мы приводить не будем, то внутреннее распределение  $\alpha_{\mathcal{S}}(\mathfrak{K})$  отношений схемы  $\mathcal{S}_H(\mathfrak{G}^n)$  в коде  $\mathfrak{K}$  можно выразить через внутреннее распределение отношений схемы  $\alpha_{\tilde{\mathcal{S}}}(\tilde{\mathfrak{K}})$  в двойственном коде  $\tilde{\mathfrak{K}}$ . В частности, каждую координату вектора  $\alpha_{\mathcal{S}}(\mathfrak{K})$  можно представить как явную функцию от координат вектора  $\alpha_{\tilde{\mathcal{S}}}(\tilde{\mathfrak{K}})$ , наподобие того как это сделано в соотношении (9.1.11).

Наиболее широко схемы отношений применяются в теории кодирования для вывода верхних оценок числа элементов кода. Это важное направление подробно рассмотрено в уже упомянутой работе [73] Дельсарта и в его более ранней работе [72]. На этом мы останавливаться не будем.

Много интересной информации о схемах отношений содержит книга [10].

# Глава 11

## Квантовые коды

По современным представлениям в любом квантовом вычислителе по законам квантовой механики должны постоянно происходить специфические ошибки: отдельные  $q$ –биты спонтанно меняют свое состояние на случайное. Эти ошибки ничего общего не имеют с ошибками в канале связи.

Работа квантового вычислителя невозможна без коррекции этих ошибок. Таким образом, основное предназначение квантовых кодов — коррекция ошибок в квантовом вычислителе.

Строить квантовые коды, корректирующие ошибки, можно только в рамках определенной математической модели квантовых вычислений. Таких моделей в настоящий момент несколько. Тот объект, который мы будем изучать под названием квантовый код, является достаточно давно сложившимся понятием. Вместе с тем "его право на существование" не является окончательным. В конечном итоге "правильная" модель квантового кода будет определено дальнейшим развитием физики.

Квантовые коды являются очень молодым направлением теории кодирования. Теория развивается по тому же направлению, что и теория классических кодов: оценки мощности кода, методы их построения, соотношения Мак-Вильямс и т. п. В решении этих задач получены много интересных результатов. В настоящей главе приведены только первые начальные результаты этого направления теории кодирования.

Основополагающей являются работы [81, 80, 46], в которых предложена конструкция для построения одного класса квантовых кодов (CSS-коды). В нашей интерпретации, которая несколько отлична от подхода в [47], CSS-коды определяются абелевыми подгруппами  $\mathcal{H}_L$  (CSS-подгруппами) экстраспециальной 2–группы  $\mathcal{E}^{\otimes n}$  порядка  $2^{2m+1}$ , у которых подпространство  $L$  пространства  $\mathbb{F}_2^n$  является самоортогональным. С помощью CSS-подгрупп в [81, 80, 46, 47] строятся CSS-коды. Для CSS-кодов достаточно просто сформулировать на привычном языке классической теории кодирования необходимые и достаточные условия того, чтобы CSS-код имел кодовое расстояние  $\geq d$ . В интересной работе [47] предложены некоторые конструкции, основанные на использовании кодов над  $\mathbb{Z}/4\mathbb{Z}$ , для построения CSS-кодов. Некоторые последующие работы также развивают это направление исследований.

В этой главе рассматриваются более широкий, чем упомянутый выше, класс квантовых кодов, который также, как в указанных работах, связан с экстраспециальной группой. Эти коды  $Q_L(\Gamma)$  определяются множествами векторов  $\Gamma \subset \{(L^\perp)^c \times L^c\}$ , где  $L$  — произвольное подпространство пространства  $\mathbb{F}_2^n$  и  $L^c$  — подпространство дополнительное

к  $L$ , т.е. для него справедливо  $\mathbb{F}_2^n = L \oplus L^\perp$ . Для кодов этого класса базисными векторами являются векторы из множества  $\{e_L^{\alpha,\beta}; \alpha, \beta \in \Gamma\}$ , где  $e_L^{\alpha,\beta}$  — собственный вектор (базисный вектор одномерного инвариантного подпространства) максимальной абелевой матричной подгруппы  $\mathcal{H}_L$  экстраспециальной группы  $\mathcal{E}^{\otimes n}$ . Заметим, что  $\mathcal{H}_L$  является CSS-подгруппой только, если  $L^\perp \subset L$ , и, кроме того, в качестве базисных векторов CSS-кода берутся только собственные векторы вида  $e_L^{\alpha,0}$ .

В главе для квантового кода  $Q_L(\Gamma)$  указаны необходимые и достаточные условия, обеспечивающие ему кодовое расстояние  $\geq$  (теорема 11.0.3). CSS-коды являются частным классом наших кодов (см. следствия 11.0.1, 11.0.2).

В § 5 построено некоторое множество различных квантовых кодов Хэмминга длины  $n = 2^m$  (коды на  $n$   $q$ -битах) и размерности  $K = 2^{n-m-2}$ , исправляющие одну ошибку. Размерность этих кодов отличается от максимально возможной не более, чем в  $\frac{4}{3}$  раз. Эти коды не являются CSS-кодами. Мотивация, по которой эти коды названы кодами Хэмминга, состоит в том, что, во-первых, их параметры (длина и число исправляемых ошибок) очень похожи на параметры обычного двоичного кода Хэмминга. Во-вторых, при их построении, по существу, используется обычный код Хэмминга, расширенный проверкой на четность.

Отметим, что в работе [62] построен квантовый код длины  $n = 8$  и размерности  $K = 2^3 = 2^{8-3-2}$ , исправляющий одну ошибку. Там же высказаны соображения о возможности построения квантового кода, исправляющего одну ошибку, с параметрами такими же, как у кода Хэмминга настоящей статьи. Эти коды, также названные "квантовыми кодами Хэмминга", не являются кодами, построенными в настоящей статье. На взгляд автора, кроме указанных результатов работы [62] в ней, по-видимому, впервые предложено использовать абелевы подгруппы экстраспециальной группы для построения квантовых кодов. Следует сказать, что математический аппарат и методы построения кодов работы [62] и настоящей статьи существенно различаются.

## 11.0.7 Определения

**Определение 11.0.4** *Квантовым кодом  $\mathcal{C}$  размерности  $K$  называется произвольное  $K$ -мерное подпространство  $2^n$ -мерного унитарного пространства  $V = \mathbb{C}^{2^n}$ . В этом случае говорят, что код построен на  $n$   $q$ -битах. Число  $n$  также называют длиной кода.*

Координаты пространства  $V$  будем индексировать элементами двоичного  $n$ -мерного пространства  $\mathbb{F}_2^n$ . Обозначим через  $\{e_\alpha | \alpha \in \mathbb{F}_2^n\}$  стандартный ортогональный базис пространства  $V$ , т.е.  $e_\alpha = (0, \dots, 0, 1, 0, \dots, 0)$ , где 1 находится на месте, индексированном элементом  $\alpha$ .

Рассмотрим множество матриц

$$\left\{ I_2 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \pm \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}. \quad (11.0.1)$$

Эти матрицы называются матрицами Паули.



Значком  $\otimes$  будем обозначать тензорное произведение матриц. Например, произведением двух  $2 \times 2$ –матриц является  $4 \times 4$ –матрицей

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} & b \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \\ c \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} & d \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \end{pmatrix}. \quad (11.0.2)$$

В общем случае тензорным произведением  $n \times m$ –матрицы и  $n' \times m'$ –матрицы является  $nn' \times mm'$ –матрица. В частности, тензорным произведением двух векторов длины  $n$  и  $n'$  является вектор длины  $nn'$ .

По определению, ошибкой или иначе оператором ошибки называется оператор вида

$$U = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n, \quad (11.0.3)$$

действующий на пространстве  $V$ , где каждая  $(2 \times 2)$ –матрица  $\sigma_i$  является одной из матриц Паули.

Оператор  $U$  будем называть оператором, порожденным не более чем  $d-1$  ошибками (обозначение  $U_{d-1}$ ), если в произведении (11.0.3) не более, чем  $d-1$  сомножителей (часто называемых  $q$ –битами) принимают значение из множества  $\{\pm\sigma_x, \pm\sigma_y, \pm\sigma_z, \}$ .

Мы будем изредка использовать физическими обозначениями. В частности, через  $\langle \mathbf{v} | U | \mathbf{w} \rangle$ ,  $\mathbf{w}, \mathbf{v} \in V$ , обозначается билинейная форма  $\mathbf{v} U \mathbf{w}^T$ .

Известно несколько эквивалентных определений кодового расстояния квантового кода.

**Определение 11.0.5** Код  $\mathcal{C}$  имеет кодовое расстояние по меньшей мере  $d$ , если и только если

$$\langle \mathbf{v} | U_{d-1} | \mathbf{w} \rangle = 0 \quad (11.0.4)$$

для всех ортогональных векторов  $\mathbf{v}$  и  $\mathbf{w}$  из  $\mathcal{C}$  и всех операторов  $U_{d-1}$ , порожденных ошибками не более чем в  $d-1$   $q$ –битах.

Таким образом, любые два ортогональных вектора кода  $\mathcal{C}$  с кодовым расстоянием  $d$  остаются ортогональными и после того, как один из них исказится не более, чем в  $d-1$   $q$ –битах.

**Определение 11.0.6** Код  $\mathcal{C}$  имеет кодовое расстояние, по меньшей мере  $d$ , если и только если

$$\langle \mathbf{v} | U_{d-1} | \mathbf{v} \rangle = \langle \mathbf{w} | U_{d-1} | \mathbf{w} \rangle \quad (11.0.5)$$

для всех ортогональных векторов  $\mathbf{v}$  и  $\mathbf{w}$  единичной длины из  $\mathcal{C}$ , где  $U_{d-1}$  — произвольный оператор, порожденный ошибками не более чем в  $d-1$   $q$ –битах.

Равенство (11.0.5), очевидно, выполнено для всех не обязательно ортогональных векторов одинаковой длины, если оно выполнено для всех ортогональных векторов единичной длины.

Как легко видеть, что если выполнено свойство (11.0.4), то выполнено и свойство (11.0.5). Действительно, если  $\mathbf{v}$  и  $\mathbf{w}$  — два различных ортогональных вектора единичной длины, то  $\mathbf{v} - \mathbf{w}$  и  $\mathbf{v} + \mathbf{w}$  также два ортогональных вектора. Поэтому из (11.0.4) вытекает соотношение

$$0 = \langle (\mathbf{v} - \mathbf{w}) | U_{d-1} | (\mathbf{v} + \mathbf{w}) \rangle = \langle \mathbf{v} | U_{d-1} | \mathbf{v} \rangle - \langle \mathbf{w} | U_{d-1} | \mathbf{w} \rangle, \quad (11.0.6)$$

которое эквивалентно (11.0.5).

Обратно, если как и прежде  $\mathbf{v}$  и  $\mathbf{w}$  — два различных ортогональных вектора единичной длины, и выполнено (11.0.5), то векторы  $\mathbf{v} + \mathbf{w}$ ,  $\mathbf{v} - \mathbf{w}$ ,  $\mathbf{v} - i\mathbf{w}$  имеют одинаковую длину. Поэтому

$$0 = \langle (\mathbf{v} + \mathbf{w}) | U_{d-1} | (\mathbf{v} + \mathbf{w}) \rangle - \langle (\mathbf{v} - \mathbf{w}) | U_{d-1} | (\mathbf{v} - \mathbf{w}) \rangle = 2(\langle \mathbf{v} | U_{d-1} | \mathbf{w} \rangle + \langle \mathbf{w} | U_{d-1} | \mathbf{v} \rangle) \quad (11.0.7)$$

и

$$\begin{aligned} 0 &= \langle (\mathbf{v} + \mathbf{w}) | U_{d-1} | (\mathbf{v} + \mathbf{w}) \rangle - \langle (\mathbf{v} - i\mathbf{w}) | U_{d-1} | (\mathbf{v} - i\mathbf{w}) \rangle = \\ &= (1 + i)\langle \mathbf{v} | U_{d-1} | \mathbf{w} \rangle + (1 - i)\langle \mathbf{w} | U_{d-1} | \mathbf{v} \rangle. \end{aligned} \quad (11.0.8)$$

Из этих соотношений вытекает (1.1.1).

Далее будем пользоваться только определением 1.

## 11.0.8 О некоторых конечных группах порядка 8

Нам удобно вместо матриц Паули рассмотреть другие матрицы, отличающиеся от них умножением на подходящую скалярную матрицу. А именно мы будем рассматривать матрицы

$$\begin{aligned} \lambda^{(0)} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2, & \lambda^{(1)} &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i\sigma_z, \\ \lambda^{(2)} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = i\sigma_y, & \lambda^{(3)} &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i\sigma_x, \end{aligned} \quad (11.0.9)$$

Следует заметить, что множество  $Q$   $(2 \times 2)$ -матриц

$$Q = \{\pm\lambda^{(0)}, \pm\lambda^{(1)}, \pm\lambda^{(2)}, \pm\lambda^{(3)}\} \quad (11.0.10)$$

является группой порядка 8. Эта группа является точным представлением группы кватернионов (см. [15]) и ее будем называть матричной группой кватернионов. Матрицы из (11.0.9) соответствуют кватернионам  $\mathbf{1}$ ,  $\mathbf{i}$ ,  $\mathbf{j}$ ,  $\mathbf{k}$ .

Для дальнейшего следует отметить, что группа кватернионов имеет пять различных неэквивалентных представлений, четыре из которых являются одномерными и одно — двумерным. Матрицы последнего как раз и образуют множество  $Q$ . Среди одномерных мы выделим одно представление  $\psi$ , которое определяется соотношениями

$$\psi(\pm\lambda^{(0)}) = \psi(\pm\lambda^{(2)}) = 1, \quad \psi(\pm\lambda^{(1)}) = \psi(\pm\lambda^{(3)}) = -1. \quad (11.0.11)$$

Рассмотрим множество матриц с действительными коэффициентами

$$\begin{aligned} \tau^{(0)} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2, & \tau^{(1)} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\ \tau^{(2)} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \tau^{(3)} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \end{aligned} \quad (11.0.12)$$

Очевидно, матрицы  $\lambda^{(j)}$  можно записать в виде

$$\lambda^{(j)} = J^{\omega(\lambda^{(j)})} \tau^{(j)}, \quad (11.0.13)$$

где  $J = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$  — скалярная матрица, и

$$\omega(\lambda^{(j)}) = \frac{1 - \psi(\lambda^{(j)})}{2} = \begin{cases} 0 & , \text{ если } \lambda^{(j)} \text{ является матрицей с} \\ & \text{действительными элементами,} \\ 1 & \text{ в противном случае .} \end{cases}$$

Множество матриц

$$\mathcal{E} = \{\pm\tau^{(0)}, \pm\tau^{(1)}, \pm\tau^{(2)}, \pm\tau^{(3)}\} \quad (11.0.14)$$

является конечной группой порядка 8, которая носит название экстраспециальной 2- группы или диэдральной группы (вернее, ее двумерным представлением). Далее будем отождествлять экстраспециальную группу и ее матричное представление  $\mathcal{E}$ . В этом случае, для того чтобы отличить это понятие от понятия "абстрактная группа", будем иногда говорить о матричной группе  $\mathcal{E}$ .

## 11.0.9 Операторы

Если соотношение (11.0.4) выполнено для какого-либо оператора  $U_{d-1}$ , то оно выполнено и для оператора  $D \cdot U_{d-1}$ , где  $D = \text{diag}(d, \dots, d) \in U^{2^n}$ ,  $d \in \mathbb{C}$ ,  $|d| = 1$ , — скалярная матрица. Действительно, если  $\langle v | U_{d-1} | w \rangle = 0$ , то  $\langle v | D \cdot U_{d-1} | w \rangle = \bar{d} \langle v | U_{d-1} | w \rangle = 0$ , и наоборот.

Поэтому без потери общности в качестве операторов ошибок мы вместо операторов  $U$  (см. (11.0.3)) будем рассматривать операторы  $S$  вида

$$S = \tau_1 \otimes \tau_2 \otimes \dots \otimes \tau_n, \quad (11.0.15)$$

где  $\tau_i \in \mathcal{E}$ .

Отметим, что ввиду соотношения (11.0.13) в (11.0.15) матрицы  $\tau$  можно заменить матрицами  $\lambda$  и строить теорию квантовых кодов на базе матричной группы кватернионов  $Q$ . Этого мы делать не будем.

Матричную группу  $\mathcal{E}^{\otimes n}$  определим соотношением  $\mathcal{E}^{\otimes n} = \mathcal{E} \otimes \dots \otimes \mathcal{E}$  ( $n$  раз). Ее элементами являются  $(2^n \times 2^n)$ -матрицы  $S$ , определенные соотношением (11.0.15). Эта группа также носит название экстраспециальной 2-группы.

Как известно, и это легко проверить непосредственно, что для любых матриц  $S$  и  $S'$  вида (1.2.12) выполнено соотношение

$$(\tau_1 \otimes \tau_2 \otimes \dots \otimes \tau_n) \cdot (\tau'_1 \otimes \tau'_2 \otimes \dots \otimes \tau'_n) = \tau_1 \tau'_1 \otimes \tau_2 \tau'_2 \otimes \dots \otimes \tau_n \tau'_n, \quad (11.0.16)$$

т.е. множество  $\mathcal{E}^{\otimes n}$  действительно является матричной группой.

**Лемма 11.0.2 (математический фольклор)** *Группа  $\mathcal{E}^{\otimes n}$  имеет порядок  $2^{2n+1}$  и изоморфна факторгруппе  $\mathcal{G} = \mathcal{E} \times \dots \times \mathcal{E} / \mathcal{H}$ , где  $\mathcal{H} = \{\epsilon_1 I_2 \times \dots \times \epsilon_n I_2 \mid \epsilon_1 \dots \epsilon_n = 1\}$ ,  $\epsilon_i \in \{1, -1\}$ , — группа порядка  $2^{n-1}$ , которая является центром группы  $\mathcal{E}^{\otimes n}$ .*

**Доказательство.** Очевидно, что

$$\tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_n = \epsilon_1 \tau_1 \otimes \epsilon_2 \tau_2 \otimes \cdots \otimes \epsilon_n \tau_n, \text{ если } \epsilon_1 \cdots \epsilon_n = 1. \quad (11.0.17)$$

С другой стороны, если

$$\tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_n = \tau'_1 \otimes \tau'_2 \otimes \cdots \otimes \tau'_n, \quad (11.0.18)$$

то  $\tau_j = \pm \tau'_j$ . Последнее равенство легко доказать индукцией по  $n$ . Отсюда следует утверждение леммы.  $\square$

Через  $\text{wt}(S)$  будем обозначать вес оператора  $S \in \mathcal{E}^{\otimes n}$ , т.е. число не скалярных (отличных от  $\pm \tau^{(0)}$ ) сомножителей  $\tau_j$  в равенстве (11.0.15). Величина  $\text{wt}(S)$  совпадает с числом ошибок, порождаемых оператором  $S$ . Как следует из доказательства леммы 11.0.2, функция  $\text{wt}(S)$  определена корректно, т.е.

$$\text{wt}(\tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_n) = \text{wt}(\tau'_1 \otimes \tau'_2 \otimes \cdots \otimes \tau'_n), \quad (11.0.19)$$

если  $\tau_1 \otimes \tau_2 \otimes \cdots \otimes \tau_n = \tau'_1 \otimes \tau'_2 \otimes \cdots \otimes \tau'_n$ .

Пусть  $\mathbb{F}_2^n = \{\mathbf{x}_1, \dots, \mathbf{x}_{2^n}\}$  — перечень в каком-либо порядке всех векторов пространства  $\mathbb{F}_2^n$ . Рассмотрим два вида матриц  $T^{(\alpha)}$  и  $S^{(\beta)}$ ,  $\alpha, \beta \in \mathbb{F}_2^n$ , которые определены следующим образом. Матрица  $T^{(\alpha)}$  имеет вид

$$T^{(\alpha)} = \text{diag}((-1)^{(\alpha, \mathbf{x}_1)}, \dots, (-1)^{(\alpha, \mathbf{x}_{2^n})}), \quad (11.0.20)$$

а матрица  $S^{(\beta)} = (s_{\gamma, \delta})$  представляет собой подстановочную  $(2^n \times 2^n)$ -матрицу, которая соответствует сдвигу  $\mathbf{x} \rightarrow \mathbf{x} + \beta$  в пространстве  $\mathbb{F}_2^n$  на элемент  $\beta$ , т.е.  $s_{\gamma, \delta} = 1$ , если  $\gamma = \delta + \beta$ , и  $s_{\gamma, \delta} = 0$  в противном случае.

Матрицы  $T^{(\alpha)}$ ,  $S^{(\beta)}$  (при соответствующей нумерации элементов  $\mathbb{F}_2^n$ ) принадлежат группе  $\mathcal{E}^{\otimes n}$ . Проверить это проще всего, если заметить, что

$$T^{(\alpha)} = (\tau^{(1)})^{\alpha_1} \otimes (\tau^{(1)})^{\alpha_2} \otimes \cdots \otimes (\tau^{(1)})^{\alpha_n} \quad (11.0.21)$$

и

$$S^{(\beta)} = (\tau^{(3)})^{\beta_1} \otimes (\tau^{(3)})^{\beta_2} \otimes \cdots \otimes (\tau^{(3)})^{\beta_n} \quad (11.0.22)$$

Кроме того, легко проверить, что

$$T^{(\alpha)} S^{(\beta)} = (-1)^{(\alpha, \beta)} S^{(\beta)} T^{(\alpha)}, \quad (11.0.23)$$

где  $(\alpha, \beta)$  — скалярное произведение векторов  $\alpha$  и  $\beta$  в поле  $\mathbb{F}_2^n$ .

Легко также видеть, что  $\mathcal{E}^{\otimes n}$  является некоммутативной матричной группой, порожденной матрицами  $T^{(\alpha)}$  и  $S^{(\beta)}$  с законом умножения (11.0.23), т.е.  $\mathcal{E}^{\otimes n} = \langle T^{(\alpha)}, S^{(\beta)} | \alpha, \beta \in \mathbb{F}_2^n \rangle$ .

Если  $S = \pm T^{(\alpha)} \cdot S^{(\beta)}$ , то, как нетрудно проверить,  $\text{wt}(S) = \text{wt}(\alpha \vee \beta)$ , где  $\text{wt}(\gamma)$  — вес Хемминга вектора  $\gamma$ , и  $\alpha \vee \beta = (\alpha_1 \vee \beta_1, \dots, \alpha_n \vee \beta_n)$ .

Рассмотрим действие оператора  $S = T^{(\alpha)} S^{(\beta)}$  на  $2^n$ -мерном пространстве  $V$ . Пусть  $\mathbf{e}_\gamma = (0, \dots, 0, 1, 0, \dots, 0)$ ,  $\gamma \in \mathbb{F}_2^n$ , (единичная координата имеет индекс  $\gamma$ ) — базисный вектор пространства  $V$ . Нетрудно убедиться, что

$$\mathbf{e}_\gamma S = \mathbf{e}_\gamma T^{(\alpha)} S^{(\beta)} = (-1)^{(\gamma, \alpha)} \mathbf{e}_{\gamma + \beta}. \quad (11.0.24)$$

### 11.0.10 Квантовые коды, образованные собственными векторами коммутативной подгруппы $\mathcal{H}_L$ группы $\mathcal{E}^{\otimes n}$

Рассмотрим коммутативную подгруппу  $\mathcal{H}$  группы  $\mathcal{E}^{\otimes n}$ . Легко установить, используя соотношение (11.0.23), что  $\mathcal{H}$  является подгруппой некоторой коммутативной группы вида  $\mathcal{H}_L = \{T^\alpha \cdot S^\beta | \alpha \in L^\perp, \beta \in L\}$ ,  $|\mathcal{H}_L| = 2^n$ , где  $L$  — подпространство размерности  $k$  пространства  $\mathbb{F}_2^n$ . Абелеву группу  $\mathcal{H}_L$  будем называть правильной.

Как нетрудно увидеть (см. (11.0.23)), что если  $P \in \mathcal{E}^{\otimes n}$ , но  $P \notin \mathcal{H}_L$ , то группа  $\langle \mathcal{H}_L, P \rangle$  будет уже некоммутативной. Таким образом, группы вида  $\mathcal{H}_L$  можно рассматривать как максимальные коммутативные подгруппы  $\mathcal{E}^{\otimes n}$ .

Через  $L^c$ ,  $\dim L^c = n - k$ , обозначим одно из пространств, дополняющих  $L$  до  $\mathbb{F}_2^n$ , т.е.  $L^c$  — подпространство такое, что  $\mathbb{F}_2^n = L \oplus L^c$ . Отметим, что  $(L^c)^c = L$ .

Обозначим через  $L^d = (L^\perp)^c$ ,  $\dim L^d = k$ , — одно из подпространств, для которого  $L^d \cap L^\perp = \mathbf{0}$ . По-другому,  $L^d$  — подпространство, для которого линейная функция  $(\beta, \mathbf{x})$ ,  $\mathbf{x} \in L$ , рассматриваемая на  $L$ , отлична от нулевой для всех  $\beta \in L^d \setminus \{\mathbf{0}\}$ . Отметим, что  $(L^d)^d = L$ .

Построить  $L^d$  можно следующим образом. Пусть  $L = L_k D$ , где  $L_k = \{(\alpha_1, \dots, \alpha_k, 0, \dots, 0) | \alpha_j \in \mathbb{F}_2\}$  — подпространство пространства  $\mathbb{F}_2^n$  и  $D$  — невырожденная матрица перехода от  $L_k$  к  $L$ . Тогда можно положить  $L^d = L_k (D^T)^{-1}$ , ибо в этом случае функцию  $(\beta, \mathbf{x})$  можно представить в виде  $(\beta, \mathbf{x}) = (\beta' (D^T)^{-1}, \mathbf{x}' D) = \beta'_1 x'_1 + \dots + \beta'_k x'_k$ . Последняя функция является ненулевой на  $L$  при всех ненулевых  $\beta \in L$ .

Пусть  $L$  — подпространство пространства  $\mathbb{F}_2^n$ . Рассмотрим вектор  $\mathbf{e}_L^{l,\tau}$ ,  $l, \tau \in \mathbb{F}_2^n$ , определяемый соотношением

$$\mathbf{e}_L^{l,\tau} = \sum_{\gamma \in L} (-1)^{(l,\gamma)} \mathbf{e}_{\gamma+\tau}, \quad (11.0.25)$$

и одномерное пространство  $L^{l,\tau} \subset \mathbb{R}^{2^n}$  ( $2^n$ -мерное евклидово пространство), базисом которого является этот вектор.

Отметим, что из (11.0.24) вытекает

$$\mathbf{e}_L^{l,\tau} = (-1)^{(\beta,l)} \mathbf{e}_L^{l+\alpha,\tau+\beta}, \quad (11.0.26)$$

если  $\beta \in L$  и  $\alpha \in L^\perp$ . Вместе с тем векторы  $\mathbf{e}_L^{l,\tau}$ ,  $\mathbf{e}_L^{l',\tau'}$ , где  $\tau, \tau' \in L^c$ ,  $l, l' \in (L^\perp)^c$ , не пропорциональны, если  $(l, \tau) \neq (l', \tau')$ . Поэтому число различных подпространств  $L^{l,\tau}$  равно  $2^n$ .

**Лемма 11.0.3** *Пространства  $L^{l,\tau}$ ,  $l, \tau \in \mathbb{F}_2^n$ , являются одномерными инвариантными подпространствами матричной группы  $\mathcal{H}_L$ .*

**Доказательство.** Пусть  $S = T^\alpha S^\beta \in \mathcal{H}_L$ , т.е.  $\alpha \in L^\perp, \beta \in L$ . Тогда из (11.0.24) и (11.0.26) следует

$$\mathbf{e}_L^{l,\tau} S = \sum_{\gamma \in L} (-1)^{(l+\alpha,\gamma)} \mathbf{e}_{\gamma+\beta+\tau} = \sum_{\gamma \in L} (-1)^{(l+\alpha,\gamma+\beta)} \mathbf{e}_{\gamma+\tau} = (-1)^{(l,\beta)} \mathbf{e}_L^{l,\tau}, \quad (11.0.27)$$

т.е. все пространства  $L^{l,\tau}$  являются инвариантными.  $\square$

Как было замечено выше, число различных подпространств  $L^{l,\tau}$  равно  $2^n$ , поэтому они исчерпывают все одномерные инвариантные подпространства группы  $\mathcal{H}_L$ . Кроме того, хорошо известно, что функция  $\varphi^{l,\tau}(S)$ ,  $S \in \mathcal{H}_L$ , определяемая соотношением  $e^{l,\tau}S = \varphi^{l,\tau}(S)e^{l,\tau}$ , является характером группы  $\mathcal{H}_L$  (ее одномерным представлением).

Рассмотрим квантовый код  $Q_L(\Gamma)$ , т.е. подпространство  $2^n$ -мерного пространства  $V$ , базисом которого является множество векторов  $\{e_L^{l,\beta} | (l,\beta) \in \Gamma\}$ , где  $\Gamma$  — некоторое подмножество множества  $(L^\perp)^c \times L^c$ . Таким образом, мы рассматриваем только коды, у которых базисными векторами являются некоторые векторы вида  $e_L^{l,\beta}$ , где  $L$  — фиксированное подпространство пространства  $\mathbb{F}_2^n$ .

Пусть  $U_{d-1} = T^{(\tau)}S^{(\tau')}$  — произвольный оператор, порожденный ошибками не более чем в  $d-1$   $q$ -битах, т.е.  $\text{wt}(\tau \vee \tau') < d$ .

Очевидно,

$$e_L^{l,\beta}U_{d-1} = \sum_{\gamma \in L} (-1)^{(l+\tau, \gamma)} e_{\gamma+\beta+\tau'} = e_L^{l+\tau, \beta+\tau'}. \quad (11.0.28)$$

Два вектора  $e_L^{l,\beta}$  и  $e_L^{l',\beta'}$ ,  $l, l' \in (L^\perp)^c$ ,  $\beta', \beta \in L^c$ , ортогональны, если  $(l, \beta) \neq (l', \beta')$ . Это следует из того, что

различные собственные векторы коммутативной матричной группы  $\mathcal{H}_L$  ортогональны. Впрочем, это утверждение легко проверить и непосредственно. Следующая лемма является уточнением этого утверждения.

Будем писать  $\beta' \not\equiv \beta \pmod L$ , если  $\beta' \neq \beta + \alpha$  при всех  $\alpha \in L$ . Если  $\beta' = \beta + \alpha$  при некотором  $\alpha \in L$ , то пишем  $\beta' \equiv \beta \pmod L$ .

**Лемма 11.0.4** *Два вектора  $e_L^{l',\beta'}$  и  $e_L^{l,\beta}$  являются ортогональными тогда и только тогда, когда выполнено, по крайней мере, одно из следующих двух соотношений*

$$l' \not\equiv l \pmod{L^\perp}, \quad \beta \not\equiv \beta' \pmod L. \quad (11.0.29)$$

Если  $l' \equiv l \pmod{L^\perp}$  и  $\beta \equiv \beta' \pmod L$ , то векторы  $e_L^{l',\beta'}$  и  $e_L^{l,\beta}$  являются пропорциональными.

Лемма следует из того, что векторы  $e_L^{l',\beta'}$  и  $e_L^{l,\beta}$  являются собственными матричной группы  $\mathcal{H}_L$  и потому ортогональными, если одномерные подпространства  $L^{l',\beta'}$  и  $L^{l,\beta}$ , базисами которых являются эти векторы, различны. Как следует из определения  $e_L^{l,\beta}$  (см. (11.0.25) и (11.0.26)), векторы  $e_L^{l',\beta'}$  и  $e_L^{l,\beta}$  являются не пропорциональными, если выполнено одно из соотношений в (11.0.29).  $\square$

**Теорема 11.0.3** *Квантовый код  $Q_L(\Gamma)$ ,  $\Gamma \subseteq (L^\perp)^c \times L^c$ , имеет кодовое расстояние не меньше  $d$  тогда и только тогда, когда для любых двух векторов  $\tau, \tau'$ , таких что  $\text{wt}(\tau \vee \tau') < d$ , и любых двух различных векторов  $(l, \beta)$  и  $(l', \beta')$  из  $\Gamma$  выполнено по меньшей мере одно из следующих двух соотношений*

$$i. \quad \beta + \beta' + \tau' \not\equiv 0 \pmod L ;$$

$$ii. \quad l' + l + \tau \not\equiv 0 \pmod{L^\perp}.$$

**Доказательство.** Как следует из определения 11.0.5, нам достаточно показать, что для любого не единичного оператора  $U_{d-1} = T^\tau S^{\tau'}$  вектор  $e_L^{l,\beta} U_{d-1} = e_L^{l+\tau, \beta+\tau'}$  (см. (11.0.28)) ортогонален вектору  $e_L^{l',\beta'}$ , где  $(l', \beta') \in \Gamma$ , если выполнено по крайней мере одно из условий i. или ii.. Это утверждение вытекает из леммы 11.0.4.

Предположим теперь, что  $\beta + \beta' + \tau' \equiv 0 \pmod L$  и  $l' + l + \tau \equiv 0 \pmod L^\perp$ . В этом случае, как следует из (11.0.26), мы имеем  $e_L^{l,\beta} U_{d-1} = e_L^{l+\tau, \beta+\tau'} = \pm e_L^{l',\beta'}$ , т.е. соотношение 11.0.5 не выполнено для двух векторов  $e_L^{l,\beta}$ ,  $e_L^{l',\beta'}$ .  $\square$

**Следствие 11.0.1** Пусть подпространство  $L$  пространства  $\mathbb{F}_2^n$  является кодом с кодовым расстоянием  $\geq d$  и пусть  $F$  — подмножество пространства  $(L^\perp)^c$ . Тогда квантовый код  $Q_L(\Gamma)$ , где  $\Gamma = F \times \mathbf{0}$ , имеет кодовое расстояние не меньше  $d$ , если и только если  $f + f' + \tau \not\equiv 0 \pmod L^\perp$  для любых двух различных  $f$  и  $f'$  из  $F$  и любого  $\tau$  веса  $\text{wt}(\tau) < d$ . В частности, если  $F$  — линейное подпространство пространства  $(L^\perp)^c$ , то код  $Q_L(\Gamma)$  является кодом с кодовым расстоянием не меньше  $d$  тогда и только тогда, когда  $f + \tau \not\equiv 0 \pmod L^\perp$  для любого ненулевого  $f \in F$  и любого  $\tau$  веса  $\text{wt}(\tau) < d$ . Другими словами, код  $Q_L(\Gamma)$  имеет кодовое расстояние  $\geq d$ , если расстояние Хемминга  $d(F \setminus \{0\}, L^\perp)$  между множествами  $F \setminus \{0\}$  и  $L^\perp$  не меньше  $d$ .

Предположим, что  $L^\perp \subset L$ . Рассмотрим подкод  $\tilde{L}$  кода  $L$  максимальной размерности, для которого  $\tilde{L} \cap L^\perp = \{0\}$ . По другому,  $\tilde{L}$  — дополнение  $L^\perp$  в пространстве  $L$ , т.е. для него справедливо соотношение  $L = L^\perp \oplus \tilde{L}$ .

Отметим, что если  $L$  — код с кодовым расстоянием не меньше  $d$ , то  $d(\tilde{L} \setminus \{0\}, L^\perp) \geq d$ . Отсюда вытекает

**Следствие 11.0.2 (CSS-коды, [81, 80, 47])** Если в условиях следствия 1  $L^\perp \subset L$  и в качестве множества  $F$  взять код  $\tilde{L}$ , то квантовый код  $Q_L(\Gamma)$ , где  $\Gamma = \tilde{L} \times \mathbf{0}$ , будет иметь кодовое расстояние не меньше  $d = d(L)$  и число элементов  $|\tilde{L}| = \frac{|L|^2}{2^n}$ . По-другому, размерность кода  $Q_L(\Gamma)$  равна  $\dim L - \dim L^\perp = n - 2l$ , где  $l = n - k$  — избыточность кода  $L$ .

Следует сказать, что квантовый код  $Q_L(\Gamma)$  из следствия 2 обнаруживает все ошибки  $U_{d-1} = T^{(\tau)} S^{(\tau')}$  (т.е. для них выполняется соотношение (11.0.4), у которых  $\text{wt}(\tau) < d$  и  $\text{wt}(\tau') < d$ . В то же время требования на  $U_{d-1}$  для кода с кодовым расстоянием  $d$  слабее:  $\text{wt}(\tau \vee \tau') < d$ , т.е. этот код обнаруживает большее число комплектов ошибок, чем это требуется.

Далее мы приведем пример кода Хэмминга, который строится более сложными методами по сравнению с кодами из следствий 11.0.1, 11.0.2, т.е. кода, у которого множество  $\Gamma$  не имеет вида  $\Gamma = \tilde{L} \times \mathbf{0}$ .

### 11.0.11 Квантовый "код Хэмминга" длины $n = 2^m$

Рассмотрим расширенный линейный код Хэмминга  $C^H$  с проверкой на четность длины  $n = 2^m$  с кодовым расстоянием 4 (см. конец раздела 1.1.3) и размерностью  $k = 2^m - 1 - m$  и линейный код  $C^{ch}$  длины  $n$  с кодовым расстоянием 2 и размерностью  $k' = 2^m - 1$ . Этот код состоит из всех двоичных векторов четного веса.

Пусть  $M = \{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subset \mathbb{F}_2^n$  — множество всех векторов веса 1 и  $\mathbf{y}$  — какой-либо фиксированный элемент множества  $M$ . Очевидно, код  $C^{ch}$  можно представить в виде объединения смежных классов кода  $C^H$ :

$$C^{ch} = \bigcup_{\mathbf{x} \in M} (C^H + \mathbf{x} + \mathbf{y}). \quad (11.0.30)$$

Имея в виду (11.0.30), множество  $M$  будем рассматривать как элементарную 2-группу, в которой групповой операцией  $\dot{+}$  является операция сложения по  $\text{mod } C^H$ , т.е.  $\mathbf{x} \dot{+} \mathbf{x}' = \mathbf{z}$ , если  $\mathbf{x} + \mathbf{y} + \mathbf{x}' + \mathbf{y} + \mathbf{z} + \mathbf{y} \equiv \mathbf{0} \text{ mod } C^H$ . Поясним все это несколько иным способом.

Будем индексировать координаты векторов из  $\mathbb{F}_2^n$ ,  $n = 2^m$ , элементами поля  $\mathbb{F}_{2^m} = \{\alpha_1, \dots, \alpha_n\}$ . Вектор  $\mathbf{a} = (a_{\alpha_1}, \dots, a_{\alpha_n})$ ,  $a_{\alpha_j} \in \mathbb{F}_2$ , принадлежит коду  $C^H$  тогда и только тогда, когда  $a_{\alpha_1}\alpha_1 + \dots + a_{\alpha_n}\alpha_n = 0$  и  $a_{\alpha_1} + \dots + a_{\alpha_n} = 0$ . Пусть  $\mathbf{a}_\alpha$  — вектор из  $M$ , у которого единичная координата имеет номер  $\alpha$ . Будем полагать, что  $\mathbf{a}_0 = \mathbf{y}$ .

Положим  $\mathbf{a}_\alpha \dot{+} \mathbf{a}_\beta = \mathbf{a}_\gamma$ , если  $\mathbf{a}_\alpha + \mathbf{y} + \mathbf{a}_\beta + \mathbf{y} + \mathbf{a}_\gamma + \mathbf{y} \in C^H$ , т.е. если  $\mathbf{a}_\alpha + \mathbf{y} + \mathbf{a}_\beta + \mathbf{y} + \mathbf{a}_\gamma + \mathbf{y} \equiv \mathbf{0} \text{ mod } C^H$ . При нашем выборе вектора  $\mathbf{y}$ , очевидно, индексы  $\alpha, \beta, \gamma$  связаны соотношением  $\alpha + \beta + \gamma = \mathbf{0}$ . Таким образом, множество  $M$  можно рассматривать как элементарную 2-группу с групповой операцией  $\dot{+}$ .

Обозначим через  $\theta$  изоморфное отображение аддитивной группы поля  $\mathbb{F}_{2^m}$  в группу  $M$ . Умножение  $\dot{\times}$  на  $M$  определим следующим образом:  $\mathbf{x} \dot{\times} \mathbf{y} = \theta(\theta^{-1}(\mathbf{x}) \cdot \theta^{-1}(\mathbf{y}))$ , где  $\cdot$  — умножение в поле  $\mathbb{F}_{2^m}$ . Итак, множество  $M$  можно рассматривать как конечное поле с операциями  $\dot{\times}$  и  $\dot{+}$ , при этом операция  $\dot{+}$  выполняется по  $\text{mod } C^H$ .

Переходим к построению квантового кода Хэмминга  $Q_L(\Gamma)$ . В качестве множества  $L$  возьмем код  $L = C^H$ . Отметим, что  $(C^H)^\perp \subset C^H$ ,  $L = (C^H)^\perp \oplus \tilde{L}$ , и следовательно  $\dim \tilde{L} = 2^m - 2m - 2$ .

Пусть  $\mathbf{z}$  — вектор из  $M$ , для которого  $\theta^{-1}(\mathbf{z}) \neq 0, 1 \in \mathbb{F}_{2^m}$ . Положим

$$\Gamma = \Gamma(\mathbf{z}) = \bigcup_{\mathbf{x} \in M} \{(\tilde{L} + \mathbf{z} \dot{\times} \mathbf{x}) \times (\mathbf{x} + \mathbf{y})\}. \quad (11.0.31)$$

**Теорема 2.** Код  $Q_L(\Gamma(\mathbf{z}))$  длины  $n = 2^m$  имеет кодовое расстояние 3 и размерность  $\frac{2^n}{4n}$ .

**Доказательство.** Пусть  $\tau, \tau' \in \mathbb{F}_2^n$ ,  $\text{wt}(\tau \vee \tau') \leq 2$ , — векторы, определяющие оператор ошибок  $U_2$ , и  $(l + \mathbf{z} \dot{\times} \mathbf{x}_i, \mathbf{x}_i + \mathbf{y}), (l' + \mathbf{z} \dot{\times} \mathbf{x}_j, \mathbf{x}_j + \mathbf{y})$ ,  $\mathbf{x}_i, \mathbf{x}_j \in M$ , — два различных элемента множества  $\Gamma$ . Ввиду теоремы 1 для доказательства достаточно показать, что выполнено, по крайней мере, одно из следующих двух соотношений:  $\mathbf{x}_i + \mathbf{x}_j + \tau' \notin L$  или  $l + l' + \mathbf{z} \dot{\times} \mathbf{x}_i + \mathbf{z} \dot{\times} \mathbf{x}_j + \tau \notin L$ , ибо  $L = \tilde{L} + L^\perp$ .

Случай 1.  $\tau' = \mathbf{0}$ ,  $0 < \text{wt}(\tau) \leq 2$ . В этом случае  $(\mathbf{x}_i + \mathbf{y}) + (\mathbf{x}_j + \mathbf{y}) \in L$  тогда и только тогда, когда  $\mathbf{x}_i = \mathbf{x}_j$ . Поэтому условие  $l + l' + \tau \notin L$ , очевидно, выполнено для всех  $\tau$  веса меньше чем 4, ибо в этом случае  $l + l' \neq \mathbf{0}$ , а кодовое расстояние кода  $L$  равно 4.

Случай 2.  $\text{wt}(\tau') = 1$ . В этом случае  $(\mathbf{x}_j + \mathbf{y}) + (\mathbf{x}_i + \mathbf{y}) + \tau' \notin L$ , ибо пространство  $L$  содержит векторы только четного веса, а вес вектора  $(\mathbf{x}_j + \mathbf{y}) + (\mathbf{x}_i + \mathbf{y}) + \tau'$  нечетен.

Случай 3а.  $\text{wt}(\tau') = 2$ ,  $\text{wt}(\tau) = 2$ . Пусть  $\mathbf{x}_i + \mathbf{x}_j + \tau' \in L$  и  $(l + \mathbf{z} \dot{\times} \mathbf{x}_i, \mathbf{x}_i + \mathbf{y}), (l' + \mathbf{z} \dot{\times} \mathbf{x}_j, \mathbf{x}_j + \mathbf{y})$  — два различных элемента множества  $\Gamma$ . В рассматриваемом случае всегда  $\mathbf{x}_j \neq \mathbf{x}_i$ , и условие  $\text{wt}(\tau \vee \tau') \leq 2$  выполняется только если  $\tau = \tau'$ . Поэтому нам надо показать, что векторы  $l + l' + \mathbf{z} \dot{\times} \mathbf{x}_i + \mathbf{x}_i + \mathbf{z} \dot{\times} \mathbf{x}_j + \mathbf{x}_j \equiv (\mathbf{z} \dot{+} \mathbf{z}') \dot{\times} \mathbf{x}_i + (\mathbf{z} \dot{+} \mathbf{z}') \dot{\times} \mathbf{x}_j \text{ mod } L$  не принадлежит  $L$ , где вектор  $\mathbf{z}' \in M$  определен условием  $\theta^{-1}(\mathbf{z}') = 1 \in \mathbb{F}_2^m$ .



Последнее утверждение вытекает из того, что векторы  $((z+z')\dot{x}_i$  и  $(z+z')\dot{x}_j$  веса 1 различны и потому  $(z+z')\dot{x}_i + (z+z')\dot{x}_j \not\equiv 0 \pmod L$ , ибо  $L$  — код с кодовым расстоянием 4, а  $\text{wt}((z+z')\dot{x}_i + (z+z')\dot{x}_j) = 2$ .

Случай 3б.  $\text{wt}(\tau') = 2, \text{wt}(\tau) = 1$ . В обозначениях случая 3а соотношение  $l+l'+z\dot{x}_i + z\dot{x}_j + \tau \in L$  не выполнено, ибо вес вектора  $l+l'+z\dot{x}_i + z\dot{x}_j + \tau$  является нечетным числом, а пространство  $L$  содержит только векторы четного веса.

Случай 3в.  $\text{wt}(\tau') = 2, \text{wt}(\tau) = 0$ . В обозначениях случая 3а имеет место соотношение  $l+l'+z\dot{x}_i + z\dot{x}_j \not\equiv 0 \pmod L$ , ибо  $x_j \neq x_i$  и поэтому  $\text{wt}(z\dot{x}_i + z\dot{x}_j) = 2$ .

Утверждение теоремы о размерности кода  $Q_L(\Gamma)$  очевидно. ■

Семейство кодов  $Q_L(\Gamma(z))$ ,  $\theta^{-1}(z) \neq 0, 1 \in \mathbb{F}_{2^m}$ , содержит  $2^m - 2$  элементов.

Построенный код  $Q_L(\Gamma)$  будем называть квантовым кодом Хэмминга. Как известно [62], верхняя оценка размерности  $K$  невырожденного квантового кода пространстве  $n$   $q$ -битов с кодовым расстоянием  $d = 2t + 1$  имеет вид

$$K \sum_{j=0}^t 3^j \binom{n}{j} \leq 2^n. \quad (11.0.32)$$

Таким образом, размерность квантового кода Хэмминга отличается от максимально возможного значения менее, чем в  $\frac{4}{3}$  раза.

Следует сказать, что в работе [47] иными методами построены коды Хэмминга с параметрами  $n = \frac{4^m - 1}{3}$ ,  $k = 2m$ ,  $d = 3$ , которые также "почти" лежат на границе (11.0.32).

### 11.0.12 Квантовый код с кодовым расстоянием 5

В настоящем разделе рассматривается метод построения одного нового семейства квантовых кодов длины  $n = 2^m$  с кодовым расстоянием не менее, чем 5. Рассматриваемый класс кодов являются более широким, чем класс кодов, построенный в работах [81, 80, 46, 47] (CSS-коды). Размерность  $K = 2^m - 3m - 3$  построенных кодов выше, чем размерность  $K = 2^m - 4m - 2$  наилучших CSS-кодов, но ниже, чем известная верхняя оценка  $K \leq 2^m - 2m + \text{const}$  размерности квантовых кодов с кодовым расстоянием 5.

Рассмотрим двоичный линейный код Боуза-Чоудхури-Хоквингема  $C_6$  с проверкой на четность длины  $n = 2^m$  с кодовым расстоянием 6 и размерностью  $k = 2^m - 1 - 2m$ . Проверочная матрица  $B$  кода  $C_6$  имеет вид

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_N & 0 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_N^3 & 0 \end{pmatrix}, \quad N = 2^m - 1, \alpha_j \in \mathbb{F}_{2^m} \setminus \{0\}. \quad (11.0.33)$$

Будем индексировать координаты векторов из  $\mathbb{F}_2^n$ ,  $n = 2^m$ , элементами поля  $\mathbb{F}_{2^m} = \{\alpha_1, \dots, \alpha_n\}$ . Через  $x_\alpha$  обозначим вектор из пространства  $\mathbb{F}_2^n$ ,  $n = 2^m$ , у которого координата с номером  $\alpha$  равна 1, а остальные его координаты равны 0.

Пусть  $M_0 = \{x_\alpha + x_{\alpha+1} \mid \alpha \in \mathbb{F}_{2^m}\}$ . Множество  $M_0$  образовано  $2^{m-1}$  различными векторами  $z_\alpha = x_\alpha + x_{\alpha+1}$  из  $\mathbb{F}_2^n$  веса 2. Так как  $z_\alpha = z_{\alpha+1}$ , то элементы  $z_\alpha$  множества  $M_0$  будем индексировать элементами  $\alpha$ , у которых в представлении в каком-либо степенном базисе  $\{y^{m-1}, \dots, y^0\}$  поля  $\mathbb{F}_2^m$  над полем  $\mathbb{F}_2$  последняя (коэффициент при  $y^0$ ) координата равна 0.

Переходим к построению квантового кода  $Q_L(\Gamma)$  с кодовым расстоянием 5. В качестве множества  $L$  возьмем код  $L = C_6$ . Отметим, что  $(C_6)^\perp \subset C_6$ ,  $L = (C_6)^\perp \oplus \tilde{L}$ , и следовательно  $\dim \tilde{L} = 2^m - 4m - 2$ .

Положим

$$\Gamma = \bigcup_{\alpha \in M_0} \{(\tilde{L} + \mathbf{x}_\alpha) \times (\mathbf{z}_\alpha)\}. \quad (11.0.34)$$

Множество  $\Gamma$ , очевидно, имеет  $2^{m-1}|\tilde{L}| = 2^{2^m-3m-3}$  элементов.

**Теорема 11.0.4** Код  $Q_L(\Gamma)$  длины  $n = 2^m$  имеет кодовое расстояние 5 и размерность  $K = 2^m - 3m - 3$ .

**Доказательство.** Пусть  $\tau, \tau' \in \mathbb{F}_2^n$ ,  $\text{wt}(\tau \vee \tau') \leq 4$ , — векторы, определяющие оператор ошибок  $U_2$ , и  $(l + \mathbf{x}_\alpha, \mathbf{z}_\alpha), (l' + \mathbf{x}_\beta, \mathbf{z}_\beta)$ ,  $\alpha, \beta \in M_0$ , — два различных элемента множества  $\Gamma$ . Ввиду теоремы 1 для доказательства достаточно показать, что выполнено, по крайней мере, одно из следующих двух соотношений:  $\mathbf{x}_\alpha + \mathbf{x}_\beta + \tau' \notin L$  или  $l + l' + \mathbf{z}_\beta + \mathbf{z}_\alpha + \tau \notin L$ , ибо  $L = \tilde{L} + L^\perp$ .

Заметим, что  $\mathbf{x}_{\alpha_1} + \dots + \mathbf{x}_{\alpha_s} \in L$  тогда и только тогда, когда выполнены следующие соотношения  $\alpha_1 + \dots + \alpha_s = 0$ ,  $\alpha_1^3 + \dots + \alpha_s^3 = 0$ ,  $s$  — четное число.

Случай 1.  $\text{wt}(\tau') = 0$ ,  $0 < \text{wt}(\tau) \leq 4$ . В этом случае  $\mathbf{z}_\alpha + \mathbf{z}_\beta \in L$  тогда и только тогда, когда  $\mathbf{x}_\alpha = \mathbf{x}_\beta$ , т.е. тогда и только тогда, когда  $\beta = \alpha$ . Поэтому условие  $l + l' + \tau \notin L$ , очевидно, выполнено для всех  $\tau$  веса меньше, чем 5, ибо кодовое расстояние кода  $L$  равно 6.

Случай 2.  $\text{wt}(\tau') = 1, 3$ . В этом случае  $\mathbf{z}_\alpha + \mathbf{z}_\beta + \tau' \notin L$ , ибо пространство  $L$  содержит векторы только четного веса, а вес вектора  $\mathbf{x}_\alpha + \mathbf{x}_\beta + \tau'$  нечетен.

Случай 3.  $\text{wt}(\tau') = 2$ ,  $\tau' = \mathbf{x}_\gamma + \mathbf{x}_\delta$ ,  $0 \leq \text{wt}(\tau) \leq 4$ . В этом случае  $\mathbf{z}_\alpha + \mathbf{z}_\beta + \tau' \in L$  тогда и только тогда, когда  $\alpha + \alpha + 1 + \beta + \beta + 1 + \gamma + \delta = \gamma + \delta = 0$ . Последнее невозможно, ибо  $\gamma + \delta \neq 0$ .

Случай 4.  $\text{wt}(\tau') = 4$ ,  $\tau' = \mathbf{x}_{\gamma_1} + \mathbf{x}_{\gamma_2} + \mathbf{x}_{\gamma_3} + \mathbf{x}_{\gamma_4}$ ,  $\text{wt}(\tau) = 4$ . Из того, что  $\text{wt}(\tau' \vee \tau) \leq 4$  вытекает, что  $\tau' = \tau$ .

Если  $\mathbf{z}_\alpha + \mathbf{z}_\beta + \tau' \in L$ , то  $\alpha + \alpha + 1 + \beta + \beta + 1 + \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 0$ .

С другой стороны, если  $\mathbf{x}_\alpha + \mathbf{x}_\beta + \tau \in L$ , то  $\alpha + \beta + \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 0$ . Последнее невозможно, ибо  $\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 0$ , а  $\alpha + \beta \neq 0$ .

Утверждение теоремы о размерности  $K$  кода  $Q_L(\Gamma)$  очевидно. *square*

Сравним наш результат о размерности кода  $Q_L(\Gamma)$  с верхней оценкой (11.0.32). В нашем случае  $t = 2$ . Таким образом, размерность построенного кода отличается от максимально возможного значения не более, чем на  $m + \text{const}$ .

## Глава 12

# Открытые системы шифрования на основе кодов, корректирующих ошибки, и как некоторые из них можно расколоть

### 12.0.13 Введение

В настоящем разделе рассматривается система открытого шифрования, основанная на кодах Рида-Соломона, рассмотренных в разделе 5. Эта система является частным классом широко известных, так называемых, кодовых систем открытого шифрования, предложенных в 1978 г. МакЛисом, [67]. Имеется обширная литература по этому направлению, в которой авторы, так или иначе, обосновывают достаточно высокую стойкость этих структур. В настоящей главе для определенных криптосистем получен в некотором смысле противоположный результат.

Основной целью данной главы является рассказ со всеми подробностями о том, как можно расколоть за полиномиальное время систему открытого шифрования МакЛиса или Нидеррайтера, построенную на основе кодов Рида-Соломона. Основные результаты этого раздела, лежащего на стыке теории кодирования и криптографии, впервые были изложены в работе Шестакова С.О и автора [13]. Мы предполагаем, что раздел будет полезной молодой ученым для выбора направления самостоятельных исследований.

Не надо думать, что все системы открытого шифрования, основанные на кодах корректирующих ошибки, являются не стойкими. Данная работа является, по-видимому, единственным известным примером кодовой системы открытого шифрования, которая раскалывается за полиномиальное время. Для этого используются многие замечательные алгебраические конструкции: группы, матрицы, конечные поля и т.п.

Вместе с тем, как полагает автор, система открытого шифрования, основанные на некоторых классах алгебро-геометрических кодах, в частности, на классе кодов Гоппы (см. раздел 5.3.3) или классе алгебро-геометрических кодов (см., например, [5]), у которых проверочная матрица определяется точками той или иной эллиптической кривой, являются по мнению автора стойкими. В частности, к ним не применимы методы анализа стойкости, рассмотренные в настоящем разделе. Это происходит из-за того, что указанные

классы алгебро-геометрических кодов являются значительно более мощными, по сравнению с классом обобщенных кодов Риды-Соломона, который, по существу, состоит только из одного класса.

Как представляет себе автор, доказательство нестойкости отдельной системы шифрования, которая основаны даже на частном классе алгебро-геометрических кодов, представляет существенный научный интерес.

### 12.0.14 Группа автоморфизмов кода $RS_q(n, d)$ , $n = q$ .

Если переставить координаты кодового вектора  $\mathbf{a}$  кода  $\mathcal{K}$ , то полученный вектор  $\mathbf{a}'$  может как принадлежать так и не принадлежать коду  $\mathcal{K}$ . Если перестановка координат  $\sigma$  такова, что  $\sigma(\mathbf{a}) = \mathbf{a}' \in \mathcal{K}$  для всех  $\mathbf{a} \in \mathcal{K}$ , то она называется автоморфизмом кода  $\mathcal{K}$ . Очевидно, что если  $\sigma'$  — другой автоморфизм, то произведение  $\sigma \cdot \sigma'$  также является автоморфизмом. Поэтому все автоморфизмы кода  $\mathcal{K}$  образуют группу  $\Sigma_{\mathcal{K}}$ , которая называется группой автоморфизмов кода  $\mathcal{K}$ . Заметим, что на множестве перестановок координат векторов пространства  $\mathbb{F}_q^n$  можно естественным образом определить операцию  $\cdot$ , по отношению к которой все они образуют группу  $S_n$  порядка  $n!$ , называемую симметрической группой.

Перестановку  $\sigma$  удобно представлять себе в виде перестановочной матрицы  $\Gamma_{\sigma} = \Gamma = \|\gamma_{i,j}\|$ , которая реализует эту перестановку в виде матричного умножения. А именно, элемент матрицы  $\gamma_{i,j}$  равен 1 тогда и только тогда, когда координата с номером  $i$  переходит посредством действия  $\sigma$  в координату с номером  $j$ . Во всех остальных случаях  $\gamma_{i,j} = 0$ . Таким образом, матрица  $\Gamma$  представляет из себя матрицу, у которой в любой строке и в любом столбце имеется ровно одна 1. Перестановочная матрица  $\Gamma$  реализует перестановку  $\sigma$  координат вектора  $\mathbf{a}$  в виде матричного умножения следующим образом  $\sigma(\mathbf{a}) = \mathbf{a}\Gamma$ . Матричная группа автоморфизмов  $G = G_{\mathcal{K}}$  образована всеми матрицами  $\Gamma_{\sigma}$ , у которых  $\sigma \in \Sigma_{\mathcal{K}}$ .

Если  $\Gamma \in G_{\mathcal{K}}$ , а матрица  $B$  является проверочная матрица кода  $\mathcal{K}$ , то  $B \cdot \Gamma$ , очевидно, также является проверочной матрицей этого кода  $\mathcal{K}$ . Поэтому она может быть представлена в виде  $B \cdot \Gamma = h \cdot B$ , где невырожденная матрица  $h$  размера  $n - k \times n - k$  является матрицей перехода от одного базиса пространства строк матрицы  $B$  к другому  $B'$ . Последнее высказывание на языке матриц записывается как раз в виде  $B' = h \cdot B$ .

Интересно отметить, что указанное отображение  $\Gamma \rightarrow h$  реализует гомоморфизм матричной группы  $G_{\mathcal{K}}$  автоморфизмов кода

$\mathcal{K}$  (матрицы размера  $n \times n$ ) в матричную группу, образованную матрицами  $h$  размера  $n - k \times n - k$ . Ядро  $J(\mathcal{K})$  этого гомоморфизма образуют элементы  $\Gamma$ , которые оставляют на месте все векторы кода  $\mathcal{K}$ . Поэтому матрицы  $h$ , на которые отображается группа  $G_{\mathcal{K}}$  посредством соответствия  $B \cdot \Gamma = h \cdot B$ , изоморфна факторгруппе  $G_{\mathcal{K}}/J(\mathcal{K})$ . Так как далее мы ограничимся рассмотрением только кодов, у которых ядро  $J(\mathcal{K})$  тривиально (состоит из одного элемента), то мы всегда будем полагать, группа образованная матрицами  $h$  изоморфна группе  $G_{\mathcal{K}}$ . К таким кодам относятся коды  $RS_q(n, d)$  и коды  $BCH_q(n, d)$ . Доказательство этого утверждения в более общей форме см. ниже (Лемма 2).

Рассмотрим ансамбль (множество)  $\mathcal{B}_{\mathcal{K}}$  кодов, определяемых проверочными матрицами из множества  $\mathcal{B} = \{B \cdot \Gamma | \Gamma \in S_n\}$ , где  $B$  — одна, не важно

какая, матрица вида (1.2.2). Число  $N_q(n, d)$  различных (как множеств) кодов  $\mathcal{K} =$

$RS_q(n, d)$  в ансамбле  $\mathcal{B}_{\mathfrak{K}}$  (по другому, кодов с проверочной матрицей вида (1.2.2)), как нетрудно видеть, равно

$$N_q(n, d) = \frac{n!}{|G_{\mathfrak{K}}|}, \quad (12.0.1)$$

где  $\mathfrak{K} = RS_q(n, d)$  — один из фиксированных кодов Рида-Соломона с проверочной матрицей (1.2.2).

Как мы видим, число различных кодов Рида-Соломона полностью определяется порядком его группы автоморфизмов. К настоящему времени группа автоморфизмов  $G_{\mathfrak{K}}$  кода  $\mathfrak{K} = RS_q(n, d)$  не вычислена. Можно только утверждать, в  $G_{RS_q(n, d)}$  входят подстановочные матрицы, которые реализуют подстановку  $x \rightarrow ax, a \in \mathbb{F}_q \setminus \{0\} = \mathbb{F}_q^*$ , элементов поля  $\mathbb{F}_q$  в себя. Эти матрицы образуют группу, которая изоморфна, так называемой, мультипликативной группе поля  $\mathbb{F}_q$ . Эта группа является циклической, поэтому и коды Рида-Соломона также как и коды Боуза-Чоудхури-Хоквингема при  $n = q - 1$  с помощью соответствующей нумерации множества  $\mathfrak{A}$  могут быть сделаны циклическими. На этом здесь останавливаться не будем.

### 12.0.15 Число проверочных матриц кода $RS_q(n, d)$

Если  $h$  — невырожденная матрица размера  $d - 1 \times d - 1$ , то, как

нетрудно видеть, проверочные матрицы  $B$  и  $hB$  определяют один и тот же код  $RS_q(n, d)$ . В качестве задачи для самостоятельного доказательства приведем следующее утверждение. *Матрицы  $B$  и  $hB$  различны, если  $h \neq E$  (единичная матрица).* Отсюда следует, что число различных проверочных матриц, которые определяют один и тот же код  $RS_q(n, d)$ , равно  $N_{q, d-1}$ , где  $N_{q, s}$  — число невырожденных квадратных матриц  $h$  размера  $s \times s$ .

**Лемма 1.** *Число  $N_{q, s}$  равно*

$$N_{q, s} = (q^s - 1)(q^s - q) \cdots (q^s - q^{s-1}). \quad (12.0.2)$$

**Доказательство.** Первую строку невырожденной матрицы  $h$  над полем  $\mathbb{F}_q$  размера  $s \times s$  можно выбрать  $q^s - 1$  способами — все векторы длины  $s$ , исключая нулевой. Вторую строку —  $q^s - q$  способами — все векторы, которые не пропорциональны первой строке. Третью строку —  $q^s - q^2$  способами — все векторы, которые не входят в подпространство размерности 2 пространства  $\mathbb{F}_q^s$ , натянутое на первые две строки. И так далее. Наконец, последнюю строку  $h$  можно выбрать  $q^s - q^{s-1}$  способами — все векторы которые не принадлежат  $s - 1$ -мерному пространству натянутому на первые  $s - 1$  строк  $h$ . Отсюда вытекает лемма 1.

Заметим, что вычислить число различных матриц достаточно просто; вместе с тем вычислить число различных кодов  $RS_q(n, d)$  значительно сложнее.

### 12.0.16 Группа обобщенных автоморфизмов кода $RS_q(n, d)$ , $n = q + 1$ , Рида-Соломона

Если в качестве обычных автоморфизмов кода  $\mathfrak{K}$  выступали перестановочные матрицы  $\Gamma$ , то в качестве обобщенных автоморфизмов выступают матрицы вида  $\Lambda = \Gamma \cdot D$ , где  $D$  — невырожденная диагональная матрица, которые носят название мономиальных. Другими словами,  $\Lambda$  — перестановочная матрица, у которых ненулевыми элементами являются ненулевые элементы поля  $\mathbb{F}_q$ .

Мономиальные матрицы сохраняют расстояние Хемминга. А именно,  $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a}\Lambda, \mathbf{b}\Lambda)$ . Как будет видно ниже, это свойство позволяет использовать эти матрицы в системе открытого шифрования. Нашей основной целью является получение нетривиальных нижних верхних оценок порядка группы обобщенных автоморфизмов кода  $RS_q(n, d)$  и затем оценок для числа различных кодов  $RS_q(n, d)$ .

Теперь переформулируем для обобщенных автоморфизмов некоторые из определений раздела 5.5.

Если мономиальная матрица  $\Lambda$  такова, что  $\mathbf{a}\Lambda = \mathbf{a}' \in \mathfrak{K}$  для всех  $\mathbf{a} \in \mathfrak{K}$ , то она называется обобщенным автоморфизмом кода  $\mathfrak{K}$ . Очевидно, что если  $\Lambda'$  — другой автоморфизм, то произведение  $\Lambda \cdot \Lambda'$  также является автоморфизмом. Поэтому все обобщенные автоморфизмы кода  $\mathfrak{K}$  образуют группу  $\Xi_{\mathfrak{K}}$ , которая называется группой обобщенных автоморфизмов кода  $\mathfrak{K}$ . Элементами группы  $\Xi_{\mathfrak{K}}$  являются, так называемые, мономиальные матрицы размера  $n \times n$ . Также как в разделе 5.5 можно рассмотреть представление  $H_{\mathfrak{K}}$  группы обобщенных автоморфизмов  $\Xi_{\mathfrak{K}}$  в виде невырожденных матриц над  $\mathbb{F}_q$  размера  $n - k \times n - k$ . А именно, элементу  $\Lambda$  из  $\Xi_{\mathfrak{K}}$  сопоставим матрицу  $h = h_{\Lambda}$ , которая определяется соотношением

$$h_{\Lambda} \cdot B = B \cdot \Lambda. \quad (12.0.3)$$

Произведение  $\Lambda \cdot \Lambda'$  двух элементов из  $\Xi_{\mathfrak{K}}$  соответствует произведению  $g(\Lambda \cdot \Lambda') = h_{\Lambda \cdot \Lambda'}$  двух элементов из  $H_{\mathfrak{K}}$ . Заметим, что порядок следования сомножителей в  $H_{\mathfrak{K}}$  обратный по сравнению с  $\Xi_{\mathfrak{K}}$ . Поэтому рассматриваемое отображение

является гомоморфизмом  $g : \Lambda \rightarrow h_{\Lambda}$  группы  $\Xi_{\mathfrak{K}}$  в группу матриц размера  $n - k \times n - k$  над полем  $\mathbb{F}_q$ .

**Лемма 2.** Для кода  $\mathfrak{K} = RS_q(n, d)$  гомоморфизм  $g$  является изоморфизмом, т.е.  $|\Xi_{\mathfrak{K}}| = |H_{\mathfrak{K}}|$ .

**Доказательство.** Ядро гомоморфизма  $g$  тривиально. Это следует из-за того, что матрица  $B$  не содержит пропорциональных столбцов и поэтому  $B \neq B \cdot \Lambda$  для любой неединичной мономиальной матрицы  $\Lambda$ . Поэтому среди неединичных мономиальных матриц  $\Lambda$  не существует такой, что  $\mathbf{a} = \mathbf{a}\Lambda$  для всех  $\mathbf{a} \in RS_q(n, d)$ . Лемма доказана.

**Теорема 1.** Порядок группы  $\Xi_{\mathfrak{K}}$  автоморфизмов кода Руда-Соломона  $\mathfrak{K} = RS_q(n, d)$  не превосходит  $N_{q, d-1}$ , где  $N_{q, s}$  — число невырожденных квадратных матриц  $h$  размера  $s \times s$  над полем  $\mathbb{F}_q$ .

**Доказательство.** Как следует из леммы 2  $|\Xi_{\mathfrak{K}}| = |H_{\mathfrak{K}}|$ . Поэтому  $|\Xi_{\mathfrak{K}}| \leq N_{q, n-k}$ ,  $k = n - d + 1$ , ибо, очевидно, что  $|H_{\mathfrak{K}}|$  не превосходит числа всех матриц размера  $d - 1 \times d - 1$  над полем  $\mathbb{F}_q$ . Теорема доказана.

Хотя оценка для числа  $\Xi_{\mathfrak{K}}$  во многих случаях, по-видимому, весьма грубая, ничего лучшего не известно.

Рассмотрим ансамбль (множество)  $\mathcal{A}_{\mathfrak{K}}$ ,  $\mathfrak{K} = RS_q(n, d)$ , кодов, определяемых проверочными матрицами из множества  $\mathfrak{B} = \{B\Lambda | \Lambda \in U_{q, n}\}$ , где  $B$  — одна, не важно какая, матрица вида (1.2.2), а  $U_{q, n}$  — множество всех мономиальных матриц над полем  $\mathbb{F}_q$ . Заметим, что ансамбль  $\mathcal{A}_{\mathfrak{K}}$  совпадает с множеством кодов, проверочные матрицы которых

имеют вид (1.1.5). Кроме того, нетрудно установить, что  $|U_{q,n}| = n!(q-1)^n$ . Нас будет интересовать число различных кодов в ансамбле  $\mathcal{A}_{\mathfrak{K}}$ .

По тем же соображениям, что приведены в разделе 5.5, для числа  $A_q(n, d)$  различных обобщенных кодов Рида-Соломона  $\mathfrak{K} = RS_q(n, d)$  в ансамбле  $\mathcal{A}_{\mathfrak{K}}$  имеет место равенство

$$A_q(n, d) = \frac{n!(q-1)^n}{|\Xi_{\mathfrak{K}}|}. \quad (12.0.4)$$

К сожалению, группа  $\Xi_{\mathfrak{K}}$  обобщенных автоморфизмов кода Рида-Соломона не известна. Поэтому мы не можем воспользоваться равенством (12.0.4) для вычисления числа  $A_q(n, d)$ .

Из теоремы 1 и соотношений (12.0.2) и (12.0.4) следует

**Следствие 1.** Для числа  $A_q(n, d)$  различных обобщенных Рида-Соломона  $\mathfrak{K} = RS_q(n, d)$  в ансамбле  $\mathcal{A}_{\mathfrak{K}}$  имеет место оценка

$$A_q(n, d) \geq \frac{n!(q-1)^n}{N_{q,k}} = \frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q) \cdots (q^{d-1}-q^{d-2})}, \quad (12.0.5)$$

где  $k = n - d + 1$  — размерность кода  $\mathfrak{K} = RS_q(n, d)$  и  $N_{q,k}$  — число различных невырожденных матриц размера  $k \times k$ .

Далее мы докажем, что группа  $\Xi_{\mathfrak{K}}$  содержит подгруппу, изоморфную группе дробно-линейных преобразований. Строение последней группы мы изучим в следующем разделе.

### 12.0.17 Группа дробно-линейных преобразований.

Мы рассматриваем некоммутативную группу дробно-линейных отображений  $\Phi_q$  множества  $\widehat{\mathbb{F}}_q = \mathbb{F}_q \cup \{\infty\}$  в себя. Элементами  $\Phi_q$  являются дробно-линейные функции  $\varphi(x) = \frac{ax+b}{cx+e}$ , отличные от постоянной, т.е. функции, у которых определитель матрицы  $\begin{pmatrix} a & b \\ c & e \end{pmatrix}$  отличен от нуля. Групповой операцией  $\cdot$  является суперпозиция функций, т.е.  $\varphi(x) \cdot \varphi'(x) = \varphi(\varphi'(x))$ . Очевидно, каждое дробно-линейное преобразование  $\phi(x)$  взаимно однозначно отображает множество  $\widehat{\mathbb{F}}_q$  в себя.

Группа  $\Phi_q$  изоморфна известной группе  $PGL(2, q)$ . Ее порядок равен  $(q+1)q(q-1)$  (Упражнение). Очень интересным свойством группы  $\Phi_q$  является ее трижды транзитивность. Это означает, что для любых двух пар троек  $(a_1, a_2, a_3)$  и  $(b_1, b_2, b_3)$ ,  $a_i, b_i \in \mathbb{F}'_q$ , с попарно различными координатами в группе  $\Phi_q$  найдется элемент  $\phi$  (всегда один), для которого выполнено  $\phi(a_i) = b_i$ ,  $i = 1, 2, 3$ . Доказательство этих свойств несложно и предоставляется читателю (см. также [23] и [3]). (Упражнение)

**Теорема 12.0.5** Группа  $\Xi_{\mathfrak{K}}$  обобщенных автоморфизмов кода  $\mathfrak{K} = RS_q(n, d)$ ,  $n = q + 1$ , Рида-Соломона с проверочной матрицей  $B$  (см. (1.2.2)) содержит подгруппу, которая изоморфна группе дробно-линейных преобразований множества  $\mathbb{F}'_q$ .

**Доказательство.** Как и выше, будем индексировать столбцы матрицы  $B$  (см. (1.2.2)) элементами множества  $\mathbb{F}'_q$ . Так столбец  $B(\alpha_j) = (\alpha_j^0, \alpha_j^1, \dots, \alpha_j^{d-2})^T$  имеет номер (индекс)  $\alpha_j$ .

Пусть  $\phi(x) = \frac{ax+b}{cx+e}$  — дробно-линейная функция. Через  $\Gamma_\phi$  обозначим подстановочную матрицу, реализующую перестановку  $x \rightarrow \phi(x)$  элементов множества  $\mathbb{F}'_q$  и через  $D_\phi =$

$\text{diag}((c\alpha_1 + e)^{d-2}, (c\alpha_2 + e)^{d-2}, \dots, (c\alpha_n + e)^{d-2})$  — диагональную матрицу, определяемую значениями знаменателя функции  $\phi(x)$  на всех элементах множества  $\mathbb{F}'_q$ .

Прямое вычисление показывает, что  $B(\alpha_j) \cdot \Gamma_\phi \cdot D_\phi = ((c\alpha_j + e)^{d-2}, (a\alpha_j + b)(c\alpha_2 + e)^{d-3}, \dots, (a\alpha_j + b)^{d-3}(c\alpha_2 + e), (a\alpha_j + b)^{d-2})^T$ . Каждый многочлен  $(ax + b)^{d-2-i}(cx + e)^i$  может быть представлен как линейная функция мономов  $1, x, \dots, x^{d-2}$ . Поэтому столбец  $B(\alpha_j) \cdot \Gamma_\phi \cdot D_\phi$  можно представить как  $B(\alpha_j) \Gamma_\phi \cdot D_\phi = h(1, x, x^2, \dots, x^{d-2})^T$ , и, следовательно, матрицу  $B \cdot \Gamma_\phi \cdot D_\phi$  — в виде  $B \cdot \Gamma_\phi \cdot D_\phi = h \cdot B$ , где строки невырожденной матрицы  $h = \{h_{i,j}\}$  определяются равенством  $(ax + b)^{d-2-i}(cx + e)^i = \sum_{j=0}^{d-2} h_{i,j} x^j$ . Таким образом, при любом  $\phi$  матрица  $\Gamma_\phi \cdot D_\phi$  входит в группу обобщенных автоморфизмов  $\Xi_{\mathfrak{K}}$ .

Матрицы  $\Lambda_\phi = \Gamma_\phi \cdot D_\phi$  образуют группу изоморфную группе  $\Phi_q$ . Для того, чтобы это проверить, заметим, что  $\Gamma_\phi^{-1} \cdot D_{\phi'} \cdot \Gamma_\phi = \text{diag}((c'\phi(\alpha_1) + e')^{d-2}, \dots, (c'\phi(\alpha_n) + e')^{d-2}) = D_{\phi', \phi}$ , если  $\phi'(x) = \frac{a'x + b'}{c'x + e'}$ . Отсюда  $D_{\phi'} \cdot \Gamma_\phi = \Gamma_\phi \cdot D_{\phi', \phi}$ . Следовательно,  $\Gamma_{\phi'} \cdot D_{\phi'} \cdot \Gamma_\phi \cdot D_\phi = \Gamma_{\phi' \otimes \phi} \cdot D_{\phi' \otimes \phi}$ . Прямая выкладка показывает, что  $D_{\phi', \phi} \cdot D_\phi = D_{\phi' \otimes \phi}$ , т.е. группа, образованная матрицами  $\Gamma_\phi \cdot D_\phi$ , изоморфна дробно-линейной группе  $\Phi_q$ . Теорема доказана.  $\square$

Этот результат будет использован при анализе стойкости системы открытого шифрования, построенной с помощью кода Рида-Соломона (см. §4).

Группа  $\Xi_{\mathfrak{K}}$  обобщенных автоморфизмов кода Рида-Соломона также является трижды транзитивной в следующем смысле. Для любой пары упорядоченных троек из попарно различных элементов  $(\beta_1, \beta_2, \beta_3)$  и  $(\gamma_1, \gamma_2, \gamma_3)$ , где  $\{\beta_1, \beta_2, \beta_3\}, \{\gamma_1, \gamma_2, \gamma_3\} \in \mathfrak{A} = \{\alpha_1, \alpha_2, \dots, \alpha_n\} = \mathbb{F}'_q$  существует такая мономальная матрица  $\Lambda_\phi \in \Xi_{\mathfrak{K}}$ , которая переводит координаты  $x_{\beta_1}, x_{\beta_2}, x_{\beta_3}$  вектора  $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$  в координаты  $x_{\gamma_1}, x_{\gamma_2}, x_{\gamma_3}$  вектора  $\mathbf{x}\Lambda_\phi$  с умножением их на соответствующие постоянные, определяемые диагональной матрицей  $D_\phi = \text{diag}(d_{\alpha_1}, d_{\alpha_2}, \dots, d_{\alpha_n})$ . Например, с помощью подходящей матрицы  $\Lambda_\phi$  можно передвинуть на первые три места любые три координаты вектора  $\mathbf{x}$ . В частности, если  $\{\beta_1 = 1, \beta_2 = 0, \beta_3 = \infty\}$  и  $\gamma_1 = \alpha_1, \gamma_2 = \alpha_2, \gamma_3 = \alpha_3$ , то  $\mathbf{x}\Lambda_\phi = (d_{\alpha_1}x_1, d_{\alpha_2}x_0, d_{\alpha_3}x_\infty, d_{\alpha_4}x_{\phi(\alpha_4)}, \dots, d_{\alpha_n}x_{\phi(\alpha_n)})$  для некоторой подходящей функции  $\phi(x)$ .

## 12.1 Декодирование

Мы приведем без доказательства ряд утверждений о декодировании кодов, которые будут играть центральную роль при обосновании стойкости рассматриваемых систем открытого шифрования. Этот раздел дополняет соответствующие результаты главы 6.

Неформально говоря, под термином "декодирование" понимается алгоритм, который позволяет по искаженному ошибками кодовому вектору  $\mathbf{a}'$  восстановить исходный кодовый вектор  $\mathbf{a}$ . Таким образом, декодирование сводится к решению уравнения

$$\mathbf{a}' = \mathbf{a} + \mathbf{e}, \mathbf{a} \in \mathfrak{K}, wt(\mathbf{e}) \leq t, \quad (12.1.1)$$

где неизвестными являются кодовый вектор  $\mathbf{a}$  и вектор ошибки  $\mathbf{e}$ .

Заметим, что далее при обсуждении сложности декодирования мы всегда предполагаем, что в уравнении (12.1.1) векторы  $\mathbf{a}$  и  $\mathbf{e}$ , определяющие вектор  $\mathbf{a}'$ , выбираются случайным и равновероятным способом в множествах  $\mathfrak{K}$  и  $\{\mathbf{e} | wt(\mathbf{e}) \leq t\}$ , соответственно.

Имеется несколько различных типов декодирования.



i. *Декодирование кода  $\mathcal{K}$  по минимуму расстояния.* Этот алгоритм по предъявленному вектору  $\mathbf{x} \in \mathbb{F}_q^n$  находит один или несколько кодовых векторов  $\mathbf{a} \in \mathcal{K}$ , ближайших (в метрике Хемминга) к  $\mathbf{x}$ .

ii. *Декодирование кода  $\mathcal{K}$  в пределах его кодового расстояния.* Это алгоритм, который по вектору  $\mathbf{x}$ , который отстоит от одного из кодовых векторов  $\mathcal{K}$  на расстояние  $\leq \frac{d(\mathcal{K})-1}{2}$ , вычисляет этот ближайший кодовый вектор. Такой вектор обязательно является единственным. Вместе с тем векторы  $\mathbf{x}$ , которые отстоят от всех кодовых точек на расстояние большее, чем половина кодового расстояния, могут быть декодированы как угодно, в частности, алгоритм может вообще отказаться от их декодирования.

iii. *Декодирование кода  $\mathcal{K}$  за пределами его кодового расстояния.* (Алгоритм промежуточного положения между i. и ii.) Это алгоритм, который по вектору  $\mathbf{x}$ , находящемуся не очень далеко ( $d(\mathbf{x}, \mathbf{a}) \leq t'$ ) от некоторого кодового вектора  $\mathbf{a}$  кода  $\mathcal{K}$ , вычисляет один или несколько кодовых векторов  $\mathbf{a}'$ , находящихся на расстоянии  $\leq t'$  от  $\mathbf{x}$ , где  $t' > \frac{d(\mathcal{K})-1}{2}$  — некоторая постоянная (параметр алгоритма).

Наиболее сильным и трудным для реализации является алгоритм п.i. В настоящее время не известно ни одного нетривиального класса кодов (т.е. с не очень маленькой, но и не очень большой скоростью передачи), которые имеют алгоритм декодирования этого типа с простой реализацией.

Другими словами, этот алгоритм может быть реализован только с помощью одного из двух следующих переборных алгоритмов.

1. Мы сравниваем  $\mathbf{x}$  со всеми векторами кода и выделять среди них ближайшие кодовые векторы.

2. Мы осуществляем просмотр векторов из окрестности  $\mathbf{x}$ , пытаясь найти в ней кодовый вектор.

Какой из этих двух алгоритмов перебора выгодней с вычислительной точки зрения зависит от соотношений между параметрами  $k$  и  $t$  кода.

Сложность реализации декодирования по максимуму правдоподобия нетривиальных кодов возрастает как экспоненциальная функция от их длины. На практике ни один из таких кодов на современных вычислительных средствах не может быть декодирован, начиная с длины кода  $\approx 100$  или даже несколько меньшей.

Наиболее легким для реализации является алгоритм декодирования типа ii.. Для большинства, так называемых, алгебраических кодов известны алгоритмы декодирования в пределах их кодового расстояния, сложность которых возрастает как полином небольшой степени от длины кода. К таким кодам относятся и уже рассмотренные нами обобщенные коды Рида-Соломона  $RS_q(n, d)$ . Их декодирование в пределах кодового расстояния может быть осуществлено не более, чем за  $O(n^3)$  операций в поле  $\mathbb{F}_q$  (см. главу 6).

Не надо думать, что для каждого кода существует простой алгоритм декодирования в пределах его кодового расстояния. По современным представлениям такие алгоритмы могут существовать только для кодов, которые снабжены определенной алгебраической или комбинаторной структурой. Вместе с тем у большинства кодов, не очень точно выражаясь, отсутствует в проверочной матрице какая-либо структура, — это коды "общего положения". Примером первого типа кодов является код Рида-Соломона или код Рида-Маллера (совершенно разные коды), а примером второго — код, у которого проверочная матрица выбрана случайно среди всех матриц определенной размерности.

Декодирование в пределах кодового расстояния (типа п.ii.) некоторых типов кодов

общего положения является NP-полной задачей, т.е. предположительно, не может быть осуществлено за полиномиальное время от их длины. Более того, общепринято, что справедливо следующее утверждение.

**Тезис А.** *декодирование последовательности кодов, которые не обладают полезной для декодирования алгебраической или комбинаторной структурой, не может быть осуществлено за полиномиальное время от их длины.*

Это достаточно расплывчатое, но очень правдоподобное утверждение строго не доказано и в настоящее время возможность его доказательства весьма проблематична. Вместе с тем на этом утверждении "держится" обоснование стойкости открытого шифрования на базе кодов, корректирующих ошибки. Мы далее, специально не указывая на это, будем постоянно его придерживаться.

Обычно при построении кода, корректирующих ошибки, стараются наделить его определенной структурой, которая обеспечивает, с одной стороны, заданное значение его

кодového расстояния, и, с другой позволяет, осуществлять его декодирование с малой вычислительной сложностью.

Приведем одно почти очевидное утверждение о сложности декодирования любого кода с помощью алгоритма типа п.ii..

**Утверждение 2.** *Любой линейный  $r$ -значный код  $\mathcal{K}$  с параметрами  $[n, k, d]_r$ ,  $d \leq n/2$ , имеет алгоритм декодирования в пределах его кодového расстояния, сложность которого не выше  $O(\min(nr^k, n \sum_{j=0}^t \binom{n}{j})),$  где  $t = \lfloor \frac{d-1}{2} \rfloor$ .*

Отметим, что  $r^k$  — число элементов в коде  $\mathcal{K}$  и  $O(nr^k)$  — число операций требуемых для перебора всех элементов кода и сравнения каждого из них с искаженным кодовым вектором  $\mathbf{a}'$ . Далее,  $\sum_{j=0}^t \binom{n}{j} (r-1)^j$  — число элементов в шаре радиуса  $t$  с центром в точке  $\mathbf{x}$  и  $O(n \sum_{j=0}^t \binom{n}{j})$  — число операций, требуемых для перебора всех элементов шара с целью нахождения среди них кодového вектора.

## 12.2 Системы открытого шифрования на основе кода, корректирующего ошибки

### 12.2.1 Система открытого шифрования Маклиса.

Идею построения системы открытого шифрования проще всего пояснить на примере кода Боуза-Чоудхури-Хоквингема  $BCH_r(n, d)$  размерности  $k$ .

Пусть  $A$  — фиксированная порождающая матрица обобщенного кода  $BCH_r(n, d)$  над  $\mathbb{F}_r$ , т.е. матрица ранга  $k$  и размера  $k \times n$ , для которой  $A \cdot C^T = 0$ , где  $C$  — матрица, определенная соотношением (5.3.1). Между прочим, в качестве  $A$  можно взять матрицу, которая имеет тот же вид, что и  $C$ . Этот факт мы использовать не будем.

Ансамбль  $\mathcal{A}_r(n, d)$  порождающих матриц  $r$ -значных обобщенных БЧХ-кодов  $BCH_r(n, d) = BCH_k(n, d)$  длины  $n$ , размерности  $k$  с гарантированным кодовым расстоянием  $d$  (см. раздел 5.3.1) определим как множество всех матриц вида  $h \cdot A \cdot \Gamma \cdot D$ , где  $h$  пробегает множество всех невырожденных  $k \times k$ -матриц над  $\mathbb{F}_r$ ,  $D$  — множество всех диагональных матриц с ненулевыми на диагоналях элементами, а  $\Gamma$  — множество всех перестановочных матриц размера  $n \times n$ .

Соответственно, ансамбль кодов  $\mathcal{K}_r(n, d)$  определяется как множество всех кодов с

порождающими матрицами из ансамбля  $\mathcal{A}_r(n, d)$ . Заметим, что ансамбль  $\mathcal{K}_r(n, d)$  содержит меньшее число элементов, чем ансамбль  $\mathcal{A}_r(n, d)$ , так как различные порождающие матрицы могут определять один и тот же код из  $\mathcal{K}_r(n, d)$ .

Отметим также, что основное предназначение матриц  $h$ ,  $\Gamma$ ,  $D$  — это "маскировка" матрицы  $A$  под матрицу общего положения.

Передача секретного сообщения, исходящего от абонента  $\mathcal{Y}$  и предназначенного абоненту  $\mathcal{X}$ , предваряется следующими действиями. Абонент  $\mathcal{X}$  случайно, равновероятно в соответствующих множествах и независимо от других абонентов выбирает матрицы  $h = h_{\mathcal{X}}$ ,  $D = D_{\mathcal{X}}$ ,  $\Gamma = \Gamma_{\mathcal{X}}$  и вычисляет матрицу  $A' = A'_{\mathcal{X}} = h_{\mathcal{X}} \cdot A \cdot \Gamma_{\mathcal{X}} \cdot D_{\mathcal{X}}$ , принадлежащую ансамблю  $\mathcal{A}_r(n, d)$ . Матрица  $A'_{\mathcal{X}}$  является открытым (общедоступным для всех абонентов) ключом (public key), а матрицы  $h_{\mathcal{X}}, \Gamma_{\mathcal{X}}, D_{\mathcal{X}}$  — секретным ключом (private key) абонента  $\mathcal{X}$ .

Шифрованная информация  $\mathbf{b}$  (криптограмма), которую абонент  $\mathcal{Y}$  передает по общедоступному каналу абоненту  $\mathcal{X}$ , в системе Маклиса [67] представляет собой вектор длины  $n$  и вида  $\mathbf{b} = \vec{a}A'_{\mathcal{X}} + \mathbf{e}$ , где  $\vec{a}$  —  $r$ -значный вектор длины  $k$ , несущий конфиденциальную информацию абонента  $\mathcal{Y}$ , а  $\mathbf{e}$  — секретный вектор ошибок веса, не превосходящего  $t$ , и длины  $n$ , который случайно и равновероятно выбирается абонентом  $\mathcal{Y}$  среди всех векторов веса не выше  $t$ .

Таким образом, для того чтобы расколоть систему, т.е. получить открытую информацию  $\vec{a}$ , достаточно (но не необходимо) представить вектор  $\mathbf{b}$  в виде

$$\mathbf{b} = \mathbf{a} + \mathbf{e}, \quad (12.2.1)$$

где вектор  $\mathbf{a} = \vec{a}A'_{\mathcal{X}}$  принадлежит коду  $K = K_{\mathcal{X}}$  с порождающей матрицей  $A'_{\mathcal{X}}$ , а вектор  $\mathbf{e}$  имеет вес  $\leq t$ .

Другими словами, злоумышленнику необходимо декодировать код  $K$  с известной порождающей матрицей  $A'_{\mathcal{X}}$ . Матрица  $A'_{\mathcal{X}}$  замаскирована матрицами  $h$ ,  $D$  и  $\Gamma$  и поэтому она, вообще говоря, представляется нападающей стороне как матрица общего положения. По тезису А в этом случае сложность декодирования не является полиномиальной от длины  $n$  кода  $K$ . Следовательно, при достаточно больших  $n$  процедура декодирования недоступна для злоумышленника из-за того, что она имеет большую вычислительную сложность, в том случае если он использует переборный алгоритм.

Вместе с тем декодирование кода  $K$  той же длины  $n$  для легитимного абонента  $\mathcal{X}$ , знающего свой секретный ключ, является достаточно простой вычислительной процедурой, ибо, как будет показано ниже, он может использовать алгоритм декодирования с полиномиальной сложностью из-за того, что он знает свой секретный ключ. Только это различие в возможностях декодирования между злоумышленником и легитимным пользователем обеспечивает секретность открытого шифрования в рассматриваемой системе.

Расскажем, как легитимный абонент  $\mathcal{X}$ , получив вектор  $\mathbf{b}$ , восстанавливает, посланную ему секретную информацию  $\vec{a}$ . Сначала он строит вектор  $\mathbf{b}' = \mathbf{b}D^{-1} \cdot \Gamma^{-1}$ , который, очевидно, является вектором кода  $BCH_r(n, d)$  с порождающей матрицей  $A$ , искаженный не более, чем в  $t$  разрядах. Как раз здесь используется тот факт, что мономиальная матрица  $D^{-1} \cdot \Gamma^{-1}$  сохраняет вес вектора-ошибки  $\mathbf{e}D^{-1} \cdot \Gamma^{-1}$  (см. раздел 12.0.16). Затем с помощью какого-либо общеизвестного полиномиального алгоритма декодирования кода  $BCH_r(n, d)$  находится кодовый вектор  $\mathbf{a}$ ,  $\mathbf{a} = \vec{a}'A$ , который удовлетворяет условию  $\mathbf{b}' = \mathbf{a} + \mathbf{e}'$ , где  $w(\mathbf{e}') \leq t$ . Затем вычисляется вектор  $\vec{a}$  в виде  $\vec{a} = \vec{a}'h^{-1}$ .

Мы будем предполагать, что  $t \leq (d-1)/2$ . Вместе с тем существуют полиномиальные алгоритмы декодирования, которые работают "почти всегда" правильно при числе ошибок  $t$  большем "половины кодового расстояния", но меньшем определенной границы сверху на  $t$ . К таким алгоритмам декодирования относятся алгоритмы работ [63] и [31] (см. также раздел 6). Как будет видно ниже, чем больше алгоритм декодирования исправляет ошибок, тем выше будет стойкость системы шифрования.

Вместе с тем при возрастании числа исправляемых ошибок, как правило, возрастает и сложность реализации этого алгоритма. В идеале, лучше всего использовать переборный алгоритм, работающий по критерию максимального правдоподобия, но его сложность является слишком высокой и он не доступен для реализации. Обычно в системе Маклиса используют алгоритмы типа п.ii. или п.iii.

### 12.2.2 Система открытого шифрования Нидеррайтера.

Эту систему шифрования мы рассмотрим на примере кода Рида-Соломона  $RS_q(n, d)$  длины  $n \leq q+1$ . Общий случай очевидным образом вытекает из рассмотренного. В системе Нидеррайтера [69] рассматривается ансамбль  $\mathcal{RS}_q(n, d)$  проверочных матриц кода  $RS_q(n, d)$ , который определяется как множество всех матриц вида

$$B' = h \cdot C \cdot D \cdot \Gamma, \quad (12.2.2)$$

где  $C$  — фиксированная проверочная матрица вида (5.0.1),  $h$  пробегает множество всех невырожденных  $n-k \times n-k$ -матриц над  $\mathbb{F}_r$ ,  $D$  — множество всех диагональных матриц с ненулевыми на диагонали элементами, а  $\Gamma$  — множество всех перестановочных матриц размера  $n \times n$ .

Подобно системе Маклиса, открытым ключом абонента  $\mathcal{X}$  в системе Нидеррайтера является матрица  $B'$ , а секретным — матрицы  $h, D, \Gamma$ .

Шифрованная информация  $\mathbf{c}$  абонента  $\mathcal{Y}$  и предназначенная абоненту  $\mathcal{X}$  в системе Нидеррайтера представляет собой  $r$ -значный вектор длины  $n-k$  и вида

$$\mathbf{c} = \mathbf{e}B'^T, \quad (12.2.3)$$

где  $B' = B'_\mathcal{X}$  проверочная матрица, которая случайно выбрана абонентом  $\mathcal{X}$  из ансамбля  $\mathcal{B}_r(n, d)$  и  $k$  — размерность кода с этой проверочной матрицей. Вектор  $\mathbf{e}$  является вектором длины  $n$  и веса, не превосходящего  $t$ , который переносит конфиденциальную (секретную) информацию абонента  $\mathcal{Y}$ .

Таким образом, в системе Нидеррайтера для передачи секретной информации абонент  $\mathcal{Y}$  должен сначала каким-либо образом представить ее в виде вектора  $\mathbf{e}$  веса не более  $t$ . В свою очередь получатель (абонент  $\mathcal{X}$ ), восстановив вектор  $\mathbf{e}$ , должен его "декодировать", т.е. восстановить исходную секретную информацию абонента  $\mathcal{Y}$ .

Заметим, что конфиденциальная информация, т.е. вектор  $\mathbf{e}$ , является одним из решений уравнения

$$\mathbf{c} = \mathbf{x}B'^T. \quad (12.2.4)$$

Найти какое-либо решение этого уравнения простая задача — это линейное уравнение с  $n-k$  уравнениями и  $n$  неизвестными. Найти среди всех решений (их число  $2^k$ ) решение с минимальным весом это уже сложная задача, которая эквивалентна задаче декодирования кода с проверочной матрицей  $B'$ .

Доказательство последнего утверждения просто. Если мы умеем находить решение  $\mathbf{e}$  уравнения (12.2.4) минимального веса, то решение уравнения (12.1.1) производится следующим образом. Сначала вычислим вектор  $\mathbf{a}'B'^T = \mathbf{e}B'^T$  (синдром  $\mathbf{a}'$ ), найдем вектор ошибок  $\mathbf{e}$ , а затем вычислим кодовый вектор  $\mathbf{a} = \mathbf{a}' - \mathbf{e}$ .

Также как в системе Маклиса в системе Нидеррайтера матрица  $B'$  представляется нападающей стороне матрицей общего положения.

В теории кодирования вектор  $\mathbf{c}$  из (12.2.4) называют синдромом вектора-ошибки  $\mathbf{e}$ . Отметим, что матрицы  $B'$  и  $A'$  связаны соотношением  $B' \cdot A'^T = 0$ , где  $A'$  — одна из матриц ансамбля  $\mathcal{A}_r(n, d)$ . Строки матрицы  $B'$  являются базисом подпространства размерности  $N - k$ , ортогонального к пространству строк матрицы  $A'$ .

Абонент  $\mathcal{X}$ , получив сообщение  $\mathbf{c}$ , находит какой-либо вектор  $\mathbf{b}$ , который является решением уравнения  $\mathbf{x}B'^T = \mathbf{c}$ . Очевидно, вектор  $\mathbf{b}$  является вектором вида  $\mathbf{b} = \vec{a}A' + \mathbf{e}$  при некотором неизвестном  $\vec{a} \in \mathbb{F}_r^k$ . Затем абонент  $\mathcal{X}$  также, как в системе Маклиса, декодирует вектор  $\mathbf{b}\Gamma^{-1} \cdot D^{-1} = \mathbf{b}' = \vec{a}'A + \mathbf{e}'$ , но вместо кодового вектора  $\vec{a}'A$  находит вектор  $\mathbf{e}' = \mathbf{b}' - \vec{a}'A$ , а затем и вектор  $\mathbf{e} = \mathbf{e}'\Gamma \cdot D$ . Отметим, что в отличие от системы Маклиса, в системе при расшифровании (восстановлении вектора  $\mathbf{e}$ ) никак не участвует матрица  $h$ . Она нужна только для маскировки матрицы  $B'$ .

Как и выше, предполагаем, что используемый алгоритм декодирования кода  $RS_q(n, d)$  всегда правильно восстанавливает вектор ошибок  $\mathbf{e}$ .

### 12.2.3 Сравнение систем открытого шифрования Маклиса и Нидеррайтера.

Системы Маклиса и Нидеррайтера обладают одинаковой стойкостью к нападению, ибо криптографическая атака на одну из систем может быть легко трансформирована в атаку на другую. Поясним это подробно.

Мы полагаем, что обе взаимно ортогональные матрицы  $A'$  (открытый ключ системы Маклиса) и  $B'$  (открытый ключ системы Нидеррайтера) известны нападающей стороне, так как одна из другой может быть получена как решение линейной системы уравнений  $A' \cdot B'^T = 0$ , т.е. с помощью не более, чем  $O(n^3)$  операций.

При известном синдроме  $\mathbf{c} = \mathbf{e}B'^T$  нетрудно вычислить вектор  $\mathbf{b} = \vec{a}A' + \mathbf{e}$  с некоторым вектором  $\vec{a} \in \mathbb{F}_r^k$  такой, что  $\mathbf{c} = \mathbf{b}B'^T$ . Для этого надо найти какое-либо решение  $\mathbf{b}$  уравнения (12.2.4). Вектор  $\mathbf{b}$  мы будем рассматривать как криптограмму в системе Маклиса.

Если для системы Маклиса найдена криптографическая атака со сложностью  $Q$ , т.е. известен алгоритм вычисления вектора  $\vec{a}$  (конфиденциальная информация в системе Маклиса), то вектор  $\mathbf{e}$  (конфиденциальная информация в системе Нидеррайтера), очевидно, представляется в виде  $\mathbf{e} = \mathbf{b} - \vec{a}A'$ , т.е. сложность определения  $\mathbf{e}$ , по существу, совпадает со сложностью определения  $\vec{a}$ .

Наоборот, если для системы Нидеррайтера известна криптографическая атака со сложностью  $Q$ , то используя в качестве криптограммы этой системы вектор  $\mathbf{c} = \mathbf{b}B'^T = (\vec{a}A' + \mathbf{e})B'^T = \mathbf{e}B'^T$ , где  $\mathbf{b}$  — криптограмма системы Маклиса, вычислим вектор ошибок  $\mathbf{e}$ , а затем и вектор  $\vec{a}$ , который является единственным решением линейного уравнения  $\vec{y}A' = \mathbf{b} - \mathbf{e}$ .

Соображения, использованные в предыдущих двух абзацах, любезно сообщены автору

в устной беседе Г.А. Кабатянским.

#### 12.2.4 Некоторые свойства систем открытого шифрования Маклиса и Нидеррайтера.

Две эти системы различаются скоростью передачи. Если код  $\mathcal{K}$  является низкоскоростным, т.е.  $k/n$  — малое число, то скорость передачи у системы Нидеррайтера всегда выше по сравнению с системой Маклиса. Поэтому далее будем рассматривать только систему Нидеррайтера. Вместе с тем будем предполагать, не оговаривая этого особо, что криптограммой системы Нидеррайтера является  $n$ -мерный вектор  $\mathbf{b} = \vec{a}A' + \mathbf{e}$ , который является каким-либо решением системы (12.2.4), где  $\mathbf{c} = \mathbf{b}B'^T = \mathbf{e}B'^T$  и  $\mathbf{e}$  — вектор веса не выше  $t$  (информационный вектор абонента  $\mathcal{Y}$ ). Это связано с тем, что алгоритмы декодирования кода  $RS_q(n, d)$ , рассмотренные в [63] и [31], а также и некоторые другие известные криптографические атаки оперируют с искаженным кодовым вектором  $\mathbf{b}$ , а не с его синдромом  $\mathbf{c}$ . Вместе с тем известны и синдромные алгоритмы декодирования.

Шифрование сообщения в системе Нидеррайтера  $\mathbf{e}$  состоит в вычислении его синдрома и поэтому сложность шифрования равна  $O((N - k)N)$  операций. Сложность расшифрования (сложность восстановления вектора  $\mathbf{e}$ ) определяется, в основном, трудоемкостью алгоритма декодирования кода  $RS_q(n, d)$  и при использовании алгоритма декодирования, описанных в главе 6, не превосходит  $O(n^3)$  операций.

Сравним некодовые системы открытого шифрования, например, систему RSA с кодовыми системами.

Во-первых, скорость передачи у кодовой системы всегда меньше 1 (обычно меньше  $1/2$ ), в то время как в системе RSA (см. [43] (стр. 135) и [32] многие другие работы) она равна 1.

Во-вторых, открытый ключ (в рассматриваемой кодовой системе — матрица  $B'$ ) имеет объем примерно в  $n - k$  раз больший, чем у упомянутой системы RSA. Если  $k$  относительно маленькое число то выгодней в качестве открытого ключа системы рассматривать матрицу  $A'$ , которая связана с  $B'$  соотношением  $B' \cdot A' = 0$ .

Кроме того исследований по оценки стойкости кодовых систем известно значительно меньше, чем исследований стойкости других криптосистем, например, системы RSA.

Вместе с тем кодовые системы открытого шифрования имеют существенные преимущества: алгоритм зашифрования информации, а в некоторых случаях и расшифрования, существенно более быстрый, чем, например, у системы RSA.

В системе открытого шифрования Нидеррайтера в качестве открытой информации выступают векторы  $\mathbf{e}$  веса  $t$  и менее. Для ее реализации необходимо иметь алгоритм, который отображает множество всех  $r$ -ных векторов длины  $s$  в множество  $W_t$  векторов длины  $n$  и веса не выше  $t$ , где  $s \leq \tau(t, N) = \lceil \lg_r \sum_{i=0}^t \binom{N}{i} (r - 1)^i \rceil$  (логарифм числа возможных сообщений в системе Нидеррайтера). Этого относительно простого вопроса мы касаться не будем.

Система Нидеррайтера полностью определяется как проверочной матрицей  $B'$ , так и ортогональной к ней порождающей матрицей  $A'$ , и наоборот. Поэтому открытым ключом этой системы естественно считать матрицу, которая содержит меньшее число строк, хотя криптограмма  $\mathbf{c} = \mathbf{e}B'$  всегда реально строится с помощью матрицы  $B'$ .

Переход от системы Маклиса к системе Нидеррайтера полезен не только с точки зрения повышения скорости передачи, но и, что, возможно, более важно, позволяет с помощью несложной модернизации существенно усилить ее стойкость к криптографическим атакам. По поводу этого вопроса см. работу [31].

## 12.3 Как раскалывается система открытого шифрования Нидеррайтера, построенная с помощью обобщенного кода Рида-Соломона ? Общие подходы.

В этом разделе мы рассматриваем систему Нидеррайтера, построенную с помощью  $q$ -значного кода из ансамбля  $RS_q(n, d)$  (см. раздел 12.2.2). Как было установлено в разделе 12.2.3, соответствующая система Маклиса (система, в которой порождающие матрицы выбираются из ансамбля  $\mathcal{A}_q(n, n - d + 1)$ ) имеет примерно ту же стойкость к нападению, что и рассматриваемая система открытого шифрования.  $RS_q(n, d)$

Имеется два вида атак на систему открытого шифрования.

i. "Чтение" открытого сообщения абонента  $\mathcal{Y}$  без использования секретного ключа абонента  $\mathcal{X}$  (безключевое чтение). Напомним, что в данном случае секретным ключом являются матрицы  $h, \Gamma, D$  абонента  $\mathcal{X}$ .

ii. Вычисление секретного ключа абонента  $\mathcal{X}$  с последующим вычислением всех открытых сообщений абонента  $\mathcal{Y}$ , направляемых им абоненту  $\mathcal{X}$ .

Рассмотрим сначала атаку i.. Для ее реализации необходимо решить уравнение (12.2.4). С точки зрения нападающей стороны матрица  $B'$  является матрицей общего положения. Поэтому для нахождения решения  $e$  уравнения (12.2.4) веса  $wt(e) \leq t$  в соответствие с тезисом А необходимо проделать экспоненциальное от его длины  $n$  число операций. Поэтому можно полагать, что при достаточно большом  $n$  атака этого невозможна.

Все сказанное выше в предыдущем абзаце справедливо только в случае, когда множество всех возможных априорных значений векторов-ошибок  $e$ , переносящих открытую информацию, имеет достаточно большую мощность. Если это не так, то атака типа i. может расколоть систему. Преодолеть эту слабость достаточно просто. На этом мы останавливаться не будем.

Другой подход, реализующий атаку i., состоит в следующем. Можно "угадать" обобщенный код Рида-Соломона, определяемый проверочной матрицей  $B'$ , и произвести декодирование (решить уравнение (12.2.4)) в этом коде. По следствию 1 число таких кодов  $A_q(n, d)$  не меньше  $\frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q)\dots(q^{d-1}-q^{d-2})}$ . Это число при  $n \approx 100$ ,  $d \leq n/2$  и  $q \geq 2$  больше, чем  $10^{77}$ . Поэтому это событие очень маловероятно и его можно не рассматривать.

Таким образом, по современному представлению с учетом тезиса А безключевое чтение (атака i.) в рассматриваемой системе при некоторых дополнительных предположениях невозможно при достаточно большом  $n$ .

Рассмотрим теперь атаку ii.. Задачей в этом случае является определение матрицы  $h, \Gamma, D$ , исходя из известной матрицы  $B'$ . Как будет показано ниже и это является основным результатом раздела, указанная задача может быть решена за  $O(s^4 + sn)$  операций в поле  $\mathbb{F}_q$ .

## 12.4 Алгоритм определения секретного ключа системы открытого шифрования, использующего обобщенный код Рида-Соломона

Любая матрица  $B'$  ансамбля  $\mathcal{B}_q(n, d)$ , определенная соотношением (12.2.2), имеет вид

$$B' = \begin{pmatrix} z_1 f_0(\omega_1) & z_2 f_0(\omega_2) & \cdots & z_n f_0(\omega_n) \\ z_1 f_1(\omega_1) & z_2 f_1(\omega_2) & \cdots & z_n f_1(\omega_n) \\ z_1 f_2(\omega_1) & z_2 f_2(\omega_2) & \cdots & z_n f_2(\omega_n) \\ \vdots & \vdots & \cdots & \vdots \\ z_1 f_{d-2}(\omega_1) & z_2 f_{d-2}(\omega_2) & \cdots & z_n f_{d-2}(\omega_n) \end{pmatrix}, \quad (12.4.1)$$

где  $f_i(x) \in \mathbb{F}_q[x]$  — многочлен степени не выше  $d-2$ , который определяется  $d-1 \times d-1$  — матрицей  $h = \|h_{i,j}\|$  следующим образом  $f_i(x) = \sum_{j=0}^{d-2} h_{i,j} x^j$ . Отметим, что многочлены  $f_i(x)$  являются линейно-независимыми, ибо матрица  $h$  является невырожденной. Последовательность элементов  $(\omega_1, \omega_2, \dots, \omega_n)$  определяется перестановочной матрицей  $\Gamma$  в (12.2.2).

Итак, перед нами стоит задача: по заданной матрице  $B'$  и известной проверочной матрицы кода Рида-Соломона  $B$  найти невырожденную матрицу  $h$ , элементы  $\omega_1, \omega_2, \dots, \omega_n \in \mathbb{F}'_q = \mathbb{F}_q \cup \{\infty\}$  и элементы  $z_1, z_2, \dots, z_n \in \mathbb{F}_q \setminus \{0\}$  такие, что  $B' = h \cdot B \cdot \Gamma \cdot D$ ,  $D = \text{diag}(z_1, z_2, \dots, z_n)$ .

Задачу будем решать в два этапа: сначала найдем элементы  $\omega_1, \omega_2, \dots, \omega_n$ , а затем элементы  $z_1, z_2, \dots, z_n$  и матрицу  $h$ .

### 12.4.1 Как определить первые три элемента $\omega_j$ ?

Перед тем как искать элементы  $\omega_1, \omega_2, \dots, \omega_n$  сделаем несколько замечаний.

Пусть  $h, \Lambda$  — некоторое решение уравнения (12.4.1), т.е.  $B' = h \cdot B \cdot \Lambda$ ,  $\Lambda = \Gamma \cdot D$ , и  $\Lambda_\phi = \Gamma_\phi \cdot D_\phi$ ,  $D_\phi = \text{diag}(z'_1, z'_2, \dots, z'_n)$ , — некоторый обобщенный автоморфизм кода  $\mathcal{K}$  с порождающей матрицей  $B$  (см. 1.1.5), соответствующий дробно-линейной функции  $\phi(x)$  (см. раздел 12.0.17). Тогда решением уравнения (12.4.1) является также пара  $h', \Lambda'$ , где  $h' = h \cdot h''^{-1}$ ,  $\Lambda' = \Lambda_\phi \cdot \Lambda$ , где матрица  $h''$  определяется соотношением  $h'' \cdot B = B \cdot \Lambda_\phi$ .

Группа обобщенных автоморфизмов  $\Xi_{\mathcal{K}}$  кода  $\mathcal{K} = RS_q(n, d)$  Рида-Соломона типа 3 (см. раздел 5.0.4) действует на координатах векторов  $\mathbf{x} = (x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n})$ . Она образована всеми мономиальными матрицами  $\Lambda_\phi$  (теорема 12.0.5) и является трижды транзитивной. Смысл этого понятия объяснен в разделе 12.0.17. Поэтому найдется дробно-линейная функция  $\phi(x)$  такая, что

$$h' \cdot B \cdot \Lambda_\phi \cdot \Lambda = \begin{pmatrix} z''_1 f'_0(1) & z''_2 f'_0(0) & z''_3 f'_0(\infty) & \cdots & z''_n f'_0(\beta_n) \\ z''_1 f'_1(1) & z''_2 f'_1(0) & z''_3 f'_1(\infty) & \cdots & z''_n f'_1(\beta_n) \\ z''_1 f'_2(1) & z''_2 f'_2(0) & z''_3 f'_2(\infty) & \cdots & z''_n f'_2(\beta_n) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ z''_1 f'_{d-2}(1) & z''_2 f'_{d-2}(0) & z''_3 f'_{d-2}(\infty) & \cdots & z''_n f'_{d-2}(\beta_n) \end{pmatrix}, \quad (12.4.2)$$

Т.е. найдется такая матрица  $\Lambda_\phi \cdot \Lambda$ , что  $(x_{\omega_1}, x_{\omega_2}, \dots, x_{\omega_n}) \Lambda_\phi \cdot \Lambda = (d_1 x_1, d_2 x_0, d_3 x_\infty, \beta_4, \dots, \beta_n)$ , где  $d_\omega$  — элементы диагональной матрицы  $D'$ , определяемой соотношением  $\Lambda_\phi \cdot \Lambda = \Lambda' = \Gamma' \cdot D'$  (см. раздел 12.0.17).



Для этого, как нетрудно видеть, нужно подобрать такую функцию  $\phi(x)$ , что  $\phi(\omega_1) = \beta_1$ ,  $\phi(\omega_2) = \beta_2$ ,  $\phi(\omega_3) = \beta_3$ , где элементы  $\beta_i$  определяются тем условием, что матрица  $\Lambda$  переводит координату  $x_{\beta_1}$  в координату  $x_1$ , координату  $x_{\beta_2}$  в координату  $x_0$  и координату  $x_{\beta_3}$  в координату  $x_\infty$ .

Таким образом, всегда можно полагать, что в (12.4.1)  $\omega_1 = 1$ ,  $\omega_2 = 0$ ,  $\omega_3 = \infty$ .

## 12.4.2 Определение элементов $\omega_j$ , $j > 3$ .

Найдем такие постоянные  $c_s^{(1)}$ ,  $s = 0, \dots, d-2$ , не все равные нулю, для которых выполнено

$$z_j \sum_{s=0}^{d-2} c_s^{(1)} f_s(\omega_j) = \sum_{s=0}^{d-2} c_s^{(1)} z_j f_s(\omega_j) = 0, \quad j = 1, d, d+1, \dots, 2d-4. \quad (12.4.3)$$

Для этого необходимо решить систему однородных линейных уравнений от  $d-1$  неизвестных  $c_s^{(1)}$  с известной матрицей коэффициентов  $\|z_j f_s(\omega_j)\|$ , которая является частью матрицы  $B'$ . Эта система всегда имеет решение, так как число  $d-2$  ее уравнений меньше, чем число ее неизвестных.

Следует отметить, что все элементы  $c_s^{(1)}$  отличны от нуля, так как в противном случае в матрице  $B'$  нашлись бы  $d-1$  линейно-зависимых столбцов, что по ее построению не может иметь место.

Положим

$$F^{(1)}(x) = \sum_{s=0}^{d-2} c_s^{(1)} f_s(x). \quad (12.4.4)$$

Очевидно,

$$\gamma_i^{(1)} = \sum_{s=0}^{d-2} c_s^{(1)} z_i f_s(\omega_i) = z_i F^{(1)}(\omega_i). \quad (12.4.5)$$

Очень существенно, что элементы  $\gamma_i^{(1)}$  могут быть вычислены, исходя только из известных элементов  $z_i f_s(\omega_i)$  матрицы  $B'$ .

Поскольку элементы  $z_i$  отличны от нуля, то из (12.4.4) следует, что элементы  $\omega_j$ ,  $j = 1, d, d+1, \dots, 2d-4$  являются корнями многочлена  $F^{(1)}(x)$ . Заметим, что ни один из элементов  $\omega_1, \omega_d, \omega_{d+1}, \dots, \omega_{2d-4}$  не равен  $\infty$ , так как  $\omega_3 = \infty$ .

Степень многочлена  $F^{(1)}(x)$  не превосходит  $d-2$ , так как степени  $f_j(x)$ , из которых он составлен, также не превосходят  $d-2$ . Кроме того, многочлен  $F^{(1)}(x)$  не равен тождественно 0, ибо многочлены  $f_s(x)$  линейно-независимы, а коэффициенты  $c_s^{(1)}$  все отличны от нуля. Отсюда вытекает, что  $F^{(1)}(x) = a^{(1)}(x-1)(x-\omega_d) \cdots (x-\omega_{2d-4})$ ,  $a^{(1)} \neq 0$ .

Отметим, что  $F^{(1)}(\omega) \neq 0$ , если  $\omega \neq \omega_j$ ,  $j = 1, d, d+1, \dots, 2d-4$ ,  $\omega \neq \infty$  и  $F^{(1)}(\infty) = a^{(1)}$ .

Теперь сделаем ту же процедуру для элементов  $\omega_j$ ,  $j = 2, d, d+1, \dots, 2d-4$ . А именно, найдем такие постоянные  $c_s^{(2)}$ ,  $s = 0, \dots, d-2$ , не все равные нулю, для которых выполнено

$$\sum_{s=0}^{d-2} c_s^{(2)} f_s(\omega_j) = 0, \quad j = 2, d, d+1, \dots, 2d-4. \quad (12.4.6)$$

Положим

$$F^{(2)}(x) = \sum_{s=0}^{d-2} c_s^{(2)} f_s(x), \quad \gamma_i^{(2)} = \sum_{s=0}^{d-2} c_s^{(2)} z_i f_s(\omega_i) = z_i F^{(2)}(\omega_i). \quad (12.4.7)$$

По тем же соображениям, что и выше, имеем  $F^{(2)}(x) = a^{(2)}x(x-\omega_d)\cdots(x-\omega_{2d-4})$ ,  $a^{(1)} \neq 0$ .

Рассмотрим функцию

$$\theta(x) = \frac{F^{(1)}(x)}{F^{(2)}(x)} = \frac{a^{(1)}(x-1)}{a^{(2)}x} \quad (12.4.8)$$

— отношение многочленов  $F^{(1)}(x)$  и  $F^{(2)}(x)$ . Как уже было замечено,  $F^{(i)}(\omega) \neq 0$ ,  $i = 1, 2$ , если  $\omega \neq \omega_j$ ,  $j = 1, 2, d, d+1, \dots, 2d-4$ ,  $\omega \neq \infty$ . Таким образом, мы можем вычислить значение функции  $\theta(x)$  во всех точках  $\omega_j$  за исключением  $j = d, d+1, \dots, 2d-4$  с точностью до постоянного множителя  $\frac{a^{(1)}}{a^{(2)}}$ .

Множитель  $\frac{a^{(1)}}{a^{(2)}}$  можно вычислить, если положить  $x = \infty$  (значению  $\omega_3$ ) в  $\theta(x)$ . В этом случае  $z_3 F^{(i)}(\infty) = \sum_{s=0}^{d-2} c_s^{(i)} z_3 f_s(\infty)$ ,  $i = 1, 2$ . Таким образом, значение  $\theta(\infty)$  может быть вычислено непосредственно, исходя из матрицы  $B'$ , ибо  $z_3 f_s(\infty)$  — элементы третьего столбца  $B'$ . Для полноты изложения заметим, что  $F^{(i)}(\infty) \neq 0$ , ибо по построению среди всех  $d-2$  корней многочлена  $F^{(i)}(x)$ , степени не выше  $d-2$ , нет корня  $\infty$ . Отсюда вытекает, что

$$\theta(x) = \frac{F^{(1)}(\infty)}{F^{(2)}(\infty)} \left( \frac{x-1}{x} \right) \quad (12.4.9)$$

Как уже отмечалось, значения многочленов  $F^{(i)}(x)$  и, следовательно, значение  $e_\omega = \theta(\omega)$  дробно-линейной функции  $\theta(x)$  можно вычислить в любой точке  $\omega \in \mathbb{F}'_q$  за исключением  $\omega \neq \omega_j$ ,  $j = 1, 2, d, d+1, \dots, 2d-4$ ,  $\omega \neq \infty$ . Отсюда вытекает, что

$$\omega_j = \theta^{-1}(e_{\omega_j}), \quad j \neq 1, 2, 3, d, d+1, \dots, 2d-4 \quad (12.4.10)$$

Заметим, впрочем, что элементы  $\omega_i$ ,  $i = 1, 2, 3$ , уже известны.

Функция  $\theta^{-1}(x)$ , как нетрудно вычислить, равна  $\theta^{-1}(x) = \frac{F^{(1)}(\infty)}{F^{(1)}(\infty) - x F^{(2)}(\infty)}$ . Таким образом, мы можем определить значения  $\omega_j$  для всех  $j$ , исключая  $j = d, d+1, \dots, 2d-4$ .

Недостающие  $\omega_j$  можно определить, если выбрать другие элементы, определяющие многочлены  $F^{(i)}(x)$ . Скажем, в качестве такого набора для определения  $F^{(1)}(x)$  можно взять

элементы  $1, \omega_{2d-3}, \omega_{2d-2}, \dots, \omega_{3d-6}$  и с их помощью вычислить недостающие  $\omega_j$ ,  $j = d, d+1, \dots, 2d-4$ .

В этом разделе произведена самая основная и трудная работа: найдена первая часть секретного ключа — элементы  $\omega_j$  для всех  $j$ . Вся остальная работа по определению оставшейся части ключа, а именно определению коэффициентов  $z_i$  и матрицы  $h$ , как это обычно и бывает, является более легкой и может быть произведена различными способами. Один из них излагается ниже.

Помимо этого заметим, что мы использовали нетривиальные свойства подгруппы группы автоморфизмов кода Рида-Соломона, а именно ее трижды транзитивность. Если бы подгруппа была только дважды транзитивной, то мы, например не смогли бы вычислить

множитель  $\frac{a^{(1)}}{a^{(2)}}$  и должны были бы его угадывать (опробовать). Следовательно, сложность всего алгоритма существенно увеличилась бы.

Трудозатраты этой части алгоритма, как нетрудно подсчитать, не больше  $O(d^3 + dn)$ . Детального обоснования этой оценки производить не будем.

### 12.4.3 Определение элементов $z_j$ и матрицы $h$ .

Заметим, что если каждый элемент матрицы  $\Lambda$  умножить на  $a \in \mathbb{F}_q \setminus \{0\}$ , а каждый элемент  $h$  на  $a^{-1}$ , то произведение  $B' = h \cdot B \cdot \Lambda$  останется неизменным. Поэтому можно считать, что  $z_1 = 1$ .

Найдем такие элементы  $c_1, c_2, \dots, c_d$ , что

$$\sum_{s=1}^d c_s z_s f_j(\omega_s) = 0, \quad j = 0, \dots, d-2. \quad (12.4.11)$$

Отметим, что все элементы  $c_1, c_2, \dots, c_d$  отличны от нуля, поскольку в противном случае код с проверочной матрицей  $B'$  имел бы кодовое расстояние меньше  $d$  (см. раздел 5.3).

Соотношение (12.4.11) в матричной форме имеет вид

$$B_d'' \cdot \text{diag}(z_1, z_2, \dots, z_d)(c_1, c_2, \dots, c_d)^T = 0, \quad (12.4.12)$$

где  $B_d'' = (f_i(\omega_j))$ ,  $i = 0, 1, \dots, d-2$ ,  $j = 1, 2, \dots, d$  — матрица размера  $d-1 \times d$ . Заметим, что матрица  $B_d'' \cdot \text{diag}(z_1, z_2, \dots, z_d)$  является матрицей, совпадающей с первыми  $d$  столбцами матрицы  $B'$ . Как нетрудно видеть  $B_d'' = h \cdot B_d$ , где

$$B_d = \begin{pmatrix} \omega_1^0 & \omega_2^0 & \cdots & \omega_d^0 \\ \omega_1 & \omega_2 & \cdots & \omega_d \\ \omega_1^2 & \omega_2^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{d-2} & \omega_2^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \quad (12.4.13)$$

Откуда и из (12.4.12) вытекает, что

$$h \cdot B_d \cdot \text{diag}(z_1, z_2, \dots, z_d)(c_1, c_2, \dots, c_d)^T = 0, \quad (12.4.14)$$

или

$$B_d \cdot \text{diag}(c_1, c_2, \dots, c_d) \cdot (z_1, z_2, \dots, z_d)^T = 0. \quad (12.4.15)$$

Соотношение (12.4.15) мы будем рассматривать как линейную систему уравнений относительно неизвестных  $z_2, z_3, \dots, z_d$  с учетом того, что ненулевые элементы  $c_1, c_2, \dots, c_d$  и элементы  $\omega_1, \omega_2, \dots, \omega_d$  уже известны, а  $z_1 = 1$ . Эта система имеет единственное решение, поскольку ее матрица коэффициентов

$$\begin{pmatrix} \omega_2^0 & \omega_3^0 & \cdots & \omega_d^0 \\ \omega_2 & \omega_3 & \cdots & \omega_d \\ \omega_2^2 & \omega_3^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_2^{d-2} & \omega_3^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \cdot \text{diag}(c_2, c_3, \dots, c_d) \quad (12.4.16)$$

является, очевидно, невырожденной. Решая эту систему, найдем элементы  $z_1, z_2, \dots, z_d$ .

Найдем теперь элементы матрицы  $h = (h_{i,j})$ ,  $i, j = 0, \dots, d-2$ . Имеем

$$z_j \sum_{s=0}^{d-2} h_{i,s} \omega_j^s = z_j f_i(\omega_j). \quad (12.4.17)$$

Зафиксировав какое-либо  $i$ ,  $0 \leq i \leq d-2$ , и изменяя  $j$  от 1 до  $d-1$ , получим систему линейных уравнений с неизвестными  $h_{i,0}, h_{i,1}, \dots, h_{i,d-2}$ . Определитель этой системы является определителем Вандермонда, поэтому ее решение  $h_{i,0}, h_{i,1}, \dots, h_{i,d-2}$  находится однозначно. Решив эту систему для каждого  $i$  мы найдем матрицу  $h$ .

Таким образом, мы сумели определить матрицу  $h$ , элементы  $\omega_1, \omega_2, \dots, \omega_d$  и элементы  $z_1, z_2, \dots, z_d$ . Для того чтобы определить оставшиеся элементы  $z_{d+1}, z_{d+2}, \dots, z_n$  проще всего поступить следующим образом.

Умножим матрицу  $B'$  слева на матрицу  $h^{-1}$ . В результате получим матрицу

$$h^{-1} \cdot B' = \begin{pmatrix} z_1 \omega_1^0 & z_2 \omega_2^0 & \cdots & z_n \omega_n^0 \\ z_1 \omega_1 & z_2 \omega_2 & \cdots & z_n \omega_n \\ z_1 \omega_1^2 & z_2 \omega_2^2 & \cdots & z_n \omega_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1 \omega_1^{d-2} & z_2 \omega_2^{d-2} & \cdots & z_n \omega_n^{d-2} \end{pmatrix}, \quad (12.4.18)$$

Вид последней матрицы делает задачу определения элементов  $z_{d+1}, z_{d+2}, \dots, z_n$  тривиальной.

Число операций, требуемых для реализации этой части алгоритма по определению оставшейся части ключа (матрицы  $h$  и всех элементов  $z_j$ ) не выше  $O(d^4 + dn)$ . Таким образом, общее число операций по реализации всего алгоритма не более, чем  $O(d^4 + dn)$ . Следовательно, сложность этого алгоритма является полиномиальной от длины  $n$  используемого кода. Соответствующая система открытого шифрования как Маклиса так и Нидеррайтера, построенная на коде Рида-Соломона, не является стойкой. Это основной результат данного раздела.

## 12.4.4 Заключительные замечания

Естественно встает вопрос о модернизации рассмотренной системы шифрования для того, чтобы увеличить ее стойкости. Наиболее естественный путь является выбор для ее построения другого кода — не Рида-Соломона. Напомним, что для использования в системе шифрования подходит только тот код, который имеет легкое декодирование. Таких кодов известно не очень много.

Возможно, подходящим вариантом может послужить обобщенный код Боуза-Чоудхури-Хоквингема длины  $n = q+1$  (см. конец раздела 5.3) над полем  $\mathbb{F}_r$ , где число  $r$  существенно меньше числа  $q$ . Нечетко выражаясь, в этом случае построить многочлены  $F^{(i)}(x)$  не удастся из-за того, матрица  $h$ , определенная над  $\mathbb{F}_r$ , "размазывает"  $z_j$  между различными коэффициентами многочленов  $f_j(x)$ . Имеются и некоторые другие сложности. Вместе с тем у автора имеются основания того, что системы шифрования, построенная на основе обобщенного кода Боуза-Чоудхури-Хоквингема, может быть расколота за полиномиальное время. Исследование криптографических свойств такой системы является достаточно привлекательным направлением для самостоятельной работы.

Другим направлением является использование в системе шифрования двоичных кодов Рида-Маллера. В работе [31] рассмотрена такая система и ее модификации. Проведен подробный анализ ее криптографических свойств. В частности, оценена ее стойкость, которая оказалась достаточно высокой.

Третьем направлением являются алгебро-геометрические коды. Эти коды образуют значительно более мощные ансамбли по сравнению с ансамблями, построенными с помощью кода Рида-Соломона. Происходит это из-за того, что мы можем варьировать не только матрицы  $h$  и  $\Lambda$ , как в случае использования кода Рида-Соломона, но и вид алгебраической кривой, с помощью которой построен этот код. Это является очень мощным методом маскировки свойств открытого ключа — проверочной матрицы  $B'$ .

Несколько неопубликованных работ по этому направлению написаны С. О. Шестаковым.

Четвертым совсем не исследованным направлением является использование каскадных кодов или сверточных кодов. По мнению автора на этом направлении могут быть найдены хорошие системы открытого шифрования. Это направление также является перспективным для самостоятельного исследования.



# Глава 13

## Совершенная секретность в полилинейных системах распределения ключей

### 13.1 Модель системы распределения ключей

#### 13.1.1 Введение

В большинстве многопользовательских системах связи возникает необходимость в секрете, который является общим для некоторого подмножества пользователей. Наиболее часто под секретом понимают общий криптографический ключ, имея который несколько пользователей (абонентов) системы могут осуществить с помощью симметрического шифрования обмен информацией по открытому каналу связи. Естественно, эта подмножество абонентов желает иметь такой ключ, который был бы недоступен в том или ином смысле другим пользователям системы.

Для группы из двух пользователей наиболее известной системой подобного типа является система Диффи-Хеллмана, в которой общим ключом пользователей служит элемент циклической группы большого порядка, который независимо один от другого вычисляется каждым пользователем, используя для этого только собственный секретный ключ и общедоступную информацию (см., например, Энциклопедия дискр. мат. [2], статья Криптография).

Система Диффи-Хеллмана является без коммутационной (noncommunicating) в том смысле, что для вычисления ключа двум пользователям не надо обмениваться между собой какой-либо дополнительной информацией. Для вычисления ключа каждый пользователь использует только свой секретный ключ и общедоступный открытый ключ другого пользователя.

В системе Диффи-Хеллмана общий ключ двух пользователей недоступен злоумышленнику из-за того, что для его вычисления ему (злоумышленнику) необходимо решить сложную математическую задачу. Для решения этой задачи необходимо произвести вычисления, сложность которых предположительно так высока, что она не может быть реализована на современной вычислительной технике. Например, для системы Диффи-Хеллмана такой сложной задачей является задача логарифмирования в мультипликативной группе

конечного поля или аддитивной группе точек эллиптической кривой над конечным полем.

Системы, которые будут рассматриваться ниже также являются без коммутационными. В отличие от системы Диффи-Хеллмана недоступность общего ключа группы абонентов в этих системах является абсолютной или, как еще говорят, система имеет совершенную секретность. Говоря немного точнее, если число нечестных пользователей в системе не слишком велико, то информация об общем ключе группы абонентов в случае, когда злоумышленнику известны ключевые данные всех нечестных пользователей, совпадает с априорной информацией об этом ключе. Другими словами, апостериорная информация для злоумышленника при условии знания им ключевых данных нескольких нечестных абонентов совпадает с априорной информацией об этом ключе, т.е. ключ является совершенно секретным.

Таким образом, стойкость системы Диффи-Хеллмана относительная, в тоже время как стойкость в рассматриваемой ниже системе — абсолютная. В этом заключено основное криптографическое различие систем типа Диффи-Хеллмана и систем распределения ключей, рассматриваемых ниже.

В настоящем разделе рассматриваются, так называемые полилинейные ключевые системы, частным видом которых является структуры, предложенные в работе Блома [75]. К настоящему времени известно, по меньшей мере, одно существенное обобщение указанной работы Блома (см. [52], [51]). В настоящем разделе мы рассмотрим другое обобщение результатов Блома, которое отлично от обобщения работ [52], [51] и включает его как частный случай.

Следует также сказать, что хотя основной результат работы Блома верен, нельзя признать его обоснование в работе [75] полным. То же можно сказать и относительно основного результата работ [52], [51]. Результаты настоящего раздела восполняют этот недостаток.

### 13.1.2 Вводные замечания

Систему распределения ключей с  $N$  пользователями для конференций размера  $t$ , т.е. для конференций с  $t$  участниками, которая обеспечивает безопасность в присутствии коалиции из  $w$  нечестных пользователей мы будем обозначать как  $(t, w)$ —система. Если  $t = 2$ , то  $(2, w)$ —систему называем полнодоступной системой парных связей.

Для того чтобы  $(t, w)$ —система могла функционировать, каждый пользователь должен получить некоторую порцию исходной секретной ключевой информации. После начального распределения порций секретной ключевой информации среди всех пользователей, система может функционировать, имея следующие свойства

1. Пусть  $T$ ,  $|T| = t$ , — произвольное подмножество множества всех пользователей. Это подмножество мы называем конференцией с  $t$  участниками. Каждый участник конференции, используя только свою порцию ключевой информации, имеет возможность вычислить ключ, который является одинаковым у всех участников конференции  $R$ . Этот ключ называется общим ключом конференции  $R$ . Построение общего ключа не требует какого-либо обмена информацией между членами коалиции.
2. Каждая коалиция  $W$ ,  $|W| = w$ , (подмножество множества всех пользователей) из  $w$  нечестных пользователей не может получить никакой информации об общем ключе конференции  $R$ .



### 13.1.3 Математическая модель системы распределения ключей

Математическая модель системы распределения ключей  $\mathcal{S}_N$  состоит из следующих объектов:

1. Множества  $\mathbf{N}$ ,  $|\mathbf{N}| = N$ , пользователей (абонентов), элементы которого мы будем индексировать элементами множества  $\mathcal{Q} = \{\mathbf{a}_1, \dots, \mathbf{a}_N\}$ , т.е.  $\mathbf{N} = \{\mathbf{N}_{\mathbf{a}_1}, \dots, \mathbf{N}_{\mathbf{a}_N}\}$ . Фактически далее мы будем работать только с множеством  $\mathcal{Q}$ , мысленно связывая элемент  $\mathbf{a} \in \mathcal{Q}$  с пользователем  $\mathbf{N}_{\mathbf{a}}$ .
2. Исходного множества независимых секретных ключей  $\mathcal{K}$ , которое генерируется неким центром доверия, свойства, права и возможности которого мы обсуждать не будем. Каждый ключ в рассматриваемой системе распределения ключей является некоторой суммой с коэффициентами из поля  $\mathbb{F}_q$  элементов из  $\mathcal{K}$ , т.е. ключ является элементом линейной оболочки  $L(\mathcal{K})$  над конечным полем  $\mathbb{F}_q$  множества  $\mathcal{K}$ .
3. Подмножеств  $\mathcal{K}_{\mathbf{a}} \subset L(\mathcal{K}_{\mathbf{a}})$ , созданных центром доверия для каждого  $\mathbf{a} \in \mathcal{Q}$ . Каждое подмножество  $\mathcal{K}_{\mathbf{a}}$  центр доверия передает пользователю  $\mathbf{a}$ , а пользователь  $\mathbf{a}$  использует его для построения общего ключа конференции, в которую он входит. Отметим, что множество  $\mathcal{K}_{\mathbf{a}}$  является единственной секретной ключевой информацией пользователя  $\mathbf{a}$ .
4. Общеизвестного алгоритма  $\mathcal{A}$  со следующими свойствами. Пусть  $T = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$  — подмножество множества  $\mathcal{Q}$ , называемое конференцией с  $t$  участниками. Алгоритм  $\mathcal{A}$  позволяет каждому пользователю  $\mathbf{a} \in T$  вычислить один и тот же общий ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции  $T$ , используя для этого только свое подмножество  $\mathcal{K}_{\mathbf{a}}$ . Мы предполагаем, что множество  $\mathbf{a}_1, \dots, \mathbf{a}_t$  индексов, участников конференции  $T$  является общеизвестным, вместе с тем ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$ , вычисленный каждым участником конференции  $T$ , является секретным для других не входящих в конференцию  $T$  пользователей системы.

Секретный ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  обычно используется участниками конференции для симметричного шифрования информации, которой они обмениваются, либо для их взаимной идентификации.

Следует сказать, что системы распределения ключей, основанные на использовании дизъюнктивных кодов и описанные в главе 14, раздел 14.4, плохо вкладываются с вышеприведенную математическую модель. Поэтому такие системы рассматриваются отдельно в разделе 14.4.

В связи с этим естественно рассматривать два типа систем распределения ключей. Тип I — это дизъюнктивные коды и тип II — системы, математическая модель которых описана выше. Грубо говоря тип II отличается от типа I тем, что в первых допускаются алгебраические операции с ключами при вычислении общего ключа конференции, а системах типа I никаких алгебраических операций с ключами не производится. Можно также сказать, что системы второго типа эффективнее систем первого типа в некоторых криптографических приложениях, так как они обладают более широкими возможностями. Вместе с тем системы первого типа имеют значительно более широкое поле для применений.

То, что мы будем рассматривать ниже является достаточно узким случаем систем типа II. Их естественно назвать полилинейными. Системы типа II другого вида описаны в работах [52], [51]. Им посвящен раздел 13.4.1.

Вопрос о том, какой мерой мерить эффективность, рассматриваемых ниже  $(t, w)$ –систем является не очень простым. В работе [50] и некоторых других предложено в качестве меры сложности  $(t, w)$ –системы  $\mathcal{S}$  использовать функцию  $D'(\mathcal{S}) = |M|^{k(t,w)}$ , где  $M$  — множество из которого выбираются ключи системы и  $k(t, w)$  — число секретных ключей, которые хранит каждый пользователь  $(t, w)$ –системы.

Это, по мнению автора достаточно разумное предложение, которое мы после незначительной его модификации будем использовать в данной работе. Модификация состоит в том, что вместо функции  $D'(\mathcal{S})$  мы будем использовать ее двоичный логарифм, т.е. в качестве меры сложности  $(t, w)$ –системы будем далее использовать функцию

$$D(\mathcal{S}) = k(t, w) \log_2 |M| \quad (13.1.1)$$

Например, если  $M$  — множество всех двоичных векторов длины  $n$ , то  $D(\mathcal{S}) = k(t, w)n$ , где  $n$  в данном случае можно трактовать как длину ключа или как число бит (двоичных ячеек), требуемых для его сохранения в электронной памяти.

В наших обозначениях, как легко установить, сложность двоичной  $(2, w)$ –системы Блома  $\mathcal{S}_B$ , т.е. системы в которой используются коды Рида-Соломона над полем  $\mathbb{F}_{2^m}$  с длиной ключа над полем  $\mathbb{F}_{2^m}$  равной  $s$ , принимает значение  $D(\mathcal{S}) = ms(w + 1)$ .

## 13.2 Определение полилинейной системы распределения ключей $\mathcal{S}$

Пусть  $\mathbb{F}_q^n$  —  $n$ –мерное пространство над конечным полем  $\mathbb{F}_q$  с  $q = p^l$  элементами. Нам удобно в качестве множества пользователей  $\mathcal{Q}$  рассматривать подмножество  $\mathcal{Q} = \{\mathbf{a}_1, \dots, \mathbf{a}_N\} \subseteq \mathbb{F}_q^n$ , которое мы называем множеством индексов пользователей. Иногда элемент  $\mathcal{Q}$  мы называем для краткости просто пользователем.

Будем полагать, что каждый ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции  $T = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$  является линейной функцией, определяемой множеством  $T$ , от элементов множества  $\mathcal{K} = \{k_1, \dots, k_D\}$ . Множество  $\mathcal{K}$  мы называем исходным множеством независимых секретных ключей системы распределения.

Можно полагать, что элементами  $\mathcal{K}$  являются линейно-независимые элементы некоторого пространства  $\mathbb{F}_q^u$  с достаточно большим значением размерности  $u$ , т.е.  $\mathcal{K} \subset \mathbb{F}_q^u$ . Заметим, что элементы множества  $\mathcal{K}$  можно складывать с умножением на скаляры из  $\mathbb{F}_q$ . В результате чего возникают новые ключи. Подобная интерпретация элементов множества  $\mathcal{K}$ , как элементов пространства  $\mathbb{F}_q^u$  хотя и естественна, но неудобна по некоторым причинам, которые мы здесь не будем приводить.

Мы будем полагать, что элементами множества  $\mathcal{K} = \{\xi_1, \dots, \xi_D\}$  являются случайные величины  $\xi_j$ , каждая из которых равномерно распределенна на элементах множества  $\mathbb{F}_q^u$ . Мы также полагаем, что различные случайные величины из  $\mathcal{K}$  являются независимыми в совокупности. Последнее свойство, в частности, означает, что любая ненулевая сумма

элементов множества  $\mathcal{K}$  является случайной величиной, равномерно распределенной на множестве  $\mathbb{F}_q^u$ .

В данной интерпретации каждый ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является суммой с коэффициентами из  $\mathbb{F}_q$  (не всеми равными нулю) элементов множества  $\mathcal{K}$ , т.е. каждый ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является одним из ненулевых элементов линейной оболочки  $L(\mathcal{K})$ , натянутой на множество исходных ключей  $\mathcal{K}$ . Из определения множества  $\mathcal{K}$  вытекает, что любой ключ является случайной величиной, равномерно распределенной на пространстве  $\mathbb{F}_q^u$ . Размерность линейного пространства  $L(\mathcal{K})$  равна  $|\mathcal{K}|$ , ибо все элементы множества  $\mathcal{K}$  по определению являются линейно-независимыми.

Отметим, что если мы рассматриваем некоторое множество из ключей  $k_1, \dots, k_j$  системы  $\mathcal{S}$ , то они в совокупности, вообще говоря, не являются независимыми случайными элементами: некоторые их суммы с коэффициентами из  $\mathbb{F}_q$  могут оказаться тождественно равными нулю.

**Лемма 13.2.1** *Если ключ  $k \in \mathcal{K}$  линейно независим от ключей множества  $k_1, \dots, k_j$ , т.е. ключ  $k$  нельзя представить в виде линейной комбинации ключей  $k_1, \dots, k_j$ , то вероятность того, что ключ  $k$  примет определенное значение на пространстве  $\mathbb{F}_q^u$  не зависит от значений, принимаемых случайными величинами  $k_{\mathbf{c}_1}, \dots, k_{\mathbf{c}_j}$ . Другими словами, если ключ  $k \in \mathcal{K}$  линейно независим от ключей множества  $k_1, \dots, k_j$ , то*

$$P(k = \mathbf{x}/k_1, \dots, k_j) = P(k = \mathbf{x}). \quad (13.2.1)$$

**Доказательство** леммы очевидно.  $\square$

В действительности, при практическом использовании структуры каждый элемент исходного множества секретных ключей  $\mathcal{K}$  представляет собой реализацию соответствующей случайной величины. В результате каждый ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  станет некоторым элементом пространства  $\mathbb{F}_q^u$ . В этом случае утверждение леммы (13.2.1) означает, что злоумышленник, который знает ключи  $k_1, \dots, k_j$  не имеет никакой дополнительной информации о ключе  $k$ , если ключ  $k$ , как случайная величина, линейно не зависит от ключей множества  $k_1, \dots, k_j$  в смысле указанном в условии этой леммы.

Каждый пользователь  $\mathbf{a} \in Q$  системы  $\mathcal{S}$  снабжается центром доверия своим множеством секретных ключей  $\mathcal{K}_{\mathbf{a}} = \{k_{\mathbf{a},1}(\mathcal{K}), \dots, k_{\mathbf{a},n}(\mathcal{K})\}$ , где  $k_{\mathbf{a},j}(\mathcal{K})$ ,  $j = 1, \dots, n$ , — значение некоторой линейной функции, зависящей от всех элементов множества  $\mathcal{K}$ . Явный вид функции  $k_{\mathbf{a},j}(\mathcal{K})$  будет указан ниже.

### 13.2.1 Свойства ключевой системы

**Определение 13.2.1** *Ключ  $k \in L(\mathcal{K})$  называется скомпрометированным относительно множества ключей  $G \subseteq L(\mathcal{K})$ , если он входит в линейную оболочку  $L(G)$  над полем  $\mathbb{F}_q$  ключей из множества  $G$ . В противном случае он называется нескомпрометированным.*

По другому можно сказать, что если  $k$  — нескомпрометированный ключ, то случайная величина  $k$  не зависит от совокупности случайных величин, входящих в множество  $G$ . Отсюда, в частности, следует, что в рамках рассмотренной выше интерпретации ключей информация о нескомпрометированном ключе  $k$  не содержится в значениях, принимаемых ключами из множества  $G$ . Таким образом, нескомпрометированный ключ является

совершенно секретным в теоретико-информационном смысле относительно ключей множества  $G$ .

Как уже указывалось, элементами множества  $\mathcal{Q}$  (множество индексов пользователей системы  $\mathcal{S}$ ) являются элементы  $\mathbf{a}$  пространства  $\mathbb{F}_q^n$ .

Мы полагаем, что в системе  $\mathcal{S}$  имеется заранее неизвестная коалиция (множество)  $\mathcal{T}_w = \{\mathbf{a}_1, \dots, \mathbf{a}_w\} \subset \mathcal{Q}$  пользователей, называемых злоумышленниками (предателями, traitors), которые пытаются вычислить общий ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции пользователей  $\mathcal{T} = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$ . Мы всегда будем полагать, что  $\mathcal{T} \cap \mathcal{T}_w = \emptyset$ .

С коалицией  $\mathcal{T}_w$  мы связываем множество скомпрометированных ключей

$$\mathcal{K}(\mathcal{T}_w) = \bigcup_{\mathbf{a} \in \mathcal{T}_w} \mathcal{K}_{\mathbf{a}} \quad (13.2.2)$$

и его линейную оболочку  $L(\mathcal{K}(\mathcal{T}_w))$ .

**Определение 13.2.2** *Ключевая система  $\mathcal{S}$  называется устойчивой относительно  $w$ -коалиции  $\mathcal{T}_w = \{\mathbf{a}_1, \dots, \mathbf{a}_w\} \subset \mathcal{Q}$ , если для всех множеств  $\mathcal{T} = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$  таких, что  $\mathcal{T} \cap \mathcal{T}_w = \emptyset$ , выполнено*

$$k_{\mathbf{a}_1, \dots, \mathbf{a}_t} \notin L(\mathcal{K}(\mathcal{T}_w)). \quad (13.2.3)$$

*т.е. если все ключи  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  являются нескомпрометированным относительно коалиции  $\mathcal{T}_w$ .*

**Определение 13.2.3** *Ключевая система  $\mathcal{S}$  называется устойчивой к  $w$  компрометациям (обозначение  $(t, w)$ -система), если она устойчива относительно всех  $w$ -коалиций  $\mathcal{T}_w = \{\mathbf{a}_1, \dots, \mathbf{a}_w\} \subset \mathcal{Q}$ . Такую  $(t, w)$ -систему мы обозначаем через  $\mathcal{R}_{t,w}(\mathcal{Q})$ .*

Мы рассматриваем следующую задачу: как при заданных числах  $N = |\mathcal{Q}|$ ,  $t$  и  $w$  построить систему распределения ключей  $\mathcal{R}_{t,w}(\mathcal{Q})$ , которая имеет достаточно малое значение параметра  $D(\mathcal{R}_{t,w}(\mathcal{Q}))$  (его определение см. в (13.1.1))

### 13.3 Конструкция полилинейной $(t, w)$ -системы распределения ключей

Конкретизируем введенные понятия. А именно, будем полагать, что

- i. Множество  $\mathcal{Q}$  индексов пользователей системы является подмножеством пространства  $\mathbb{F}_q^n$ :  $\mathcal{Q} \subset \mathbb{F}_q^n$ .
- ii. Множество  $\mathcal{K}$  независимых секретных ключей имеет вид  $\mathcal{K} = \{\xi_{i_1, \dots, i_t} \mid 1 \leq i_1 \leq i_2 \leq \dots \leq i_{t-1} \leq i_t \leq n\}$ . Мы полагаем, что  $\xi_{j_1, \dots, j_t} = \xi_{i_1, \dots, i_t}$ , если набор  $j_1, \dots, j_t$  является перестановкой некоторого набора  $i_1, \dots, i_t$  такого, что  $1 \leq i_1 \leq i_2 \leq \dots \leq i_{t-1} \leq i_t \leq n$ . Таким образом, множество  $\mathcal{K}$  образовано независимыми случайными величинами вида  $\xi_{j_1, \dots, j_t}$ , где  $1 \leq j_1 \leq \dots \leq j_t \leq n$ . Как нетрудно показать, множество  $\mathcal{K}$  содержит  $\binom{n+t-1}{t}$  элементов (независимых случайных величин). (Упражнение).

iii. Подмножество  $\mathcal{K}_{\mathbf{a}}$ ,  $\mathbf{a} = (a_1, \dots, a_n) \in \mathcal{Q}$ , образовано  $\binom{n+t-2}{t-1}$  элементами вида

$$\xi_{i_1, \dots, i_{t-1}}(\mathbf{a}) = \sum_{i=1}^n a_i \xi_{i_1, \dots, i_{t-1}, i}, \quad 1 \leq i_1 \leq i_2 \leq \dots \leq i_{t-1} \leq n. \quad (13.3.1)$$

Мы полагаем, что  $\xi_{i_1, \dots, i_{t-1}}(\mathbf{a}) = \xi_{j_1, \dots, j_{t-1}}(\mathbf{a})$ , если набор  $j_1, \dots, j_{t-1}$  является перестановкой некоторого набора  $i_1, \dots, i_{t-1}$  такого, что  $1 \leq i_1 \leq i_2 \leq \dots \leq i_{t-1} \leq n$ .

Мы будем представлять множество  $\mathcal{K}_{\mathbf{a}}$  в виде  $\binom{n+t-2}{t-1}$ -мерного вектора, координатами которого являются элементы  $\xi_{i_1, \dots, i_{t-1}}(\mathbf{a})$ ,  $1 \leq i_1 \leq \dots \leq i_{t-1} \leq n$ . Вектор  $\mathcal{K}_{\mathbf{a}}$  будем называть ключевым вектором пользователя  $\mathbf{a}$ .

iv. Общий ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции пользователей  $\mathbf{a}_1, \dots, \mathbf{a}_t$  имеет вид

$$k_{\mathbf{a}_1, \dots, \mathbf{a}_t} = \sum_{j_1, j_2, \dots, j_{t-1}=1}^n a_{1, j_1} a_{2, j_2} \dots a_{t-1, j_{t-1}} \xi_{j_1, \dots, j_{t-1}}(\mathbf{a}_t) = \sum_{j_1, j_2, \dots, j_t=1}^n a_{1, j_1} a_{2, j_2} \dots a_{t, j_t} \xi_{j_1, \dots, j_t}. \quad (13.3.2)$$

Отметим, что первое равенство в (13.3.2) показывает, что ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  может быть вычислен пользователем  $\mathbf{a}_t$ , а второе показывает, что ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является одинаковым у всех пользователей  $\mathbf{a}_1, \dots, \mathbf{a}_t$  из-за того, что случайная величина  $\xi_{j_1, \dots, j_t}$  по ее определению не меняется при перестановке порядка следования ее индексов.

Ключевую систему, построенную в соответствии с п.i - п.iv будем обозначать через  $\mathcal{R}_t(\mathcal{Q})$ .

Функция  $J(\mathbf{x}_1, \dots, \mathbf{x}_t) = \sum_{j_1, j_2, \dots, j_t=1}^n x_{1, j_1} x_{2, j_2} \dots x_{t, j_t} \xi_{j_1, \dots, j_t}$  является симметричной полилинейной формой от координат векторов  $\mathbf{x}_1, \dots, \mathbf{x}_t$ . Слово симметричная означает, что значение формы  $J(\mathbf{x}_1, \dots, \mathbf{x}_t)$  не меняется при перестановке векторов множеств  $\mathbf{x}_1, \dots, \mathbf{x}_t$ , а слово полилинейная — то, что она линейна по каждой координате  $\mathbf{x}_j$ :  $J(\mathbf{x}_1, \dots, a\mathbf{x}_j' + b\mathbf{x}_j, \dots, \mathbf{x}_t) = aJ(\mathbf{x}_1, \dots, \mathbf{x}_j, \dots, \mathbf{x}_t) + bJ(\mathbf{x}_1, \dots, \mathbf{x}_j', \dots, \mathbf{x}_t)$ ,  $a, b \in \mathbb{F}_q$ .

Мы рассмотрим вопрос о том как меняется форма  $J(\mathbf{x}_1, \dots, \mathbf{x}_t)$  при линейном преобразовании векторов  $\mathbf{x}_1, \dots, \mathbf{x}_t$  с помощью невырожденной матрицы  $P = \|p_{i,j}\|_{i,j=1, \dots, n}$ .

**Лемма 13.3.1** Если  $\mathbf{x}_1 = \mathbf{y}_1 P, \dots, \mathbf{x}_t = \mathbf{y}_t P$ , то форма  $J(\mathbf{x}_1, \dots, \mathbf{x}_t)$  в новых переменных  $\mathbf{y}_1, \dots, \mathbf{y}_t$  имеет следующий вид

$$J(\mathbf{x}_1, \dots, \mathbf{x}_t) = \sum_{j_1, j_2, \dots, j_t=1}^n y_{1, j_1} y_{2, j_2} \dots y_{t, j_t} \xi'_{j_1, \dots, j_t}, \quad (13.3.3)$$

где  $\xi'_{j_1, \dots, j_t} = \xi'_{j_1, \dots, j_t}$ , если набор  $j_1, \dots, j_t$  является перестановкой набора  $i_1, \dots, i_t$  и случайные величины вида  $\xi'_{j_1, \dots, j_t}$ ,  $1 \leq j_1 \leq \dots \leq j_t \leq n$  являются независимыми в совокупности, т.е. свойства случайных величин  $\xi'_{j_1, \dots, j_t}$  полностью совпадают со свойствами случайных величин  $\xi_{i_1, \dots, i_t}$ .

**Доказательство.** Обозначим через  $\pi$  перестановку координат символов множества  $(1, \dots, n)$ . Покажем, что для любой перестановки  $\pi$  выполнено  $\xi'_{i_1, \dots, i_t} = \xi'_{\pi(i_1), \dots, \pi(i_t)}$ .

Действительно, если  $\mathbf{x}_k = \mathbf{y}_k P$ , то  $x_{k,s} = \sum_{j=1}^n y_{k,j} p_{j,s}$ , где  $x_{k,s}$  и  $y_{k,j}$  —  $s$ -ая и  $j$ -ая координаты векторов  $\mathbf{x}_k$  и  $\mathbf{y}_k$ . Отсюда следует, что

$$\begin{aligned} J(\mathbf{x}_1, \dots, \mathbf{x}_t) &= \sum_{j_1, j_2, \dots, j_t=1}^n \left( \sum_{s=1}^n y_{1,s} p_{s,j_1} \right) \left( \sum_{s=1}^n y_{2,s} p_{s,j_2} \right) \cdots \left( \sum_{s=1}^n y_{t,s} p_{s,j_t} \right) \xi_{j_1, \dots, j_t} \\ &= \sum_{s_1, s_2, \dots, s_t=1}^n y_{1,s_1} y_{2,s_2} \cdots y_{t,s_t} \sum_{j_1, j_2, \dots, j_t=1}^n p_{s_1, j_1} p_{s_2, j_2} \cdots p_{s_t, j_t} \xi_{j_1, \dots, j_t}. \end{aligned} \quad (13.3.4)$$

Положим  $\xi'_{s_1, \dots, s_t} = \sum_{j_1, j_2, \dots, j_t=1}^n p_{s_1, j_1} p_{s_2, j_2} \cdots p_{s_t, j_t} \xi_{j_1, \dots, j_t}$ . Очевидно,

$$\xi'_{s_1, \dots, s_t} = \sum_{j_1, j_2, \dots, j_t=1}^n p_{s_1, j_1} \cdots p_{s_t, j_t} \xi_{\pi(j_1), \dots, \pi(j_t)} = \xi'_{\pi(s_1), \dots, \pi(s_t)} \quad (13.3.5)$$

Таким образом мы доказали, что случайная величина  $\xi'_{s_1, \dots, s_t}$  не меняется при перестановке ее индексов.

Докажем теперь, что все  $\binom{n+t-1}{t}$  случайных величин  $\xi'_{s_1, \dots, s_t}$ ,  $1 \leq s_1 \leq \dots \leq s_t \leq n$ , являются линейно независимыми в совокупности.

Действительно, если указанные случайных величины являются линейно-зависимыми, то возвратимся к случайным величинам  $\xi_{i_1, \dots, i_t}$ , где  $1 \leq i_1 \leq \dots \leq i_t \leq n$ , которые, по определению, являются линейно-независимыми в совокупности. Это сделать возможно, из-за того, что матрица  $P$  является по условию леммы невырожденной. Таким образом,  $\binom{n+t-1}{t}$  линейно-зависимых случайных величин  $\xi'_{s_1, \dots, s_t}$ ,  $1 \leq s_1 \leq \dots \leq s_t \leq n$ , были преобразованы с помощью линейного преобразования в совокупность из  $\binom{n+t-1}{t}$  линейно-независимых случайных величин. Очевидно, что этого быть не может. Поэтому  $\xi'_{s_1, \dots, s_t}$ ,  $1 \leq s_1 \leq \dots \leq s_t \leq n$ , — линейно-независимые случайные величины. Лемма доказана.  $\square$

## 13.4 Основной результат

**Теорема 13.4.1** Система  $\mathcal{R}_t(\mathcal{Q})$  устойчива к  $w$  компрометациям, т.е. является  $(t, w)$ -системой, тогда и только тогда, когда любые различные  $w+1$  векторов множества  $\mathcal{Q}$  являются линейно-независимыми над полем  $\mathbb{F}_q$ .

**Доказательство.** 1. Необходимость. Предположим, что  $\mathbf{a}, \mathbf{b}_1, \dots, \mathbf{b}_t \in \mathcal{Q}$  и  $\mathbf{a} = c_1 \mathbf{b}_1 + \dots + c_t \mathbf{b}_t$ ,  $c_j \in \mathbb{F}_q$ . В этом случае  $\mathbf{K}_{\mathbf{a}} = c_1 \mathbf{K}_{\mathbf{b}_1} + \dots + c_t \mathbf{K}_{\mathbf{b}_t}$ , если под  $\mathbf{K}_{\mathbf{a}}$  понимать  $\binom{n+t-2}{t-1}$ -мерный вектор с координатами  $\xi_{i_1, \dots, i_{t-1}}(\mathbf{a})$  (см. (13.3.1)).

Отсюда следует, что множество  $\mathbf{K}_{\mathbf{a}}$  пользователя  $\mathbf{a}$  может быть получено из множеств пользователей  $\mathbf{b}_1, \dots, \mathbf{b}_t$ . Следовательно, общий ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции  $T = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$  с  $t$  участниками, в число которых входит абонент  $\mathbf{a}$ , может быть вычислен коалицией злоумышленников  $\mathcal{T}_w = \{\mathbf{b}_1, \dots, \mathbf{b}_t\}$ .

2. Достаточность. Предположим, что каждый вектор из множества  $T = \{\mathbf{a}_1, \dots, \mathbf{a}_t\} \subset \mathcal{Q}$  является линейно-независимым от векторов множества  $\mathcal{T}_w = \{\mathbf{b}_1, \dots, \mathbf{b}_w\} \subset \mathcal{Q}$ , т.е.  $\mathbf{a}_j \notin L(\mathcal{T}_w)$ . Покажем, что в этом случае ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  не может быть представлен в виде линейной комбинации ключей, входящих в объединение множеств  $\mathbf{K}_{\mathbf{b}_1}, \dots, \mathbf{K}_{\mathbf{b}_t}$ .

Предположим обратное, а именно, предположим, что

$$k_{\mathbf{a}_1, \dots, \mathbf{a}_t} = \langle \mathbf{z}_1, \mathfrak{K}_{\mathbf{b}_1} \rangle + \dots + \langle \mathbf{z}_t, \mathfrak{K}_{\mathbf{b}_t} \rangle, \quad (13.4.1)$$

где  $\langle \mathbf{z}, \mathfrak{K}_{\mathbf{b}} \rangle$  — скалярное произведение в поле  $\mathbb{F}_q$   $\binom{n+t-2}{t-1}$ -мерного вектора  $\mathbf{z} \in F_q^{\binom{n+t-2}{t-1}}$  и  $\binom{n+t-2}{t-1}$ -мерного вектора  $\mathfrak{K}_{\mathbf{b}}$ .

Ввиду того, что по условию теоремы векторы  $\mathbf{a}, \mathbf{b}_1, \dots, \mathbf{b}_w$  линейно-независимы, мы можем преобразовать базис пространства  $\mathbb{F}_q^n$  так, что в новом базисе  $\omega = \{\omega_1, \dots, \omega_n\}$  векторы  $\mathbf{a}, \mathbf{b}_1, \dots, \mathbf{b}_w$  примут вид  $\mathbf{a} = \mathbf{e}_{w+1}, \mathbf{b}_1 = \mathbf{e}_1, \dots, \mathbf{b}_w = \mathbf{e}_w$ , где  $\mathbf{e}_j = (\underbrace{0, \dots, 0}_{j-1}, 1, \underbrace{0, \dots, 0}_{n-j})$ ,  $j = 0, \dots, n$ .

Как следует из леммы 13.3.1 в новом базисе  $\omega$  пространства  $\mathbb{F}_q^n$  случайные величины  $\xi_{i_1, \dots, i_{t-1}}$  заменятся на случайные величины  $\xi'_{i_1, \dots, i_{t-1}}$  с теми же свойствами. Поэтому мы можем полагать, что изначально векторами  $\mathbf{a}, \mathbf{b}_1, \dots, \mathbf{b}_w$  являются векторы  $\mathbf{e}_{w+1}, \mathbf{e}_1, \dots, \mathbf{e}_w$ .

Отсюда вытекает, что координатами вектора  $\mathfrak{K}_{\mathbf{b}_j}$  являются случайные величины вида

$$\xi_{i_1, \dots, i_{t-1}}(\mathbf{b}_j) = \xi_{i_1, \dots, i_{t-1}, j}, \quad 1 \leq i_1 \leq i_2 \leq \dots \leq i_{t-1} \leq n. \quad (13.4.2)$$

Таким образом, каждый ключ  $\xi_{i_1, \dots, i_{t-1}}(\mathbf{b}_j) \in \mathfrak{K}_{\mathbf{b}_j}$ ,  $j = 1, \dots, w$ , является суммой с ненулевыми коэффициентами только тех независимых секретных ключей  $\xi_{s_1, \dots, s_{t-1}, s_t} \in \mathfrak{K}$ , у которых, по крайней мере, один индекс  $s_j$  принимает значение, меньшее  $w+1$ .

Другими словами, если в сумму  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  (см. (13.3.2)) входит с ненулевым коэффициентом ключ  $\xi_{s_1, \dots, s_{t-1}, s_t} \in \mathfrak{K}$ , у которого все индексы больше  $w$ , то ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является линейно-независимым от ключей множества  $\mathfrak{K}_{\mathbf{b}_1} \cup \mathfrak{K}_{\mathbf{b}_2} \cup \dots \cup \mathfrak{K}_{\mathbf{b}_w}$ , т.е. для ключа  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  с указанным свойством равенство (13.4.1) заведомо не выполняется.

Таким образом, для завершения доказательства теоремы достаточно показать, что ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции, в которую входит пользователь  $\mathbf{a}$ , т.е.  $\mathbf{a} \in \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$ , является суммой элементов множества  $\mathfrak{K}$ , в которую с ненулевым коэффициентом входит, по меньшей мере одна, случайная величина  $\xi_{s_1, \dots, s_{t-1}, s_t} \in \mathfrak{K}$ , у которой все индексы  $s_1, \dots, s_{t-1}, s_t$  больше  $w$ . Докажем это утверждение.

Так как по условию теоремы  $\mathbf{a}_j \notin L(\{\mathbf{b}_1, \dots, \mathbf{b}_w\})$ ,  $j = 1, \dots, t$ , то каждый вектор  $\mathbf{a}_j$  имеет вид

$$\mathbf{a}_j = (a_{j,1}, \dots, a_{j,w}, a_{j,w+1}, \dots, a_{j,n}) \quad (13.4.3)$$

где подвектор  $(a_{j,w+1}, \dots, a_{j,n})$  имеет, по меньшей мере, одну ненулевую координату  $a_{j,s_j}$ ,  $s_j > w$ . Отсюда и из равенства (13.3.2) следует, что в ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  входит с ненулевым коэффициентом  $\prod_{j=1}^t a_{j,s_j}$  случайная величина  $\xi_{s_1, \dots, s_t}$ ,  $s_k > w$ . Это завершает доказательство теоремы.  $\square$

**Следствие 13.4.1** *Ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является нескомпрометированным относительно  $w$ -коалиции  $\mathcal{T}_w = \{\mathbf{b}_1, \dots, \mathbf{b}_w\} \subset \mathcal{Q}$  злоумышленников тогда и только тогда, когда каждый вектор  $\mathbf{a}_j$ ,  $j = 1, \dots, t$ , линейно независим от совокупности векторов  $\{\mathbf{b}_1, \dots, \mathbf{b}_w\}$ .*

**Доказательство.** Если хотя бы один вектор  $\mathbf{a}_j$  принадлежит линейной оболочке множества  $\{\mathbf{b}_1, \dots, \mathbf{b}_w\}$ , то ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  линейно зависит от совокупности ключей множества  $\mathfrak{K}_{\mathbf{b}_1} \cup \mathfrak{K}_{\mathbf{b}_2} \cup \dots \cup \mathfrak{K}_{\mathbf{b}_w}$ . Это утверждение следует из первой части доказательства теоремы.

Если каждый вектор  $\mathbf{a}_j$ ,  $j = 1, \dots, t$ , не принадлежит линейной оболочке множества  $\{\mathbf{b}_1, \dots, \mathbf{b}_w\}$ , то ключ  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является нескомпрометированным относительно множества

ключей  $\mathcal{K}_{b_1} \cup \mathcal{K}_{b_2} \cup \dots \cup \mathcal{K}_{b_w}$ . Это утверждение непосредственно следует из второй части доказательства теоремы.  $\square$

Очень интересно, что из теоремы 13.4.1 следует, что число  $t$  никак не влияет на свойства множества  $\mathcal{Q}$  — основного объекта полиномиальной системы  $\mathcal{R}_{t,w}(\mathcal{Q})$ . Структуру множества  $\mathcal{Q}$  полностью определяют только числа  $N$  (число пользователей системы) и  $w$  (число злоумышленников в системе распределения ключей).

Вместе с тем число ключей  $\binom{n+t-2}{t-1}$  в каждом множестве  $\mathcal{K}_a$ ,  $a \in \mathcal{Q}$ , определяется числами  $n$  (длина векторов множества  $\mathcal{Q}$ ) и  $t$  (числом участников конференции). Например, если  $t = 2$  (система распределения ключей для парной связи пользователей), то мы имеем  $|\mathcal{K}_a| = n$ .

Следует также привести для рассматриваемых систем  $\mathcal{R}_{t,w}(\mathcal{Q})$  вид функции  $D(\mathcal{R}_{t,w}(\mathcal{Q})) = k(t, w) \log_2 |M|$  (см. (13.1.1)), которая определяет эффективность рассматриваемых  $(t, w)$ —систем распределения ключей.

В нашем случае  $k(t, w) = \binom{n+t-2}{t-1}$  (число ключей, хранимых каждым пользователем) и  $\log_2 |M| = u \log_2 q$  — число двоичных ячеек памяти, требуемых для хранения в электронной памяти одного ключа системы. Заметим, что числа  $w$  и  $N$  (число пользователей системы и только оно) определяют число  $n$ .

Таким образом, в рассматриваемом случае полилинейной системы распределения ключей

$$D(\mathcal{R}_{t,w}(\mathcal{Q})) = \binom{n+t-2}{t-1} u \log_2 q, \quad (13.4.4)$$

где  $D(\mathcal{R}_{t,w}(\mathcal{Q}))$  — количество информации (измеряемой битами), которые содержатся в ключевом множестве  $\mathcal{K}_a$  каждого пользователя  $a \in \mathcal{Q}$   $(t, w)$ —системы  $\mathcal{R}_{t,w}(\mathcal{Q})$   $u$  — длина ключа и  $q$  — значность одного его разряда.

### 13.4.1 Возможные конструкции множеств $\mathcal{Q}$

Из теоремы 13.4.1 следует, что если множество векторов  $\mathcal{Q}$  длины  $n$ , у которого любые  $w + 1$  элементов линейно-независимы, рассмотреть как столбцы проверочной матрицы  $B$  кода  $\mathcal{C}$  длины  $N = |\mathcal{Q}|$ , то код  $\mathcal{C}$  будет иметь кодовое расстояние  $d \geq 2 + w$ . И наоборот, множество столбцов  $\mathcal{Q}$  любого линейного кода  $\mathcal{C}$  над полем  $\mathbb{F}_q$  с кодовым расстоянием  $d \geq 2 + w$  порождает  $(t, w)$ —систему распределения ключей  $\mathcal{R}_t(\mathcal{Q})$ .

Из этого очевидного утверждения вытекает, что в качестве множества пользователей  $\mathcal{Q}$   $(t, w)$ —системы распределения ключей можно рассматривать столбцы проверочных матриц любого линейного кода с кодовым расстоянием  $d \geq 2 + w$ . Далее мы рассмотрим в качестве множества  $\mathcal{Q}$  проверочные матрицы кодов Хемминга и Рида-Соломона и вычислим для них значения функции  $D(\mathcal{R}_{t,w}(\mathcal{Q}))$ .

1. Естественно начать с двоичного кода Хемминга длины  $N = 2^n - 1$  с кодовым расстоянием 3 (см. раздел 1.1.3, лемма 1.1.3). Пусть  $B_n$  — множество столбцов проверочной матрицы этого кода Хемминга, т.е.  $B_n$  — множество всех ненулевых столбцов высоты  $n$ .

В этом случае  $(t, 1)$ —система распределения ключей  $\mathcal{S}$  с множеством пользователей  $B_n$  имеет следующие параметры:

Число абонентов  $N = 2^n - 1$ , число двоичных ключей у каждого абонента  $\binom{n+t-2}{t-1}$  и  $D(\mathcal{R}_t(\mathcal{Q})) = \binom{n+t-2}{t-1} u$ , где  $u$  — длина каждого двоичного ключа системы.



Если в качестве множества  $\mathcal{Q}$  взять столбцы проверочной матрицы расширенного кода Хемминга длины  $N = 2^n$  с кодовым расстоянием 4, то в этом случае  $(t, 2)$ -система распределения ключей  $\mathcal{R}_t(\mathcal{Q})$  будет иметь следующие параметры.

Число абонентов  $N = 2^n$ , число двоичных ключей у каждого абонента  $\binom{n+t-1}{t-1}$  и  $D(\mathcal{R}_t(\mathcal{Q})) = u \binom{n+t-1}{t-1}$ , где  $u$  — длина каждого ключа системы.

2.  $q$ -ичный код Рида-Соломона  $RS_q(q+1, w+2)$  длины  $q+1$  с кодовым расстоянием  $w+2$  (см. раздел 5.0.4). (случай  $t=2$  рассмотрен Бломом [75]).

В этом случае  $(t, w)$ -система распределения ключей  $\mathcal{S}$  с множеством пользователей  $B_n$  имеет следующие параметры.

Число абонентов  $N = q+1$ , число  $n = w+1$ , число ключей у каждого абонента  $\binom{n+t-2}{t-1} = \binom{w+t-1}{t-1}$  и  $D(\mathcal{R}_{t,w}(\mathcal{Q})) = u \binom{w+t-1}{t-1} \log_2 q$ , где  $u$  — длина каждого  $q$ -ичного ключа системы. Если  $w=1$ , то  $n=2$  и число ключей, хранимых у каждого пользователя равно  $\binom{n+t-2}{t-1} = \binom{t}{1} = t$ .

Заметим, что в разделе 13.6 будет показано, что число  $\binom{w+t-1}{t-1}$  является минимально возможным значением для числа ключей, которые необходимо хранить каждому пользователю полиномиальной  $(t, w)$ -системы распределения ключей.

## 13.5 Системы распределения ключей Блундо и др.

Мы коротко опишем достаточно интересную  $(t, w)$ -систему  $\mathfrak{B}_{t,w}$  распределения ключей с  $N$  пользователями, предложенную в работах [52], [51].

Пусть  $q \geq N$  — степень простого числа. Рассмотрим симметричный многочлен  $f_w(x_1, \dots, x_t)$  степени  $w$  от  $t$  с коэффициентами из поля  $\mathbb{F}_q$ :

$$f_w(\mathbf{x}) = f_w(x_1, \dots, x_t) = \sum_{i_1=0, \dots, i_t=0}^w a_{i_1, \dots, i_t} x_1^{i_1} \cdots x_t^{i_t}, \quad a_{i_1, \dots, i_t} \in \mathbb{F}_q. \quad (13.5.1)$$

Слово симметричный означает, что для любых двух наборов  $\mathbf{c} = (c_1, \dots, c_t)$ ,  $\mathbf{c}' = (c'_1, \dots, c'_t)$  таких, что второй набор является перестановкой координат первого, значения  $f_w(\mathbf{c})$  и  $f_w(\mathbf{c}')$  многочленов в точках  $\mathbf{c}$  и  $\mathbf{c}'$  совпадают. Очевидно, многочлен  $f_w(\mathbf{x})$  является симметрическим, когда и только тогда, когда

$$a_{i_1, \dots, i_t} = a_{j_1, \dots, j_t}, \quad (13.5.2)$$

для всех наборов  $i_1, \dots, i_t$  и  $j_1, \dots, j_t$ , которые можно перевести один в другой с помощью перестановки их символов.

Таким образом, мы рассматриваем многочлен  $f_w(\mathbf{x})$  вида (13.5.1), у которого коэффициенты удовлетворяют соотношению (13.5.2). Эти многочлены можно записать в виде

$$f_w(\mathbf{x}) = \sum_{0 \leq i_1 \leq \dots \leq i_t \leq w} a_{i_1, \dots, i_t} \sum_{i_1, \dots, i_t}^* x_1^{i_1} \cdots x_t^{i_t}, \quad (13.5.3)$$

где суммирование в сумме  $\sum_{i_1, \dots, i_t}^*$  производится по всем перестановкам координат набора  $(i_1, \dots, i_t)$ . Многочлены  $\sigma_{i_1, \dots, i_t}(\mathbf{x}) = \sum_{i_1, \dots, i_t}^* x_1^{i_1} \cdots x_t^{i_t}$  называются однородными симметрическими многочленами.

Как нетрудно установить и это хорошо известно (см. [28] и многие другие работы), что число многочленов  $\sigma_{i_1, \dots, i_t}(\mathbf{x})$  таких, что  $0 \leq i_1 \leq \dots \leq i_t \leq w$ , равно  $\binom{w+t}{t}$ . В случае  $t = 2$  число различных многочленов  $\sigma_{i_1, i_2}(\mathbf{x})$  будет равным  $\binom{w+2}{2}$ .

В системе  $\mathfrak{B}_{t,w}$  исходным множеством секретных ключей  $\mathfrak{K}$  является множество коэффициентов симметрического многочлена  $f_w(\mathbf{x})$ . т.е. фактически множеством  $\mathfrak{K}$  является сам симметрический многочлен  $f_w(\mathbf{x})$ .

Множеством индексов пользователей  $\mathcal{Q}$  совпадает с конечным полем  $\mathbb{F}_q$ , т.е.  $\mathcal{Q} = \mathbb{F}_q$ .

Секретной ключевой информацией пользователя  $\mathbf{a} \in \mathbb{F}_q$  является многочлен  $g_{\mathbf{a}}(x_1, \dots, x_{t-1}) = f_w(x_1, \dots, x_{t-1}, \mathbf{a})$  или, выражаясь несколько точнее, множеством  $\mathfrak{K}_{\mathbf{a}}$  является множество коэффициентов многочлена  $g_{\mathbf{a}}(x_1, \dots, x_{t-1})$ .

Заметим, что не важно какому переменному  $x_j$  многочлена  $f_w(\mathbf{x})$  придать значение  $\mathbf{a}$ , чтобы получить многочлен  $g_{\mathbf{a}}$ . При любом  $j$  получится один и тот же симметрический многочлен  $g_{\mathbf{a}}(x_1, \dots, x_{t-1})$ .

Очевидно, число секретных ключей пользователя  $\mathbf{a}$  равно  $\binom{w+t-1}{t-1}$  — числу коэффициентов у симметрического многочлена  $g_{\mathbf{a}}(x_1, \dots, x_{t-1})$  от  $t-1$  переменных, степень которого по каждой переменной не превосходит  $w$ .

Алгоритм  $\mathfrak{A}$  выработки общего ключа  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  конференции с участниками  $T = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$  очень прост, а именно, общим ключем  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$  является элемент поля  $\mathbb{F}_q$ , который имеет вид

$$k_{\mathbf{a}_1, \dots, \mathbf{a}_t} = g_{\mathbf{a}_j}(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \mathbf{a}_{j+1}, \dots, \mathbf{a}_t), \quad (13.5.4)$$

т.е. каждый пользователь  $\mathbf{a}_j$  конференции  $T$  вычисляет значение своего секретного многочлена  $g_{\mathbf{a}_j}(x_1, \dots, x_{t-1})$  в точках, которые являются индексами других пользователей конференции  $T$ .

Так как многочлен  $f_w(x_1, \dots, x_{t-1}, x_t)$  симметрический, то ключи  $k_{\mathbf{a}_1, \dots, \mathbf{a}_t}$ , вычисленные у различных пользователей конференции  $T$ , одинаковы.

Отметим, что в случае  $t = 2$  многочлен  $g_{\mathbf{a}}(x_1, \dots, x_{t-1})$  является многочленом первой степени и множество секретных ключей  $\mathfrak{K}_{\mathbf{a}}$  содержит  $\binom{w+1}{1} = w+1$  элементов — коэффициентов многочлена  $g_{\mathbf{a}}(x_1, \dots, x_{t-1})$ . Этот случай и был предметом изучения Блома [75].

Как легко увидеть, если в уже рассмотренной системе распределения ключей  $\mathcal{R}_t(\mathcal{Q})$  с параметром  $n$  равным  $w+1$  в качестве  $\mathcal{Q}$  взять матрицу, у которой типичный столбец  $Q$  имеет вид  $Q = (1, a^1, a^2, \dots, a^w)^T$ ,  $a \in \mathbb{F}_q$ , то мы получим систему распределения ключей Блундо и др.  $\mathfrak{B}_{t,w}$ . Нетрудно увидеть, что система Блундо и др. является частным случаем систем  $\mathcal{R}_{t,w}(\mathcal{Q})$ , рассмотренной в разделе 13.3.

## 13.6 Нижние оценки числа ключей у пользователей $(w, t)$ —системы распределения ключей

Мы изложим в усовершенствованном виде часть результатов работы Beimel и Chor [50].

Зафиксируем подмножество  $Q_{t+w}$  множества  $\mathcal{Q}$  из  $t+w$  элементов:  $Q_{t+w} = \{\mathbf{c}_1, \dots, \mathbf{c}_{t+w}\} \subseteq \mathcal{Q}$ . Пусть  $\mathcal{T}(\mathbf{a}) = \{T_1, \dots, T_l\}$  — множество всех  $t$ -подмножеств множества  $Q_{t+w}$ , которые включают в себя фиксированного пользователя  $\mathbf{a} \in Q_{t+w}$ , где  $l = \binom{w+t-1}{t-1}$ . Обозначим через  $k_{T_j}$  общий ключ конференции  $T_j$ .

**Лемма 13.6.1** *Ключи  $k_{T_j}$ ,  $j = 1, \dots, l$ , любой  $(t, w)$ -системы распределения ключей являются линейно-несвязанными, т.е. для любых  $a_j \in \mathbb{F}_q$  выполнено  $\sum_{j=1}^l a_j k_{T_j} \neq 0$ .*

**Доказательство.** Предположим обратное. А именно предположим, что

$$k_{T_1} = \sum_{j=2}^l a_j k_{T_j}. \quad (13.6.1)$$

Предположим, что  $T_1 = \{\mathbf{a}_1, \dots, \mathbf{a}_t\}$ . Рассмотрим коалицию злоумышленников  $\mathcal{T}_w = \{\mathbf{b}_1, \dots, \mathbf{b}_w\}$ , которая не включает в себя пользователей конференции  $T_1$ , т.е.  $\mathcal{T}_w = Q_{t+w} \setminus T_1$  и, следовательно,  $T_1 \cap \mathcal{T}_w = \emptyset$ .

Очевидно,

$$\mathcal{T}_w \setminus T_j \neq \emptyset, \text{ если } j > 1. \quad (13.6.2)$$

Следовательно, каждый ключ  $k_{T_j}$ ,  $j > 1$ , может быть вычислен коалицией злоумышленников  $\mathcal{T}_w$ .

Отсюда и из равенства (13.6.1) следует, что и общий ключ  $k_{T_1}$  конференции  $T_1$  может быть вычислен коалицией злоумышленников  $\mathcal{T}_w$  несмотря на то, что  $T_1 \cap \mathcal{T}_w = \emptyset$ . Это для  $(t, w)$ -системы распределения ключей невозможно. Отсюда следует, что равенство (13.6.1) для  $(t, w)$ -системы не выполнено, т.е. доказывает утверждение леммы.  $\square$

**Теорема 13.6.1** *Для числа  $|\mathfrak{K}_a|$  ключей в ключевом векторе  $\mathfrak{K}_a$  (числа ключей у каждого пользователя системы) полилинейной  $(t, w)$ -системы распределения ключей  $\mathcal{R}_t(\mathcal{Q})$  справедлива оценка*

$$|\mathfrak{K}_a| \geq \binom{w+t-1}{t-1}. \quad (13.6.3)$$

**Доказательство.** Заметим, что каждый ключ множества  $\mathfrak{K}_a$  является независимой случайной величиной. Предположим, что в ключевом векторе  $\mathfrak{K}_a$  число ключей меньше, чем  $\binom{w+t-1}{t-1}$ .

В этом случае все случайные величины, входящие в множество  $\mathcal{T}(\mathbf{a})$ , во-первых, в силу леммы 13.6.1 являются линейно-несвязанными, и, во-вторых, должны быть линейно-зависимыми от ключей, входящих в множество  $\mathfrak{K}_a$ .

Последнее означает, что каждый ключ  $k_{T_j} \in \mathcal{T}(\mathbf{a})$  полилинейной системы должен иметь представление следующего вида

$$k_{T_j} = l_j(\mathfrak{K}_a), \quad (13.6.4)$$

где  $l_j(\mathbf{z})$  — некоторая невырожденная линейная функция от  $|\mathfrak{K}_a|$  переменных.

Очевидно, такого не может быть, в виду того, что линейные функции  $l_j(\mathbf{z})$ ,  $j = 1, \dots, \binom{w+t-1}{t-1}$ , обязательно являются линейно-зависимыми, ибо число переменных, от которых зависит каждая из этих функций, меньше, чем общее число этих функций. Таким образом, ключи  $k_{T_j}$  обязательно являются линейно-зависимыми. Это противоречит лемме 13.6.1.  $\square$

Заметим, что лемма 13.6.1 справедлива без предположения о полиномиальности системы. Вместе с тем система распределения ключей в теореме 13.6.1 обязательно должна

быть полилинейной. Если рассматривать в теореме неполиномиальные системы, то для них верен некоторый аналог теорема 13.6.1, как это показано в работе Beimel и Chor [50].

Теорема 13.6.1 устанавливает, что минимально возможное число ключей пользователя в полилинейной  $(t, w)$ –системе распределения ключей имеет  $(t, w)$ –система, у которой  $n = w + 1$ . В частности, это свойство выполнено для  $(t, w)$ –системы  $\mathcal{R}_t(\mathcal{Q})$ , у которой длина векторов  $n$  множества  $\mathcal{Q}$  равна  $n = w + 1$ . Например, это условие выполнено в том случае, когда множество  $\mathcal{Q}$   $(t, w)$ –системы  $\mathcal{R}_t(\mathcal{Q})$  образовано столбцами проверочной матрицы кода Рида-Соломона  $RS_q(q+1, w+2)$  длины  $q+1$  с кодовым расстоянием  $w+2$ .

# Глава 14

## Дизъюнктные и разделяющие коды

Дизъюнктные и разделяющие коды это интересные, но относительно мало известные математические конструкции. Их интенсивное исследование началось только в последние 15 лет. Эти объекты хотя традиционно и называются кодами, но они имеют не очень много сходства с традиционными кодами, например, кодами корректирующими ошибки или неравномерными кодами, которые используются для сжатия информации. Областями использования дизъюнктных кодов являются планирование экспериментов, криптография и т.п. Можно также сказать, что дизъюнктные коды занимают промежуточное положение между комбинаторикой и теорией кодирования.

Мы сначала изучим дизъюнктные и разделяющие коды, а затем очень коротко расскажем об их применениях.

### 14.1 Дизъюнктные коды (superimposed code)

**Определение 14.1.1** Пусть  $w \geq 1$  и  $r \geq 0$  и  $T \geq 2$  — целые числа такие, что  $w + r \leq T$ . Набор  $\mathcal{A} = \{A_1, \dots, A_T\}$  подмножеств множества  $[N] = \{1, \dots, N\}$  называется  $(w, r)$ —семейством непокрывающих множеств (*cover-free  $(w, r)$ -family*), если для него выполнены следующие свойства:

$$\bigcap_{s=1}^w A_{i_s} \not\subseteq \bigcup_{j=1}^r A_{k_j}, \text{ для всех } \{i_1, \dots, i_w\}, \{k_1, \dots, k_r\} \subseteq [T] \quad (14.1.1)$$

таких, что  $\{i_1, \dots, i_w\} \cap \{k_1, \dots, k_r\} = \emptyset$ .

В частности, если  $r = 0$ , тогда

$$\bigcap_{s=1}^w A_{i_s} \neq \emptyset \text{ для всех } \{i_1, \dots, i_w\} \subseteq [T]. \quad (14.1.2)$$

Заметим что среди элементов множеств  $\{i_1, \dots, i_w\}$  и  $\{k_1, \dots, k_r\}$  могут быть повторяющиеся, т.е. фактически, каждое из этих множеств может содержать меньшее, чем  $w$  и  $r$  число элементов, соответственно.

Мы также будем рассматривать конструкцию, называемую дизъюнктным  $(w, r)$ —кодом, которая эквивалентна понятию  $(w, r)$ —семейством непокрывающих множеств.

А именно, с каждым подмножеством  $(w, r)$ –семейства свяжем столбец  $\bar{A}_j$  высоты  $N$ , координатами которого являются символы  $0, 1$ , при этом  $j$ –ая координата равна 1 тогда и только тогда, когда  $j \in A_j$ . Столбец  $\bar{A}_j$  называется характеристическим столбцом подмножества  $A_j$ .

$N \times T$  матрицу  $\mathfrak{K} = \mathfrak{K}(\mathcal{A})$ , образованную всеми характеристическими столбцами  $\bar{A}_j$ ,  $j = 1, \dots, T$ ,  $(w, r)$ –семейства непокрывающих множеств мы будем называть дизъюнктым  $(w, r)$ –кодом.

Как следует из определения 14.1.1, матрица  $\mathfrak{K} = \mathfrak{K}(\mathcal{A})$  дизъюнктного  $(w, r)$ –кода обладает следующим свойством.

- i. Для всех подмножеств  $\{i_1, \dots, i_w\}, \{k_1, \dots, k_r\} \subseteq [T]$  таких, что  $\{i_1, \dots, i_w\} \cap \{k_1, \dots, k_r\} = \emptyset$ , в матрице  $\mathfrak{K} = \mathfrak{K}(\mathcal{A})$  найдется строка, у которой координаты, индексированные элементами множества  $\{i_1, \dots, i_w\}$ , равны 1, а координаты, индексированные элементами множества  $\{k_1, \dots, k_r\}$  равны 0.

Очевидно,  $(w, r)$ –семейство непокрывающих множеств и соответствующая ему матрица  $\mathfrak{K} = \mathfrak{K}(\mathcal{A})$  — это один и тот же объект, но в разных обозначениях.

Следует отметить, что по наблюдению автора некоторые читатели предпочитают использовать теоретико-множественный язык, т.е. определение 14.1.1. В то время как для других читателей более удобен "теоретико-кодовый" язык, т.е. язык дизъюнктных кодов. Мы далее в работе будем пользоваться, преимущественно, теоретико-множественным языком.

Число  $N$  обычно называется длиной дизъюнктного кода  $\mathfrak{K}$ , а число  $T$  — числом его элементов.

Обычно стремятся при заданных  $N, (w, r)$  максимизировать число  $T$  элементов дизъюнктного  $(w, r)$ –кода длины  $N$ .

Вместе с тем, по мнению автора, для некоторых приложений, например, криптографических, более естественно максимизировать число  $T$  при заданном числе элементов  $a$  у каждого из множеств  $A_j$ . (Подробнее об этом сказано в разделе 14.4).

Определение дизъюнктного  $(1, w)$ –кода впервые было дано в работе [65]. Там же были указаны некоторые области их возможного использования. Затем в 1982 г. были определены дизъюнктные  $(w, r)$ –коды и начались их исследования. Библиография по этому направлению имеется в работе [56].

Наиболее широко дизъюнктные  $(w, r)$ –коды используются для построения схем планирования экспериментов (см. [56] и литературу, приведенную в этом источнике). Они находят применения и в криптографии (см., например, [82, 56], а также многие другие работы). Криптографическим приложениям дизъюнктных кодов также рассмотрены в разделе 14.4 данной главы.

Обозначим через  $N(T, w, r)$  минимально возможную длину дизъюнктного  $(w, r)$ –кода с числом элементов  $T$ , а через  $N(T, a, w, r)$  — минимально возможную длину дизъюнктного  $(w, r)$ –кода с числом элементов  $T$ , который образован строками, вес Хемминга которых не превосходит  $a$ .

На теоретико-множественном языке определение числа  $N(T, w, r)$  звучит так.  $N(T, w, r)$  — это минимально возможное число элементов множества  $[N]$ , у которого имеется  $T$  подмножеств, образующих  $(w, r)$ –семейство непокрывающих множеств. Точно также звучит и определение числа  $N(T, a, w, r)$  с добавлением, что каждое его подмножество  $A_j \subseteq [N]$ ,  $j = 1, \dots, T$ , семейства имеет не более, чем  $a$  элементов.

Примером  $(w, r)$ – дизъюнктного кода  $\mathfrak{K}_s = \mathfrak{K}_s(N)$  является код, образованный всеми двоичными  $\binom{n}{s}$  строками длины  $n$ , вес Хемминга которых равен  $s$ , где  $w \leq s \leq N - r$ . Дизъюнктный код  $\mathfrak{K}_s$  имеет длину  $N = \binom{n}{s}$  и число элементов  $T = n$ . Этот код носит название тривиального дизъюнктного кода.

Следующее утверждение легко доказать. (Упражнение)

**Лемма 14.1.1** Код  $\mathfrak{K}_s(n)$  является  $(w, r)$ – дизъюнктным кодом, если  $w \leq s \leq n - r$ .

Непосредственно из этой леммы вытекает, что

**Следствие 14.1.1**

$$N(n, w, r) \leq \min \left\{ \binom{n}{w}, \binom{n}{n-r} \right\},$$

$$N(n, a, w, r) \leq \binom{N}{a}, \quad \text{если } w \leq a \leq N - r.$$
(14.1.3)

Код  $\mathfrak{K}_s$  обычно называют тривиальным  $(w, r)$ – дизъюнктным кодом. Обычно удается построить  $(w, r)$ – дизъюнктный код, длина которого значительно меньше, чем  $\min \left\{ \binom{N}{w}, \binom{N}{N-r} \right\}$ . Этим мы займемся в следующих параграфах.

### 14.1.1 Разделяющие коды

Разделяющий код это объект, который интересен не только сам по себе, но и как промежуточная конструкция для построения дизъюнктных кодов.

**Определение 14.1.2**  $q$ – значный код  $\mathcal{C}$  длины  $n$  называется разделяющим  $(w, r)$ – кодом (*separating  $(w, r)$ – code*), где  $w, r \geq 1$ , если для любых  $\mathbf{y}_1, \dots, \mathbf{y}_w \in \mathcal{C}$  и любых  $\mathbf{x}_1, \dots, \mathbf{x}_r \in \mathcal{C}$ , таких, что  $\{\mathbf{y}_1, \dots, \mathbf{y}_w\} \cap \{\mathbf{x}_1, \dots, \mathbf{x}_r\} = \emptyset$ , существует компонента (координата)  $i \in [n] = \{1, \dots, n\}$  такая, что

$$\{y_{1,i}, \dots, y_{w,i}\} \cap \{x_{1,i}, \dots, x_{r,i}\} = \emptyset.$$
(14.1.4)

Как следует из определения разделяющим  $(w, r)$ – кода, числа  $w$  и  $r$  симметричны, т.е.  $(w, r)$ – код одновременно является и  $(r, w)$ – кодом.

Например, код  $\mathcal{C} = \mathbb{F}_q^n$  является разделяющим  $(1, 1)$ – кодом, ибо у любых двух различных векторов  $\mathbf{x}, \mathbf{y} \in \mathcal{C}$  найдется разряд, в котором они различаются, т.е. для которых выполнено соотношение (14.1.4).

Построить разделяющий  $(1, 2)$ – код значительно сложнее. Один из возможных способов следующий.

Рассмотрим код  $\mathcal{C} \subset \mathbb{F}_q^n$  длины  $n = q$ , образованный векторами, координаты которых являются значениями многочленов степени  $m < \frac{q}{2}$ , т.е. код  $\mathcal{C}$  является  $q$ – значным кодом Рида-Соломона длины  $q$  и порядка  $m$ . Очевидно, размерность  $\mathcal{C}$  равна  $m + 1$ . Докажем, что код  $\mathcal{C}$  является разделяющим  $(1, 2)$ – кодом.

Действительно, достаточно показать, что для любых трех векторов  $\mathbf{x}, \mathbf{y}_1, \mathbf{y}_2$  найдется координата, для которой  $x_i \notin \{y_{1,i}, y_{2,i}\}$  или, что одно и то же, координата, для которой справедливо  $(y_{1,i} - x_i)(y_{2,i} - x_i) \neq 0$ .

Последнее неравенство для указанного кода Рида-Соломона выполнено в виду того, что ненулевой многочлен вида  $F(x) = (g_1(x) - f(x))(g_2(x) - f(x))$ , у которого  $\deg f, g_1, g_2 < \frac{q}{2}$ , имеет степень, меньшую, чем  $q$ , и поэтому принимает ненулевые значения, когда переменная  $x$  пробегает все элементы поля  $\mathbb{F}_q$ .

К настоящему времени развитой теории построения разделяющих кодов не существует. Вместе с тем известно несколько не очень сложных результатов, в которых известные коды, корректирующие ошибки, рассматриваются в качестве разделяющих кодов. Об этом более подробно мы расскажем ниже.

Скоростью  $R(\mathcal{C})$   $q$ -ичного разделяющего  $(w, r)$ -кода  $\mathcal{C}$  длины  $n$  называется величина

$$R(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{n}. \quad (14.1.5)$$

Пусть  $R_q(n, r, w) = \max R(\mathcal{C})$ , где максимум берется по всем  $q$ -ичным разделяющим  $(w, r)$ -кодам длины  $n$ .

Величина

$$R_q(w, r) = \overline{\lim}_{n \rightarrow \infty} R_q(n, r, w), \quad (14.1.6)$$

называется относительной скоростью  $q$ -ичного разделяющего  $(w, r)$ -кода.

Заметим, что стандартными методами похожими на метод получения оценки Варшамова-Гилберта для кодов, корректирующих ошибки, (см. раздел 2.0.8) нетрудно получить нижние оценки скорости  $R_q(n, r, w)$ , для которой существуют  $q$ -ичные разделяющие  $(w, r)$ -коды длины  $n$ . Эти оценки получены, например, в работе [58], chapter 6, и мы не будем приводить их в общем виде.

Основной вывод из этих оценок следующий. При  $q, w, r = \text{const}, n \rightarrow \infty$  нижний предел скорости передачи

$$\underline{R}_q(w, r) = \underline{\lim}_{n \rightarrow \infty} R_q(n, r, w), \quad (14.1.7)$$

является положительной постоянной  $\underline{R}_q(w, r)$ . Вместе с тем следует сказать, что эти оценки получены только кодов, которые, вообще говоря, не являются линейными. Нижние оценки для скорости передачи линейных  $q$ -ичных разделяющих  $(w, r)$ -кодов не известны.

Из теоремы 14.3.2 и теоремы 13 работы [58] (нижней границы существования двоичного разделяющего  $(w, r)$ -кода) непосредственно вытекает

**Теорема 14.1.1** *Существует бесконечная последовательность двоичных разделяющих  $(w, r)$ -кодов, у которой скорость  $\underline{R}_2(w, r)$  не меньше, чем  $Y(w, r)$ , где*

$$Y(w, r) = \frac{1}{w + r - 1} \max_{0 < p < 1} \log_2 ((1 - p^w(1 - p)^r - p^r(1 - p)^w)^{-1}). \quad (14.1.8)$$

Для недвоичных кодов подобная оценка также известна, но имеет более сложный вид. Отметим, что, в частности,  $Y(2, 1) = 0.2075$ .



## Код Рида-Соломона и код Рида-Маллера как разделяющие коды

Пусть  $RS_q(n, d)$  — код Рида-Соломона над полем  $\mathbb{F}_q$  длины  $n \leq q + 1$  с кодовым расстоянием  $d$  и размерностью  $k = n - d + 1$ . (см. раздел 5)

**Лемма 14.1.2** (Сагалович [30]) *Код  $RS_q(n, d)$  является разделяющим  $(r, w)$ –кодом, если  $n \geq wr(k - 1) + 1$  и  $q^k > r + w$ .*

**Доказательство.** Мы будем рассматривать векторы  $\mathbf{x}$  кода  $RS_q(n, d)$  как последовательности  $\alpha_f$  (см. (5.0.4)) значений многочленов  $f(x)$  степени не выше  $k - 1$  на множестве  $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$ , образованных некоторыми элементами поля  $F_q$ . Это возможно ввиду следствия 5.0.1. В частности, если  $n = q$ , то это множество совпадает со всем полем  $\mathbb{F}_q$ .

Очевидно, соотношение (14.1.4) выполнено, если каждый ненулевой многочлен

$$F(x) = \prod_{i=1}^w \prod_{j=1}^r (f_i(x) - g_j(x)) \quad (14.1.9)$$

принимает ненулевое значение хотя бы одном элементе множества  $\{\alpha_1, \dots, \alpha_n\}$ , где  $f_i(x)$  и  $g_j(x)$  — многочлены, которые порождают последовательности  $\mathbf{y}_1, \dots, \mathbf{y}_w \in RS_q(n, d)$  и  $\mathbf{x}_1, \dots, \mathbf{x}_r \in RS_q(n, d)$ .

Неравенство  $n \geq wr(k - 1) + 1$  леммы как раз и обеспечивает выполнение условия  $\deg F(x) < n$ . Из последнего неравенства, очевидно, вытекает, что ненулевой многочлен  $F(x)$  принимает на множестве  $\{\alpha_1, \dots, \alpha_n\}$ , по крайней мере, одно ненулевое значение.  $\square$

Пусть  $RM_{t,m}$  — двоичный код Рида-Маллера длины  $n = 2^m$  порядка  $m$  с кодовым расстоянием  $d = 2^{m-t}$  и размерностью  $k = \sum_{j=0}^t \binom{m}{j}$ . (см. главу 7, определение 7.0.2)

**Лемма 14.1.3** *Код  $RM_{s,m}$  является разделяющим  $(r, w)$ –кодом, если  $m \geq srw$  и  $2^m > r + w$ .*

**Доказательство** в идейном плане не отличается от доказательства леммы 14.1.2 и его предоставляется провести читателю. (Упражнение)

### 14.1.2 Построение разделяющих $(w, 1)$ –кодов, [30]

В настоящем разделе мы, используя теорему 14.3.2 и следуя работе [30], получим простые необходимые и достаточные условия для существования разделяющих линейных  $(w, 1)$ –кодов.

Пусть  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ . Произведением (не скалярным)  $\mathbf{x} \cdot \mathbf{y}$  векторов  $\mathbf{x}, \mathbf{y}$  назовем вектор

$$\mathbf{x} \cdot \mathbf{y} = (x_1 y_1, \dots, x_n y_n). \quad (14.1.10)$$

**Лемма 14.1.4** *Линейный над полем  $\mathbb{F}_q$  код  $\mathcal{C}$  является разделяющим  $(w, 1)$ –кодом тогда и только тогда, когда для любых ненулевых векторов  $\mathbf{x}_1, \dots, \mathbf{x}_w \in \mathcal{C}$  выполнено*

$$\mathbf{x}_1 \cdots \mathbf{x}_w \neq 0. \quad (14.1.11)$$

**Доказательство.** Пусть  $\mathbf{x}'_1, \dots, \mathbf{x}'_w, \mathbf{x} \in \mathcal{C}$ ,  $\mathbf{x} \notin \{\mathbf{x}'_1, \dots, \mathbf{x}'_w\}$ .

Предположим, что для всех координат  $x_i$  у вектора  $\mathbf{x}$  выполнено включение  $x_i \in \{x'_{1,i}, \dots, x'_{w,i}\}$ ,  $i = 1, \dots, n$ . Тогда для векторов  $\mathbf{x}_1 = \mathbf{x}'_1 - \mathbf{x}, \dots, \mathbf{x}_w = \mathbf{x}'_w - \mathbf{x}$ , принадлежащих коду  $\mathcal{C}$ , соотношение (14.1.11) не выполняется.

Наоборот, если существуют координаты  $x_i$  у вектора  $\mathbf{x}$ , для которой  $x_i \notin \{x'_{1,i}, \dots, x'_{w,i}\}$ , тогда выполняется соотношение (14.1.11).  $\square$

**Лемма 14.1.5** *Двоичный линейный код  $\mathcal{C}$  является разделяющим  $(2, 1)$ -кодом, если для любых  $\mathbf{x}, \mathbf{y} \in \mathcal{C} \setminus \{0\}$*

$$wt(\mathbf{x} + \mathbf{y}) < wt(\mathbf{x}) + wt(\mathbf{y}), \quad (14.1.12)$$

где  $wt(\mathbf{x})$  — вес вектора  $\mathbf{x}$ .

**Доказательство.** Если  $\mathbf{x} \cdot \mathbf{y} = (0, \dots, 0)$ ,  $\mathbf{x}, \mathbf{y} \in \mathcal{C} \setminus \{0\}$ , то, очевидно,  $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y})$ . Если же  $\mathbf{x} \cdot \mathbf{y} \neq (0, \dots, 0)$ , то, очевидно, в этом случае выполнено неравенство (14.1.12). (Упражнение)  $\square$

**Следствие 14.1.2** [30] *Линейный над полем  $\mathbb{F}_q$  код  $\mathcal{C}$  является разделяющим  $(2, 1)$ -кодом, если для любого  $\mathbf{x} \in \mathcal{C} \setminus \{0\}$  выполнено*

$$\frac{n}{3} < wt(\mathbf{x}) < \frac{2n}{3}. \quad (14.1.13)$$

**Доказательство.** Если  $\mathbf{x} \cdot \mathbf{y} = 0$ , то  $wt(\mathbf{x} + \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) > \frac{2n}{3}$ , что противоречит предположению следствия.  $\square$

Вопросы конструктивного построения разделяющих  $(w, r)$ -кодов разработаны слабо.

В частности, автору не известно конструктивных методов построения бесконечных семейств  $q$ -ичных разделяющих  $(w, r)$ -кодов при  $q = \text{const}$ ,  $w > 1$ ,  $n \rightarrow \infty$ , которые имеют ненулевую скорость. Вместе с тем следствие 14.1.2, несмотря на свою простоту, позволяет доказать существование таких "хороших" кодов при  $q = 2$ .

А именно, известные методы получения границы Варшамова-Гилберта существования линейного кода с заданным кодовым расстоянием (см. лемму 2.0.52) могут быть с помощью незначительных изменений трансформированы в методы получения границы существования для линейного кода, у которого ограничены снизу и сверху расстояния между парами элементов. При этом асимптотическое поведение границы не изменится.

Эта усовершенствованная граница позволяет доказать существование двоичных линейных кодов, для которых выполняется соотношение (2.0.8), с относительной скоростью  $R = 1 - H_2\left(\frac{1}{3}\right) = 0.0817042$ , что также доказывает существование линейных разделяющих  $(2, 1)$ -кодов с ненулевой скоростью 0.0817042.

Рассмотрим код, порождающая матрица которого является стандартной проверочной матрицей двоичного ВСН-кода с удаленной единичной строкой и подходящим гарантированным кодовым расстоянием. Используя оценку А. Вейля (Карлица-Ушиямы) (9.2.2), легко установить справедливость оценки (14.1.13) для таких кодов. К сожалению, этот способ позволяет построить конструктивным методом бесконечную последовательность разделяющих  $(2, 1)$ -кодов только с нулевой скоростью.

## 14.2 Каскадная конструкция дизъюнктивных кодов

Следующую простую и естественную конструкцию каскадного дизъюнктивного кода мы изложим сначала на теоретико-множественном языке, т.е. как семейства непересекающихся множеств.

**Определение 14.2.1** [*Каскадный дизъюнктивный код  $\mathcal{A}_n(\mathcal{C})$* ]

Пусть  $\mathcal{C}$  — произвольный  $q$ -значный код длины  $n$  и  $\mathcal{A}^{(k)} = \{\mathcal{A}_1^{(k)}, \dots, \mathcal{A}_q^{(k)}\}, k = 1, \dots, n$ , — множество семейств из  $q$  подмножеств такое, что каждое семейство  $\mathcal{A}_1^{(k)}$  является семейством подмножеств, которые в свою очередь являются подмножествами множества  $[1 + (k-1)N, kN] = \{1 + (k-1)N, \dots, kN\}$ . Таким образом, семейства  $\mathcal{A}_1^{(k)}$  и  $\mathcal{A}_1^{(k')}$  при  $k \neq k'$  определены на непересекающихся множествах  $[1 + (k-1)N, kN]$  и  $[1 + (k'-1)N, k'N]$ , а потому их элементы (их подмножества) также не пересекаются.

Набор подмножеств  $\mathcal{A}_n(\mathcal{C})$  образованный всеми подмножествами

$$\mathcal{A}_{\mathbf{x}} = \mathcal{A}_{x_1}^{(1)} \cup \mathcal{A}_{x_2}^{(2)} \cup \dots \cup \mathcal{A}_{x_n}^{(n)}, \mathbf{x} = (x_1, \dots, x_n) \in \mathcal{C}, |\mathcal{A}_{\mathbf{x}}| = nq, \quad (14.2.1)$$

множества  $\mathcal{N}_n = \bigcup_{k=1}^n \{(k-1)N + 1, \dots, N + (k-1)N\} = \{1, \dots, nN\} = [nN]$ , называется каскадным дизъюнктивным кодом, порожденным кодом  $\mathcal{C}$  и набором семейств  $\mathcal{A}_n = (\mathcal{A}^{(1)}, \dots, \mathcal{A}^{(n)})$ .

Очевидно, число элементов (обычно обозначаемое как  $T$ ) семейства  $\mathcal{A}_n(\mathcal{C})$  равно  $|\mathcal{C}|$ , а число элементов множества  $\mathcal{N}_n$  (длина соответствующего дизъюнктивного кода  $\mathcal{A}_n(\mathcal{C})$ ) равно  $|\mathcal{N}_n| = nN$ .

На теоретико-кодовом языке определение 14.2.1 выглядит следующим образом.

Пусть  $\mathcal{C} \subseteq \mathbb{F}_q^n$  —  $q$ -значный код длины  $n$  и  $\mathcal{A}$  — дизъюнктивный код длины  $N$  с  $q$  элементами, занумерованными элементами поля  $\mathbb{F}_q$ . В каждом векторе кода  $\mathcal{C}$  заменим элементы поля  $\mathbb{F}_q$  соответствующими им элементами дизъюнктивного кода  $\mathcal{A}$ . В результате получим дизъюнктивный каскадный код  $\mathcal{A}_n(\mathcal{C})$ , который имеет длину  $nN$  и  $|\mathcal{C}|$  элементов.

Код  $\mathcal{C}$  называется внешним кодом каскадного кода  $\mathcal{A}_n(\mathcal{C})$ , а дизъюнктивный код  $\mathcal{A}$  — внутренним кодом кода  $\mathcal{A}_n(\mathcal{C})$ .

Далее всюду полагается, что  $\mathcal{A}^{(k)} = \mathcal{A}^{(0)} + kN$ , т.е. каждое множество  $A_j^{(k)} \in \mathcal{A}^{(k)}$  является сдвигом множества  $A_j^{(0)}$ , а именно, состоит из элементов множества  $A_j^{(0)} = A_j$ , к которым прибавлено число  $(k-1)N$ .

**Теорема 14.2.1** Пусть

- i.  $\mathcal{C}$  —  $q$ -значный разделяющий  $(w, r)$ -код длины  $n$ ,
- ii  $\mathcal{A}_n = (\mathcal{A}^{(1)}, \dots, \mathcal{A}^{(n)})$  — набор  $(w, r)$ -семейств, непересекающихся множеств длины  $N$ , где каждое семейство  $\mathcal{A}^{(s)}$  определено на множестве  $[N] + (s-1)N$  и содержит  $q$  элементов (подмножеств).

Тогда каскадный код  $\mathcal{A}_n(\mathcal{C})$  является дизъюнктивным  $(w, r)$ -кодом длины  $nN$  с числом элементов равным  $|\mathcal{C}|$ .

**Доказательство** является достаточно простым и его предлагается провести читателю. (Упражнение)

## Скорость каскадного дизъюнктивного кода

Величина

$$\tau(\mathfrak{K}) = \frac{\log_2 |\mathfrak{K}|}{N} \quad (14.2.2)$$

называется скоростью дизъюнктивного кода  $\mathfrak{K}$  длины  $N$ .

Пусть  $\bar{\mathcal{K}} = \mathfrak{K}_1, \dots, \mathfrak{K}_m, \dots$ , бесконечная последовательность дизъюнктивных  $(w, r)$ -кодов с безграницно возрастающей длиной. Величина

$$\tau(\bar{\mathcal{K}}, r, w) = \overline{\lim}_{j \rightarrow \infty} \tau(\mathfrak{K}_j). \quad (14.2.3)$$

называется предельной скоростью последовательности  $\bar{\mathcal{K}}$ .

Мы хотим с помощью теоремы 14.2.1 и разделяющего  $(r, w)$ -кода Рида-Соломона построить бесконечную последовательность дизъюнктивных  $(w, r)$ -кодов  $\bar{\mathcal{K}} = \mathfrak{K}_1, \dots, \mathfrak{K}_m, \dots$ , с возможно большей предельной скоростью.

В качестве исходного кода  $\mathfrak{K}_1$  мы возьмем произвольный дизъюнктивный  $(w, r)$ -код длины  $n_1$  с  $q_1$  элементами, где  $q_1$  примарное число. Предположим, что код  $\mathfrak{K}_m$  длины  $n_m$  уже построен. Построим теперь код  $\mathfrak{K}_{m+1}$ , используя для этого разделяющий  $(r, w)$ -код Рида-Соломона с и теорему 14.2.1.

Пусть  $q_m$  — наибольшее примарное число такое, что  $|\mathcal{C}_m| = T_m \geq q_m$ . Отметим, что если  $T_m \rightarrow \infty$  при  $m \rightarrow \infty$ , тогда  $q_m \sim T_m$  при  $m \rightarrow \infty$ . Это вытекает из того факта, что простые числа в натуральном ряде расположены достаточно плотно.

Возьмем в качестве кода  $\mathcal{C}_{m+1}$  каскадный дизъюнктивный код  $\mathcal{A}_{q_m}(RS_{q_m}(n_m, d_m))$ , у которого внутренним кодом является дизъюнктивный  $(r, w)$ -код  $\mathcal{C}_m$ , а внешним —  $q_m$ -ичный разделяющий  $(w, r)$ -код  $RS_{q_m}(n_m, d_m)$ . Параметры  $n_m, d_m$  выберем так, чтобы код  $RS_{q_m}(n_m, d_m)$  имел наибольшее возможное число элементов.

Согласно лемме 14.1.2 если в качестве  $n_m$  взять число  $q_m$ , а в качестве  $k_m$  (размерности  $RS_{q_m}(n_m, d_m)$ ) взять наибольшее число для которого выполнено неравенство  $n_m > wr(k_m - 1)$ , то код  $RS_{q_m}(n_m, d_m)$  будет  $q_m$ -ичным разделяющим  $(w, r)$ -кодом, который имеет  $q_m^{k_m}$  элементов и длину  $n_m = q_m$ . Согласно теореме 14.2.1 код  $\mathcal{A}_{q_m}(RS_{q_m}(n_m, d_m))$  является дизъюнктивным  $(r, w)$ -кодом, который имеет длину  $q_m N_m$  и число элементов  $q_m^{k_m}$ ,  $k_m \leq \frac{q_m}{wr} + 1$ , где  $N_m$  — длина дизъюнктивного  $(r, w)$ -кода  $\mathcal{C}_m$ .

**Лемма 14.2.1** При  $wr > 1$  скорость  $\tau(s)_q(\bar{\mathcal{K}}, r, w)$ , построенной последовательности  $\bar{\mathcal{K}}$  дизъюнктивных  $(r, w)$ -кодов, равна нулю.

**Доказательство.** В виду того, что  $|\mathcal{C}_m| \sim q_m$  мы имеем

$$\tau(\mathfrak{K}_{m+1}) \sim \frac{\log_2 q_m}{wr N_m} \sim \frac{1}{wr} \tau(\mathfrak{K}_m), \quad m \rightarrow \infty. \quad (14.2.4)$$

Отсюда при любом постоянном  $s$  следует, что

$$\tau(\mathfrak{K}_m) \sim \left( \frac{1}{wr} \right)^s \tau(\mathfrak{K}_{m-s}), \quad s = \text{const}, \quad (14.2.5)$$

Из этого соотношения вытекает, что  $\lim_{m \rightarrow \infty} \tau(\mathfrak{K}_m) = 0$ .  $\square$

Автору неизвестен способ построения бесконечной последовательности дизъюнктивных  $(w, r)$ –кодов, где  $w = \text{const} \geq 2, r = \text{const} \geq 1, N \rightarrow \infty$ , с ненулевой скоростью, используя только лемму 14.1.2 и теорему 14.2.1.

Вместе с тем известно (см., например, [56], section 3.5), что величина

$$\tau(w, r) = \lim_{N \rightarrow \infty} \frac{\log_2 T(N, w, r)}{N}, \quad (14.2.6)$$

где  $T(N, w, r)$  — максимальное значение  $T$  при заданных  $N, w, r$ , является положительной при фиксированных  $w, r$  (теорема существования дизъюнктивных кодов с положительной скоростью). Из этой оценки следует, что существует бесконечная последовательность дизъюнктивных  $(w, r)$ –кодов (не обязательно каскадных) с положительной скоростью.

### 14.3 Максимальные дизъюнктивные $l$ –коды

**Определение 14.3.1** Пусть  $\mathcal{A}, |\mathcal{A}| = T \geq 2$ , — набор подмножеств множества  $[N]$  и  $l \leq T$ . Набор  $\mathcal{A}$  называется максимальным  $l$ – семейством неперекрывающихся множеств, если для набора  $\mathcal{A}$  выполнено соотношение (1.1.1) при всех  $w = 1, \dots, l$  и всех значений  $r$  таких, что  $w + r \leq T$ .

Соответствующая характеристическая матрица максимального семейства неперекрывающихся множеств называется максимальным дизъюнктивным  $l$ – кодом.

**Пример 14.3.1** Набор  $\mathcal{A} = \{\{1, 2\}, \{1, 3\}\}$  из двух подмножеств ( $T = 2, N = 3$ ) множества  $[3] = \{1, 2, 3\}$  и набор  $\mathcal{A}' = \{\{1, 2, 4\}, \{1, 3, 5\}, \{2, 3, 6\}\}$  из трех подмножеств ( $T = 3, N = 6$ ) множества  $[6]$  являются 2– семействами неперекрывающихся множеств.

Соответствующие дизъюнктивные максимальные 2– коды  $\mathcal{A}$  и  $\mathcal{A}'$  имеют вид.

$$\mathcal{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{и} \quad \mathcal{A}' = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (14.3.1)$$

Максимальные дизъюнктивные  $l$ – коды обладают следующим свойством: какие бы  $w, 0 \leq w \leq l$  столбцов в матрице максимального дизъюнктивного  $l$ – кода  $\mathcal{K}$  мы не выбрали, найдется строка, у которой на пересечении выбранных  $w$  столбцов с этой строкой находятся единицы, а все оставшиеся координаты этой строки равны нулю. Это очень сильное свойство. Поэтому, в некотором смысле, они (максимальные дизъюнктивные  $l$ – коды) являются вырожденными кодами, которые имеют большую длину и малое число элементов. Вместе с тем эти коды позволяют в теореме 14.2.1 заменить условие *ii*. на более слабое условие и тем самым построить новый класс каскадных дизъюнктивных кодов.

Максимальные дизъюнктивные  $l$ – коды  $\mathcal{A}$  мы будем называть максимальными кодами с  $q$  элементами, если  $|\mathcal{A}| = q$ . Например, код  $\mathcal{A}'$  является 2– кодом с тремя элементами.

### 14.3.1 Максимальный дизъюнктивный $l$ -код $\mathcal{Q}_{q,l}$ с $q$ элементами

Пусть

$$R_q^{(t)} = \{\{i_1, \dots, i_t\} \mid 1 \leq i_1 < \dots < i_t \leq q\}, \quad 1 \leq t \leq q, \quad (14.3.2)$$

— множество всех  $t$ -элементных подмножеств множества  $[q] = \{1, \dots, q\}$ . Очевидно,  $|R_q^{(t)}| = \binom{q}{t}$ .

Пусть  $R_q^{(t)}(s)$  — множество, состоящее из всех подмножеств  $R_q^{(t)}$ , которые содержат элемент  $s \in [q]$ . Очевидно,  $|R_q^{(t)}(s)| = \binom{q-1}{t-1}$ .

Пусть

$$Q_{q,l}(s) = R_q^{(1)}(s) \cup R_q^{(2)}(s) \cup \dots \cup R_q^{(l)}(s). \quad (14.3.3)$$

Очевидно,

$$|Q_{q,l}(s)| = \binom{q-1}{0} + \binom{q-1}{1} + \dots + \binom{q-1}{l-1} = B(q, l). \quad (14.3.4)$$

Таким образом, элементами множества  $Q_{q,l}(s)$  являются все подмножества множества  $[q]$  с числом элементов не более, чем  $l$ , содержащие фиксированный элемент  $s \in [q]$ .

В определении 14.1.1 положим  $N = B(q, l)$  и занумеруем в произвольном порядке элементы (подмножества)  $\kappa \in R_q^{(1)} \cup R_q^{(2)} \cup \dots \cup R_q^{(l)}$  с помощью элементов (чисел) множества  $[B(q, l)]$ . Номер элемента (множества)  $\kappa$  обозначаем через  $n(\kappa) \in [B(q, l)]$ .

В качестве подмножества  $A_s \subset [B(q, l)]$  в определении 14.1.1 возьмем множество, состоящее из всех номеров подмножеств из  $Q_{q,l}(s)$ , т.е.  $A_s = A_s^{(l)} = \{n(\kappa) \mid \kappa \in Q_{q,l}(s)\}$ .

Пример. Для  $l = 2$  и  $q = 3$  имеем  $|R_3^{(1)} \cup R_3^{(2)}| = 6$ . Множество  $A_s$  имеет вид  $A_s = \{n(\{s, 1\}), n(\{s, 2\}), n(\{s, 3\})\}$ ,  $s = 1, 2, 3$ , где  $n(\{s, j\})$ ,  $s \leq j$ , — номер подмножества  $\{s, j\} \subset \{1, 2, 3\}$ . При нумерации  $n(\{1, 2\}) = 1, n(\{1, 3\}) = 2, n(\{2, 3\}) = 3, n(\{1\}) = 4, n(\{2\}) = 5, n(\{3\}) = 6$  элементов множества  $R_3^{(1)} \cup R_3^{(2)}$  мы будем иметь  $A_1 = \{1, 2, 4\}, A_2 = \{1, 3, 5\}, A_3 = \{2, 3, 6\}$ , что дает набор  $\mathcal{A}'$  из примера 14.3.1. Отметим, что пересечение любых двух множеств  $A_s$  не пусто.

#### Определение 14.3.2 [Дизъюнктивный код $\mathcal{Q}_{q,l}$ ]

Пусть  $l \leq q$ . Набор множеств

$$\mathcal{Q}_{q,l} = \{\{Q_{q,l}(1)\}, \dots, \{Q_{q,l}(q)\}\} \quad (14.3.5)$$

и соответствующий ему набор

$$\mathcal{A}_q^{(l)} = \{A_1^{(l)}, \dots, A_q^{(l)}\}. \quad (14.3.6)$$

подмножеств множества  $[B(q, l)]$  будем называть элементарным дизъюнктивным  $l$ -кодом на  $q$ -множестве.

**Теорема 14.3.1** *Элементарный дизъюнктивный код  $\mathcal{Q}_{q,l}$  на  $q$ -множестве является  $l$ -семейством неперекрывающихся множеств. Его характеристическая матрица является дизъюнктивным  $l$ -кодом длины  $N = B(q, l)$  и числом элементов  $T = q$ .*

**Доказательство.** Пусть  $S = \{s_1, \dots, s_t\}$ ,  $1 \leq t \leq l$  —  $t$ -элементное подмножество множества  $[q]$  и  $\bar{S} = [q] \setminus S = \{s'_1, \dots, s'_{q-t}\}$  — дополнение к  $S$  в  $[q]$ . Если  $t = q$ , то  $\bar{S} = \emptyset$ . Для доказательства теоремы достаточно показать, что

$$\begin{aligned} A_{s_1}^{(l)} \cap \dots \cap A_{s_t}^{(l)} &\not\subset A_{s'_1}^{(l)} \cup \dots \cup A_{s'_{q-t}}^{(l)} \text{ или, что одно и то же} \\ Q_{q,l}(s_1) \cap \dots \cap Q_{q,l}(s_t) &\not\subset Q_{q,l}(s'_1) \cup \dots \cup Q_{q,l}(s'_{q-t}). \end{aligned} \quad (14.3.7)$$

Действительно,

$$\{s_1, \dots, s_t\} \subset Q_{q,l}(s_1) \cap \dots \cap Q_{q,l}(s_t), \quad (14.3.8)$$

так как в  $Q_{q,l}(s_j)$  по построению входят все  $u$ -множества,  $u = 1, \dots, l$ , содержащие элемент  $s_j \in S$ .

С другой стороны, множество  $\{s_1, \dots, s_t\}$  не принадлежит ни одному из  $t$ -множеств, входящих в  $Q_{q,l}(s'_i)$ , из-за того, что каждое множество в  $Q_{q,w}(s'_i)$  содержит элемент  $s'_i \in [q] \setminus S$ , который не принадлежит множеству  $\{s_1, \dots, s_t\} \subseteq S$ .

Заметим, что множество  $\{s_1, \dots, s_t\}$  заведомо не совпадает ни с каким множеством, у которого число элементов отлично от  $t$ .

Это доказывает справедливость соотношения (14.3.7).  $\square$

#### Теорема 14.3.2 Пусть

- i.  $\mathcal{C}$  —  $q$ -ичный разделяющий  $(w, r)$ -код длины  $n$ ;
- ii.

$$\mathcal{A}_n = (\mathcal{A}^{(1)}, \dots, \mathcal{A}^{(n)}) \quad (14.3.9)$$

— набор  $l$ -семейств, непокрывающих множеств с  $T = q$  элементами в каждом  $\mathcal{A}^{(j)}$  такой, что каждое семейство содержит  $q$  элементов. (см. определение 14.2.1)

Тогда каскадный набор подмножеств  $\mathcal{A}_n(\mathcal{C}) = \{A_{\mathbf{x}} | \mathbf{x} \in \mathcal{C}\}$  является  $(w, r)$ -семейством, непокрывающих множеств при любом  $r$ , если  $w \leq l$ , или, если  $w \geq q$  и  $l = q - 1$ .

**Доказательство.** Сначала рассмотрим случай  $w \leq l$ . Пусть  $\mathbf{x}_1, \dots, \mathbf{x}_w, \mathbf{y}_1, \dots, \mathbf{y}_r \in \mathcal{C}$  и  $\{\mathbf{y}_1, \dots, \mathbf{y}_r\} \cap \{\mathbf{x}_1, \dots, \mathbf{x}_w\} = \emptyset$ . Легко видеть, что

$$A_{\mathbf{x}_1} \cap \dots \cap A_{\mathbf{x}_w} = (A_{x_1}^{(1)} \cap \dots \cap A_{x_w}^{(1)}) \cup \dots \cup (A_{x_n}^{(n)} \cap \dots \cap A_{x_n}^{(n)}). \quad (14.3.10)$$

С одной стороны,  $\mathcal{C}$  — разделяющий  $(w, r)$ -код, поэтому существует такой номер  $k$  координаты векторов кода, что

$$\{x_{1,k}, \dots, x_{w,k}\} \cap \{y_{1,k}, \dots, y_{r,k}\} = \emptyset. \quad (14.3.11)$$

Обозначим через  $w'$  и  $r'$  число различных элементов множеств  $\{x_{1,k}, \dots, x_{w,k}\}$  и  $\{y_{1,k}, \dots, y_{r,k}\}$ . Понятно, что  $w' \leq w$  и при любом  $r$   $r' \leq q - w'$ .

С другой стороны, каждое семейство  $\mathcal{A}^{(k)} = \{A_1^{(k)}, \dots, A_q^{(k)}\}$  является семейством, непокрывающих множеств и  $l \geq w$ . Поэтому из определения  $l$ -семейств  $l$ -семейства вытекает, что

$$A_{x_{1,k}}^{(k)} \cap \dots \cap A_{x_{w,k}}^{(k)} \not\subset A_{y_{1,k}}^{(k)} \cup \dots \cup A_{y_{r,k}}^{(k)}. \quad (14.3.12)$$

при любом  $r' \leq q - w'$ .

Отсюда при любом  $r$  следует требуемое соотношение

$$\mathcal{A}_{x_1} \cap \dots \cap \mathcal{A}_{x_w} \not\subset \mathcal{A}_{x_1} \cup \dots \cup \mathcal{A}_{x_r}. \quad (14.3.13)$$

Рассмотрим теперь случай  $w \geq q$  и  $l = q - 1$ . В этом случае множество  $\{x_{1,k}, \dots, x_{w,k}\}$  из равенства (14.3.11) имеет не более, чем  $q - 1$  элемент, ибо число элементов у объединения этого множества и непустого множества  $\{y_{1,k}, \dots, y_{r,k}\}$  не превосходит  $q$ . Отсюда непосредственно вытекает требуемое соотношения (14.3.13) для этого случая.  $\square$

Отметим, что утверждение теоремы для случая  $w = 2$  было получено автором совместно с О.Ю. Приходовым в 1969 г. Совместная статья в том же году была опубликована в периодическом закрытом журнале, посвященном криптографической тематике.

Следует заметить, что теорема 14.3.2 существенно отличается от похожей на нее и широкоизвестной теоремы 14.2.1.

В условии теоремы 14.2.1 требуется, чтобы каждый код  $\mathcal{A}^{(s)}$  был дизъюнктным  $(w, r)$ -кодом, а  $\mathcal{C}$  — разделяющим  $(w, r)$ -кодом. Это требование в некоторых случаях является излишне сильным: теорема 14.3.2 утверждает, что в качестве  $\mathcal{A}^{(s)}$  можно взять произвольный дизъюнктивный  $w$ -код и в этом случае код  $\mathcal{A}_n(\mathcal{C})$  при любом  $r$  является дизъюнктивным  $(w, r)$ -кодом.

Таким образом, для построения дизъюнктивного  $(w, r)$ -кода теорема 14.3.2 в качестве внешнего кода  $\mathcal{C}$  допускает использование произвольного  $q$ -значного разделяющего  $(w, r)$ -кода с любым значением  $q > 1$ , а в качестве внутреннего кода  $\mathcal{A}^{(s)}$  — любого максимального  $w$ -семейства, непокрывающих множеств, с  $q$  элементами.

Отметим, что в теореме 14.2.1 параметр  $r$  фигурирует только в условии i. на разделяющий код  $\mathcal{C}$ . В условии ii. на семейство  $\mathcal{A}^{(s)}$  этот параметр не фигурирует.

Таким образом, теорема 14.2.1 позволяет свести построение дизъюнктивного  $(w, r)$ -кода к построению двух объектов:

(а)  $q$ -ичного разделяющего  $(w, r)$ -кода, где  $q \geq 2$  — любое;

и

(б) максимального дизъюнктивного  $w$ -кода с  $q$  элементами. Одним из возможных таких кодов является код  $\mathcal{Q}_{q,l}$  (см. теорему (14.3.1)).

Множество всех каскадных дизъюнктивных кодов заметно уже множества всех дизъюнктивных кодов. Поэтому следует ожидать, что дизъюнктивный код с наилучшими параметрами не является каскадным дизъюнктивным кодом. Вместе с тем структурность каскадных дизъюнктивных кодов, по мнению автора, делает их предпочтительными в практических приложениях, в частности, в криптографических.

Говоря не очень строго, мы ниже доказываем, что существуют бесконечная последовательность каскадных дизъюнктивных кодов с фиксированными параметрами  $w$  и  $r$ , скорость которой отлична от нуля. Все эти коды строятся с помощью теоремы 14.2.1 и соответствующих наилучших разделяющих кодов, известных из теоремы их существования. Как построить последовательность каскадных дизъюнктивных кодов, скорость которой отлична от нуля без использования теоремы 14.3.2, неизвестно. Одна из неудачных попыток такого рода приведена в лемме 14.2.1.



### Бесконечная последовательность каскадных дизъюнктивных кодов с ненулевой скоростью существует

Пусть  $\tau_q(N, w, r)$  — максимальная скорость дизъюнктивного каскадного  $(w, r)$ — кода длины  $N$ , у которого внешним кодом является  $q$ — значный разделяющий код, а внутренним — дизъюнктивный код  $\mathfrak{K}$  с  $q$  элементами. Положим

$$\tau_q(w, r) = \overline{\lim}_{N \rightarrow \infty} \tau_q(N, w, r). \quad (14.3.14)$$

Как уже отмечалось, что существуют  $q$ — ичные разделяющие  $(w, r)$ — коды длины  $n$  (см., например, [58], chapter 6) с ненулевой скоростью при  $q, w, r = \text{const}$ ,  $n \rightarrow \infty$ . Слово "скорость" в данном случае означает скорость кода в обычном теоретико-кодовом смысле.

Из теоремы 14.3.2 и теоремы 13 работы [58] (нижней границы существования двоичного разделяющего  $(w, r)$ — кода) непосредственно вытекает

**Теорема 14.3.3** *Рассмотрим бесконечную последовательность  $\overline{\mathfrak{K}} = \mathfrak{K}(\mathcal{C}_1), \mathfrak{K}(\mathcal{C}_2), \dots$ , каскадных дизъюнктивных  $(2, r)$ — кодов длины  $N_j$ , у которых внутренним дизъюнктивным кодом  $\mathfrak{K}$  является, рассмотренный в примере 14.3.1, максимальный дизъюнктивный 2— код с двумя элементами и длины 3, а внешними кодами — бесконечная последовательность  $\overline{\mathcal{C}} = \mathcal{C}_1, \mathcal{C}_2, \dots$ , двоичных разделяющих  $(2, r)$ — кодов  $\mathcal{C}_j$  длины  $n_j$ . Пусть  $n_j \rightarrow \infty$ , когда  $j \rightarrow \infty$ , и  $R_2(\overline{\mathcal{C}}) = \overline{\lim}_{j \rightarrow \infty} \frac{\log_2 |\mathcal{C}_j|}{n_j}$  — скорость последовательности  $\overline{\mathcal{C}}$  разделяющих двоичных  $(2, r)$ — кодов.*

*Тогда скорость  $\tau(\overline{\mathfrak{K}}) = \overline{\lim}_{j \rightarrow \infty} \frac{\log_2 |\mathfrak{K}(\mathcal{C}_j)|}{N_j}$  последовательности  $\overline{\mathfrak{K}}$  равна*

$$\tau(\overline{\mathfrak{K}}) = \frac{1}{3} R_2(\overline{\mathcal{C}}). \quad (14.3.15)$$

*В частности, если каждый код  $\mathcal{C}_j$  является разделяющим  $(2, r)$ — кодом с максимальным числом элементов, то*

$$\tau_2(2, r) \geq \frac{1}{3} R_2(2, r) \geq \frac{1}{3} Y(2, r). \quad (14.3.16)$$

где функция  $Y(w, r)$  определена равенством (14.1.8).

**Доказательство** теоремы являются непосредственно вытекают из следующих определений: каскадного дизъюнктивного  $(2, r)$ — кода, максимального дизъюнктивного 2— кода, и теорем 14.3.2 и 14.1.1.  $\square$

Подобную теорему можно доказать и для всех фиксированных  $q > 2$ .

Для величины  $\tau(2, 1)$  (см. (14.3.14)) справедлива оценка  $\tau(2, 1) \geq \underline{\tau}(2, 1) = 0,149$ , где  $\underline{\tau}(2, 1)$  — нижняя оценка величины  $\tau(2, 1)$ , полученная в [56].

В тоже самое время, правая часть (14.3.16) для этого случая равна  $\frac{R_2(2, 1)}{3} = \frac{Y(2, 1)}{3} = \frac{0.2075}{3} = 0.0691667$  (см. (14.1.7) и теорему 14.1.1).

Хотя это число заметно меньше числа  $\underline{\tau}(2, 1)$ , этот результат устанавливает справедливость следующего нетривиального результата: предельная скорость бесконечной последовательности каскадных дизъюнктивных  $(2, 1)$ — кодов, построенных с помощью одного внутреннего двоичного дизъюнктивного 2— кода  $\mathfrak{K}$  примера 14.3.1 длины 3 и бесконечной последовательности максимальных разделяющих двоичных  $(2, 1)$ — кодов (внешний коды), является положительной.

## 14.4 Криптографические приложения дизъюнктивных кодов

Перед чтением этого параграфа читателю рекомендуется ознакомиться с материалами главы 13, раздел 13.1. Некоторые введенные там понятия мы будем использовать без объяснения.

Мы рассматриваем только случай  $w = 2$ . Общий случай рассматривается аналогичным образом.

Системы распределения ключей, использующие дизъюнктивные  $(2, r)$ -коды, рассматривались в работах [54, 74, 82] и многих других.

Мы будем пользоваться обозначениями, введенными в начале раздела 13.1.3.

Сформулируем основные идеи, которые позволят построить системам распределения ключей с помощью дизъюнктивных кодов. Система включает в себя следующие объекты.

- 1 Множество  $\mathfrak{T}$ ,  $|\mathfrak{T}| = T$ , пользователей (абонентов), элементы которого индексируются элементами множества  $\mathcal{Q} = [T] = \{1, \dots, T\}$ , Далее мы будем работать только с множеством  $\mathcal{Q}$ , мысленно связывая элемент  $j \in \mathcal{Q}$  с пользователем  $\mathfrak{T}_j$
- 2 Исходное множество независимых секретных ключей  $\mathfrak{K} = \{k_1, \dots, k_N\}$  генерируется центром доверия. Подмножества множества  $\mathfrak{K}$  являются секретными ключами пользователей. Никаких алгебраических действий с ключами в рассматриваемой системе не производится. Этим она отличается систем, рассмотренных в предыдущей главе.
- 3 Пусть  $\mathcal{A} = \{A_1, \dots, A_T\}$  — общеизвестное  $(2, r)$ -семейство непокрывающих множеств на множестве  $[N]$  с числом элементов  $T$  (дизъюнктивный  $(2, r)$ -код длины  $N$  и числом элементов  $T$ ).

Центр доверия снабжает каждого пользователя  $j \in \mathcal{Q}$  множеством секретных ключей

$$\mathfrak{K}_j = \{k_s \mid s \in A_j\} \subset \mathfrak{K}. \quad (14.4.1)$$

Множество  $\mathfrak{K}_j$  является совокупностью ключей, которые пользователь  $j$  использует для порождения ключей для связи с другим пользователем.

- 4 Множество  $\mathfrak{K}_{i,j}$  общих ключей пары пользователей  $i, j \in \mathcal{Q}$  представляет собой множество

$$\mathfrak{K}_{i,j} = \mathfrak{K}_i \cap \mathfrak{K}_j. \quad (14.4.2)$$

Как легко видеть, в рассматриваемой схеме распределения ключей, основанной на дизъюнктивном  $(2, r)$ -коде, каждая коалиция  $S \subset \mathcal{Q}, |S| \leq r$ , пользователей не имеет возможностей для получения всех ключей множества  $\mathfrak{K}_{i,j}$ , если  $i, j \notin S$ , т.е. всегда у пары  $i, j$  имеется, по меньшей мере один общий ключ из  $\mathfrak{K}_i \cap \mathfrak{K}_j$ , который не входит в объединение ключей недобросовестных пользователей из коалиции  $S$ . Подобные системы распределения ключей называются системами, устойчивыми к  $r$  компрометациям.

Совокупность ключей множества  $\mathfrak{K}_i \cap \mathfrak{K}_j$  используется как общая ключевая информация пользователей  $i$  и  $j$ .

**5** Сложностью рассмотренной системы распределения ключей естественно назвать число

$$a = \max_{j \in \mathcal{Q}} |\mathfrak{K}_j|, \quad (14.4.3)$$

т.е. число равное верхней границе числа секретных ключей, которые каждый пользователь хранит в своей электронной памяти. Если все числа  $|\mathfrak{K}_j|$  равны, то  $a$  является числом ключей, хранимых каждым пользователем системы.

Таким образом, для криптографических приложений естественно максимизировать  $T$  (число пользователей) при заданном числе  $a$  ключей, которое хранит каждый пользователь системы.

Например, сложность (в нашей терминологии) тривиального 2- семейства  $\mathcal{Q}_{q,2}$  равна  $a(Q_{q,2}) = B(q, 2) = \binom{q-1}{0} + \binom{q-1}{1} = q$  (см. (14.3.4)), а сложность каскадного  $(2, r)$ - семейства  $\mathcal{Q}_n(\mathcal{C})$  равна  $a(\mathcal{Q}_n(\mathcal{C})) = qn$ , где  $n$  — длина разделяющего  $q$ - значного  $(w, r)$ - кода  $\mathcal{C}$ .



# Литература

- [1] Казарин Л.С., *Личное сообщение*.
- [2] *Дискретная математика, Энциклопедия, Из-во*.
- [3] Нечаев А.А. Глухов М.М., Елизаров В.П, *Алгебра*, vol. часть 2, Москва, 1991.
- [4] Нечаев А.А. Кузмин А.С, Куракин А.А., *Кольца Галуа в приложениях к кодам и линейным рекуррентам*, Москва, 1998.
- [5] М.А. Цфасман С.Г. Влэдущ, Д.Ю. Ногин, *Алгеброгеометрические коды*, МЦНМО, 2003.
- [6] Зайцев Г.В, Зиновьев В.А., Семаков Н.В., *Быстрое корреляционное декодирование блочных кодов*, Сб. Кодирование и передача сообщений в системах блочных кодов, М. Наука. **24** (1976), 74–85.
- [7] МакВильямс Ф. Дж., Слоэн Н.Д.А., *Коды, корректирующие ошибки*, Связь, М., 1979.
- [8] А.А. Нудельман М.Г. Крейн, *Проблемы моментов Маркова и экстремальные задачи*, Наука, Физматлит, Москва, 1973.
- [9] Зяблов В.В. Блох Э.Л., *Обобщенные каскадные коды*, Связь, М., 1976.
- [10] Т. Ито Э. Баннаи, *Алгебраическая комбинаторика. Схемы отношения*, Москва, Мир, 1987.
- [11] Г. Нидеррайтер Р. Лидл, *Конечные поля, т.1, 2*, Мир, Москва, 1988.
- [12] Сидельников В.М., Першаков А.С., *Декодирование кодов Рида-Маллера при большом числе ошибок*, Пробл. передачи информации **28** (1992), по. 3, 80–94.
- [13] В.М. Сидельников С.О. Шестаков, *О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона*, Дискретная математика **4** (1992), по. 3, 57–63.
- [14] Серр Ж.-П, *Линейные представления конечных групп*, Мир, М., 1970.
- [15] Кострикин А. И., *Введение в алгебру*, Наука, М., 1977.
- [16] В. М. Сидельников, *Об экстремальных многочленах, используемых при оценках мощности кодов*, Проблемы передачи информации **16** (1980), по. 3, 17–30.

- [17] Лицын С.Н. , *О сложности декодирования низкоскоростных кодов Риды-Маллера*, Тр. IX Всесоюзн. конф. по теории кодирования и передачи информации **Ч.1** (Одесса, 1988), 202–204.
- [18] Лидл Р., Пильц Г., *Прикладная абстрактная алгебра: Учеб. пособие.*, пер. с англ., Екатеринбург, 1996.
- [19] Сидельников В.М., Струнков С.П., *О спектре орбитных кодов в пространстве матриц*, Вест. Моск. ун-та, математика, механика (1998), по. 5, 58–61.
- [20] Ким Ш.Х., Лебедев В.С., *Об оптимальности тривиальных кодов, свободных от  $(w, r)$ –перекрываний*, Проблемы передачи информации **40** (2004), по. 3, 13–20.
- [21] Н.И. Ахиезер, *Классическая проблема моментов*, Физматлит, Москва, 1961.
- [22] Ф.Р. Гантмахер, *Теория матриц*, Из-во Наука. Москва, 1966.
- [23] Ленг С., *Алгебра*, Мир, Москва, 1968.
- [24] Сидельников В.М., *О спектре весов двоичных кодов Боуза-Чоудхури-Хоквингема*, Проблемы передачи информации **7** (1971), по. 1, 16–22.
- [25] В.Д. Гошпа, *Коды на алгебраических кривых*, ДАН СССР **259** (1981), по. 6, 1289–1290.
- [26] Сидельников В.М., *Линейные троичные квазисовершенные коды, исправляющие две ошибки*, Проблемы передачи информации **22** (1986), по. 4, 43–48.
- [27] Нечаев А.А., *Код Кердока в циклическом виде*, Дискретная математика **1** (1989), по. 4, 123–139.
- [28] И.Я. Виленкин, *Специальные функции и теория представлений групп*, 2 ed., Наука, Москва, 1991.
- [29] Нечаев А.А., *Линейные рекуррентные последовательности над коммутативными кольцами*, Дискретная математика **3** (1991), по. 3, 107–121.
- [30] Ю.Л. Сагалович, *Разделяющие системы*, Проблемы передачи информации **30** (1994), по. 2, 14–35.
- [31] Сидельников В.М., *Декодирование кода Риды-Соломона при числе ошибок, большем  $\frac{(d-1)}{2}$ , и нули многочленов нескольких переменных*, Проблемы передачи информации **30** (1994), по. 1, 51–69.
- [32] Н. Коблиц, *Курс теории чисел и криптография*, Из-во ТВП, Москва, 2001.
- [33] Лебедев В.С., *Асимптотическая верхняя оценка граница для скорости кодов, свободных от  $(w, r)$ –перекрываний*, Проблемы передачи информации **39** (2003), по. 4, 3–10.
- [34] Бассалыго Л.А., *Новые верхние границы для кодов, исправляющих ошибки*, Пробл. передачи информации **4** (1965), 41–44.

- [35] Сидельников В.М., *О взаимной корреляции последовательностей*, Проблемы кибернетики (1971), no. 24, 15–42.
- [36] Сидельников В.М., *О взаимной корреляции последовательностей*, Доклады АН СССР **196** (1971), no. 4.
- [37] ———, *О плотнейшей укладке шаров на поверхности  $n$ -мерной евклидовой сферы и числе векторов двоичного кода с заданным кодовым расстоянием*, Доклады АН СССР **213** (1973), no. 5.
- [38] ———, *Верхние оценки числа точек двоичного кода с заданным кодовым расстоянием*, Пробл. передачи информации **10** (1974), no. 2.
- [39] И.М. Гельфанд, *Лекции по линейной алгебре*, МЦНМО, Москва, 1998.
- [40] Кострикин А.И., *Линейная алгебра*, Физ.-мат. лит., Москва, 2000.
- [41] А.И. Кострикин, *Основные структуры алгебры. Ч. III*, Физ. Мат. Лит., Москва, 2001.
- [42] Сидельников В.М., *Ассоциативные схемы и метрики на конечной группе*, Доклады РАН **396** (2004), no. 4.
- [43] *Дискретная математика*, Из-во Большая Российская энциклопедия, 2004.
- [44] Frieze A. Dyer M., Fenner T. and Thomason A., *On Key Storage in Secure Networks*, J. Cryptology **8** (1995), no. 4, 189–200.
- [45] A.E Brouwer, A.M Cohen , A. Neumaier , *Distance-Regular Graphs*, Springer-Verlag, Berlin Heidelberg New York, 1989.
- [46] P. W. Shor A. R. Calderbank, *Good quantum codes exist*, Phys. Rev Letters **54** (1996), no. 2, 1098–1105.
- [47] P. W. Shor N.J.A. Sloan A. R. Calderbank, E.M. Rains, *Quantum error correction via codes over  $gf(4)$* , IEEE Trans. on Inform. Theory **44** (1998), no. 4, 1369–1387.
- [48] E.F. Assmus and H.F. Mattson, *Coding and combinatorics*, SIAM Review **16** (1974), 349–388.
- [49] A. Beimel and B. Chor, *Interaction in key distribution schemes*, In Advances in cryptology — CRYPTO’93 (1993), 444–455.
- [50] A. Beimel and B. Chor, *Communication in key distribution schemes*, IEEE Trans. on Inform. Theory **42** (1996), no. 1, 19–28.
- [51] Mattos L. A. F. Blundo, C. and D. R. Stinson, *Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution*, In Advances in cryptology — CRYPTO’96 (1996), 387–400.
- [52] Herzberg A. Kutten S. Vaccaro U. Blundo C., De Santis A. and M. Yung, *Perfectly-secure key distribution for dynamic conferences*, In Advances in cryptology — CRYPTO’92 (1992), 471–486.

- [53] P.J. Cameron, *Permutation groups*, London Mathematical Society, Cambridge University Press, 1999.
- [54] Mitchell C.J. and Piper F.C., *Key storage in secure network*, Discrete Applied Mathematics **21** (1988), 215–228.
- [55] Higman D.G., *Intersection matrices for finite permutation groups*, J. Algebra **6** (1967), 22–42.
- [56] A. D'yachkov, A. Macula P. Vilenkin, and D. Torney, *Families of finite sets in which no intersectin of  $l$  sets is covered by the union of  $s$  other*, J. of Combinatorial Theory **S. A 99** (2002), 195–218.
- [57] T. Ito E. Bannai, *Algebraic Combinatocs I*, Benjamin/Cummings, Menlo Park, California, USA, 1984.
- [58] H.G. Schaathum G.D. Cohen, *Asymptotic overview on separating codes*, Report No 248 (May 2003).
- [59] S.W. Golomb, *Shifty-register sequences*, Aegean Park Press, 1982.
- [60] Li Gong and Wheeler D.H., *A matrix key distribution scheme*, Journal of cryptology **2** (1990), 51–59.
- [61] C. D. Gonsil, *Algebraic combinatorics*, Charman and Hall, New York, 1993.
- [62] D.A. Gottesman, *Class quantum error-correcting saturating the quantum hamming codes bound*, Phys. Rev. A. **54** (1998), 1862–1868.
- [63] V. Guruswami and M Sudan, *Improved decoding of reed-solomon and algebraic-geometric codes*, IEEE Trans. on Inform. Theory **45** (1999), no. 6, 1757–1767.
- [64] Hyun Kwang Kim, Vladimir Lebedev, *On optimal superimposed codes*, Journal Combinatorial Designs **12** (2004), no. 2, 373–384.
- [65] W.H. Kautz and R.C. Singleton, *Nonrandom binary superimposed codes*, IEEE Trans. Inform. Theory **10** (1964), 363–377.
- [66] V.I Levenshtein, *Bounds self-complementary codes and their applications*, Eurocode 1992 (Springer-Verlag, Wien-New York), 1993, pp. 159–171.
- [67] R.J. McEliece, *Public-key cryptosystem based on algebraic coding theory*, In DSN Progress Report 42-44, (1978), 114–116.
- [68] Akihiro Munemasa, *Personal communication*.
- [69] H. Niederreiter, *Knapsack-type cryptosystem and algebraic coding theory*, Probl. Control and Inform. Theory **15** (1986), 19–34.
- [70] Sloane N.J.A., *Covering arrays and intersecting codes*, J. Combinatorial Designs **1** (19), no. 1.



- [71] Camion P., *Codes and associaton schemes: Basic properties of association schemes relevant to coding*, vol. II, Elsevier, Amsterdam, 1998.
- [72] Delsarte Ph., *An algebraic approach to association schemes in coding theory*, Philips Res. Reps. Suppl. **10** (1973).
- [73] Delsarte Ph. and Levenshtein V., *Association schemes and coding theory*, IEEE Trans., IT **44** (1998), no. 6, 2477–2504.
- [74] K.A.S. Quinn, *Some constructions for key distribution pattens*, Designs, Codes and Cryptography **4** (1994), 177–191.
- [75] Blom R., *An optimal class of symmetric key generation systems*, Eurocrypt' 84 (1984), 335–338.
- [76] Stinson Doug R. and Tran Van Trung, *Some new results on key distribution pattens and broadcast encryption*, Design, codes and cryptography **14** (1998), no. 3, 261–280.
- [77] M. Gr R. Grahem (ed.).
- [78] Sh. Zigangirov R. Johannesson, K., *Fundamentals of covolutional coding*, DigitalMobile Communication, IEEE, Inc., New York, 1999.
- [79] R.J. McEliece, E.R. Rodemich, H.C. Rumsey, Jr. and L.R. Welch, *New upper bounds on the rate of a code via the delsartre-macwillams inequaties*, IEEE Trans. Inform. Theory **23** (1977).
- [80] A.M Steane, *Erlargement of calderbank-shor-steane codes*, IEEE Trans. on Inform. Theory **45** (1996), no. 7, 2492–3495.
- [81] ———, *Error-correcting codes in quantum theory*, Phys. Rev Letters **77** (1996), 793–797.
- [82] D.R. Stinson, *On some methods for unconditionally secure key distribution and broadcast encryption*, Designs, Codes and Cryptography **12** (1997), 215–243.
- [83] Th. Ericson, V. Zinoviev, *Codes on euclidean spheres*, Elsevier, Amsterdam-London-New York-Oxford-Paris-Shannon-Tokyo, 2001.
- [84] V.I. Levenshtein, *Universal bounds for codes and designs*, Handbook of coding theory, Elsevier Science, Edited by V.S. Pless and W.C. Huffman, 1998.