О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ ФОРМУЛАМИ

О. Б. ЛУПАНОВ

(МОСКВА)

Для оценки сложности схем (в частности, формул), реализующих функции алгебры логики, Риорданом и Шенноном [1, 2] была введена функция $L(n)$, характеризующая минимальное число элементов в схеме, достаточное для реализации любой функции алгебры логики n аргументов.

В предлагаемой работе выводится асимптотическое выражение для аналогичной функции в случае формул, построенных из функций некоторого базиса, удовлетворяющего определенным условиям. При этом оказывается, что все базисы в некотором смысле эквивалентны. В качестве следствия получается (§ 2) асимптотическое выражение для $L(n)$ в случае контактных П-схем.

Эти результаты основаны, с одной стороны, на нижних оценках для индекса простоты рассматриваемого здесь вида, полученных Р. Е. Кричевским [3], и, с другой стороны, на некоторых результатах автора [4, 5, 6]. В построении существенную роль играют некоторые факты из теории самокорректирующихся кодов [7].

Основной результат работы может быть обобщен на случай функций k-значной логики.

§ 1

Пусть $\Phi=\{\varphi_1, \ldots, \varphi_Q\}$ —полная [8, 9, 10] система функций алгебры логики (называемая в дальнейшем базисом)*). Выражения вида $\varphi_i(x_1, \ldots, x_{k_i})$ $(1\leqslant i\leqslant Q)$, состоящие каждое из знака функции базиса левой и правой скобок и знаков существенных аргументов этой функции, назовем *базисными формулами*. Пусть далее каждой функции φ_i из Φ поставлено в соответствие неотрицательное число P_i—*индекс простоты* этой функции; будем предполагать, что функция φ_i существенно зависит от k_i аргументов $(i=1, \ldots, Q)$. Систему Φ функций φ_i с приписанными им индексами простоты P_i будем обозначать $\hat{\Phi}$.

Будем рассматривать формулы, являющиеся суперпозициями базисных формул. *Индекс простоты* $L(F)$ *формулы* F определим как сумму индексов простоты всех вхождений в F символов функций базиса.

Например,

$$L(\varphi_1(x_1, \ldots, x_{k_1}))=P_1,$$

$$L(\varphi_1(\varphi_1(x_1, \ldots, x_{k_1}), \varphi_1(x_1, \ldots, x_{k_1}), x_1, \ldots, x_1))=3P_1.$$

*) То есть такая, что всякая функция алгебры логики может быть выражена через функцию из Φ.

Обозначим через $L(f)$ минимальный индекс простоты формул F, реализующих функцию f. Пусть $L_{\hat{\Phi}}(n)$— минимальное число L такое, что формулами с индексом простоты, не превосходящим L, можно реализовать любую функцию алгебры логики n аргументов. Другими словами, $L_{\hat{\Phi}}(n)=\max L(f)$, где максимум берется по всем функциям n переменных.

Мы не будем различать функций, получающихся друг из друга добавлением или изъятием несущественных переменных.

Все числа, фигурирующие в дальнейшем, суть целые неотрицательные числа (за исключением индексов простоты, которые принимают действительные неотрицательные значения).

Нашей основной целью является доказательство следующего утверждения.

Основная теорема. *Если для всех функций базиса, существенно зависящих более чем от одного аргумента,* $P_i > 0$, *то*

$$L_{\hat{\Phi}}(n) \sim \varrho \frac{2^n}{\lg_2 n},$$

где

$$\varrho = \min_{k_i \geqslant 2} \frac{P_i}{k_i - 1}.$$

Из сформулированной теоремы следует, что функция $L_{\hat{\Phi}}(n)$ очень слабо зависит от $\hat{\Phi}$: именно зависит только от «удельного веса» $\frac{P_i}{k_i-1}$ самой хорошей функции базиса.

Для иллюстрации этой теоремы, еще до доказательства ее, в следующем параграфе (§ 2) приводится ее приложение к нахождению асимптотической формулы для аналогично определяемой функции $L^{\text{п}}(n)$, оценивающей число контактов в параллельно-последовательных схемах. Правда, эта формула может быть получена непосредственно (т. е. без применения теоремы) более просто.

Доказательство заключается в установлении соотношений

$$L_{\hat{\Phi}}(n) \geqslant \varrho \frac{2^n}{\lg_2 n}, \tag{1.1}$$

$$L_{\hat{\Phi}}(n) \leqslant \varrho \frac{2^n}{\lg_2 n}. \tag{1.2}$$

Первое из них (даже при более общих предположениях) получено Р. Е. Кричевским [3]*). Ниже будет установлено второе асимптотическое неравенство.

Ввиду некоторой сложности доказательства приведем его схему. Сначала в § 3 описываются специального вида суперпозиции функций базиса и доказываются некоторые их свойства. В § 4 приводятся верхние оценки индексов простоты ряда вспомогательных формул. В § 5 вводится основное понятие—регулярность разбиения множеств наборов и доказывается соотношение (1.2) в предположении, что регулярное разбиение существует. Последующие параграфы (§ 6—9) посвящены доказательству существования такого разбиения. В § 6 излагаются некоторые свойства самокорректирующихся кодов и описывается разбиение множества всех наборов опреде-

*) Кроме того, из результатов Р. Е. Кричевского следует, что для любого $\varepsilon>0$ и $n > n_\varepsilon$ доля функций f, для которых $L(f) < (1-\varepsilon)\,\varrho\,\frac{2^n}{\lg_2 n}$, стремится к нулю с ростом n. Отсюда и из (1. 2) вытекает, что почти все функции почти так же плохи, как самая плохая, а для этого большинства функций описываемый ниже метод позволяет строить асимптотически наилучшие формулы.

ленной длины на попарно не пересекающиеся подмножества, называемые сферами и обладающие определенными свойствами. В § 7 строится другое разбиение наборов, основанное на утверждениях § 6 и связанное с базисом. В § 8—9 устанавливается, что это разбиение является регулярным, и тем самым завершается доказательство основной теоремы этой работы.

§ 2

Пусть $L^{\text{П}}(f)$ (соответственно $L^{\text{П}}(n)$)—минимальное число контактов, достаточное для реализации функции f (соответственно любой функции алгебры логики n аргументов) в классе П-схем.

Теорема*).

$$L^{\text{П}}(n) \sim \frac{2^n}{\lg_2 n}.$$

Доказательство. Рассмотрим базис

$$\Phi = \{\varphi_1(x, y),\ \varphi_2(x, y),\ \varphi_3(x)\},$$

где

$$\varphi_1(x, y) = x \vee y,\ \varphi_2(x, y) = x \,\&\, y,\ \varphi_3(x) = \overline{x},$$

и пусть $P_1 = P_2 = 1$, $P_3 = 0$ (см. § 1). В этом случае согласно основной теореме (§ 1)

$$L_{\hat{\Phi}}(n) \sim \frac{2^n}{\lg_2 n}. \tag{2.1}$$

Далее, очевидно, что

$$L_{\hat{\Phi}}(f) = L^{\text{П}}(f) - 1$$

и, следовательно,

$$L_{\hat{\Phi}}(n) = L^{\text{П}}(n) - 1. \tag{2.2}$$

Утверждение теоремы вытекает из (2.1) и (2.2).

Теорема доказана.

§ 3

Пусть формула $G(y_1, \ldots, y_s)$ (являющаяся, как было сказано, суперпозицией базисных функций) реализует функцию $g(x_1, \ldots, x_n)$ ($y_1, \ldots, y_s$ суть все вхождения переменных $x_1, \ldots, x_n$ в формулу G) и пусть $x_{i_1}, \ldots, x_{i_m}$—все существенные переменные функции g. Будем называть формулу G *правильной*, если в ней можно выделить вхождения $y_{j_1}, \ldots, y_{j_m}$ соответственно переменных $x_{i_1}, \ldots, x_{i_m}$ (называемые в дальнейшем *выделенными* вхождениями), так что результат замещения только этих вхождений константами $\sigma_{i_1}, \ldots, \sigma_{i_m}$ тождественно равен $g(\sigma_1, \ldots, \sigma_n)$, причем последнее справедливо для любого набора $(\sigma_1, \ldots, \sigma_n)$.

Пример. Пусть $\varphi(x, y)$ есть базисная формула, выражающая функцию $\overline{x} \vee \overline{y}$. Тогда формула $\varphi(x, x)$ не является правильной, а формула $\varphi(x, \varphi(x, x))$ является таковой.

Замечание 1. Всякая базисная формула является правильной.

Замечание 2. Всякая формула, выражающая константу, является правильной.

Замечание 3. Если формулы

$$G_1(y_1, \ldots, y_k, y_{k+1}, \ldots, y_s) \text{ и } G_2(z_1, \ldots, z_l, z_{l+1}, \ldots, z_t)$$

*) Известно, что $L^{\text{П}}(n) \geqslant \frac{2^n}{\lg_2 n}$ [1] и $L^{\text{П}}(n) \leqslant \frac{2^{n+1}}{\lg_2 n}$ [5].

правильны и $y_1, \ldots, y_k$ и $z_1, \ldots, z_l$ суть все выделенные вхождения переменных соответственно в формулах G_1 и G_2, причем множества $\{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k\}$ и $\{z_1, \ldots, z_l\}$ не пересекаются, то формула

$$G_1(y_1, \ldots, y_{i-1}, G_2(z_1, \ldots, z_l), y_{i+1}, \ldots, y_s)$$

(т. е. результат замещения вхождения y_i в формуле G_1 формулой G_2) является правильной и $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_k, z_1, \ldots, z_l$ — выделенные вхождения в ней.

Следствие (из замечаний 2, 3). Если функция $g(x_1, \ldots, x_n)$ может быть выражена правильной формулой, то и всякая функция, получающаяся из $g(x_1, \ldots, x_n)$ путем подстановки констант (а константы в силу полноты базиса и замечания 2 допускают представление правильными формулами), также может быть выражена правильной формулой.

Замечание 4. Если функция $g_1(x_1, \ldots, x_n)$ реализуется правильной формулой G_1, а функция $g_2(y_1, \ldots, y_m)$ — формулой G_2 (множества $\{x_1, \ldots, x_n\}$ и $\{y_1, \ldots, y_m\}$ могут пересекаться; G_2 не обязательно правильная), то для функции $g = g_1(x_1, \ldots, x_{i-1}, g_2(y_1, \ldots, y_m), x_{i+1}, \ldots, x_n)$ справедливо соотношение

$$L(g) \leqslant L(G_1) + L(G_2).$$

Замечание 5. Если функция g получается из функции f путем отождествления некоторых подмножеств переменных, то $L(g) \leqslant L(f)$.

Лемма 1. *Существуют правильные формулы, выражающие функции*

1) *константы* 0 *и* 1,

2) $\bar{x}$,

3) $x \vee y$, $x \& y$.

(леммы)

Доказательство. 1) Первое утверждение теоремы следует из полноты базиса и замечания 2.

2) В силу теоремы Поста о полноте системы функций [8, 9, 10] в базис Ф входит немонотонная функция. Из нее путем подстановки констант можно получить немонотонную функцию одного переменного [10], т. е. $\bar{x}$, и поэтому в силу следствия можно построить правильную формулу для $\bar{x}$.

3) В силу упомянутой теоремы Поста в Ф входит нелинейная функция. Из нее путем подстановки констант можно получить нелинейную функцию двух переменных [10]*) (в силу следствия эта функция может быть реализована правильной формулой); это может быть одна из функций (с точностью до наименований переменных):

$$x \& y,\ x \& \bar{y},\ \bar{x} \& \bar{y},\ x \vee y,\ x \vee \bar{y},\ \bar{x} \vee \bar{y}.$$

Очевидно, что, используя отрицание, из каждой из этих функций можно получить функции $x \& y$ и $x \vee y$, причем из замечания 3 и п. 2 доказательства этой леммы следует, что соответствующие формулы могут быть выбраны правильными.

Лемма доказана.

§ 4

Обозначим через P_{-}, $P_{\vee}$, $P_{\&}$ индексы простоты правильных формул, выражающих соответственно функции $\bar{x}$, $x \vee y$, $x \& y$. Существование таких формул доказано в лемме 1.

---

*) Для установления этого факта можно воспользоваться, например, представлением функции в виде полинома Жегалкина [11], т. е. суммы по mod 2 конъюнкций переменных (без отрицаний) и, быть может, единицы.

Пусть f и f_i, $1 \leqslant i \leqslant n$, — произвольные функции. Тогда в силу следствия из замечаний 2 и 3

$$L(\bar{f}) \leqslant P_- + L(f), \tag{4.1}$$

$$L(f_1 \vee \ldots \vee f_n) \leqslant (n-1) P_\vee + \sum_{i=1}^{n} L(f_i), \tag{4.2}$$

$$L(f_1 \,\&\, \ldots \,\&\, f_n) \leqslant (n-1) P_\& + \sum_{i=1}^{n} L(f_i). \tag{4.3}$$

Будем обозначать конъюнкцию *) $x_1^{\sigma_1} \ldots x_n^{\sigma_n}$ через $K_{\sigma_1, \ldots, \sigma_n}(x_1, \ldots, x_n)$. Из (4.1) и (4.3) следует, что для любой такой конъюнкции K

$$L(K) \leqslant nP_- + (n-1) P_\&. \tag{4.4}$$

Далее, пусть функция f от n переменных принимает значение 1 на k наборах. Из (4.2) и (4.4) следует, что

$$L(f) \leqslant (k-1) P_\vee + knP_- + k(n-1) P_\& \leqslant kn (P_\vee + P_- + P_\&). \tag{4.5}$$

Лемма 2. *Пусть функция* $f(x_1, \ldots, x_m, y_1, \ldots, y_n)$ *представима в виде* **)

$$\bigvee_{(\sigma_1, \ldots, \sigma_m)} K_{\sigma_1, \ldots, \sigma_m}(x_1, \ldots, x_m) \,\&\, F_{\sigma_1, \ldots, \sigma_m}(y_1, \ldots, y_n).$$

Тогда

$$L(f) \leqslant (2^m - 1)(2P_\& + P_\vee + P_-) + \sum_{(\sigma_1, \ldots, \sigma_m)} L(F_{\sigma_1, \ldots, \sigma_m}). \tag{4.6}$$

Доказательство будем проводить индукцией по m. Для $m = 0$ утверждение леммы верно. Допустим, что оно верно для $m_1 = m-1$. Имеем

$$f(x_1, \ldots, x_m, y_1, \ldots, y_n) =$$
$$= \bar{x}_m f(x_1, \ldots, x_{m-1}, 0, y_1, \ldots, y_n) \vee x_m f(x_1, \ldots, x_{m-1}, 1, y_1, \ldots, y_n). \tag{4.7}$$

По предположению индукции,

$$L(f(x_1, \ldots, x_{m-1}, \sigma, y_1, \ldots, y_n)) \leqslant$$
$$\leqslant (2^{m-1} - 1)(2P_\& + P_\vee + P_-) + \sum_{\substack{(\sigma_1, \ldots, \sigma_m) \\ \sigma_m = \sigma}} L(F_{\sigma_1, \ldots, \sigma_m}), \ \sigma = 0,1. \tag{4.8}$$

Соотношение (4.6) следует из (4.2), (4.3), (4.7), (4.8).

Лемма доказана.

§ 5

Пусть $\mathfrak{C}$ — некоторое множество наборов (из нулей и единиц) длины m и $\chi_\mathfrak{C}$ — его характеристическая функция (т. е. функция, принимающая значение 1 на всех наборах из $\mathfrak{C}$ и только на них).

Множество $\mathfrak{C}$ будем называть *ε-регулярным*, если для каждой функции f от m аргументов, принимающей значение 0 вне множества $\mathfrak{C}$, существует функция φ такая, что:

а) $\varphi\chi_\mathfrak{C} = f$ (т. е. на множестве $\mathfrak{C}$ функции φ и f совпадают; если $\mathfrak{C}$ — множество всех наборов, то $\varphi = f$);

б) $L(\varphi) \leqslant \varrho \frac{|\mathfrak{C}|}{\lg_2 m}(1+\varepsilon)$, где $|\mathfrak{C}|$ означает число наборов в $\mathfrak{C}$, а ϱ определено в § 1.

*) В некоторых случаях символ & будет опускаться.

**) Мы считаем, что конъюнкция связывает сильнее, чем дизъюнкция.

Заметим, что из результатов Р. Е. Кричевского [3] следует, что какова бы ни была последовательность множеств $\mathfrak{C}_1, \ldots, \mathfrak{C}_m, \ldots$ наборов длины $1, \ldots, m, \ldots$ такая, что $\frac{|\mathfrak{C}_m|}{\lg_2 m} \to \infty$, для почти всех указанных выше функций φ имеет место асимптотическое соотношение

$$L(\varphi) \gtrsim \varrho \frac{|\mathfrak{C}_m|}{\lg_2 m}.$$

Отсюда вытекает, что ε-регулярность множества означает возможность реализовать определенные на нем функции способом, близким к наилучшему.

Определение. Пусть $\mathfrak{N}_1^{(m_1)}, \ldots, \mathfrak{N}_n^{(m_n)}, \ldots$ есть последовательность множеств всех наборов длины соответственно $m_1, \ldots, m_n, \ldots$ Разбиение множеств этой последовательности на попарно не пересекающиеся подмножества

$$\mathfrak{N}_n^{(m_n)} = \mathfrak{M}_{n,1}^{(m_n)} \cup \ldots \cup \mathfrak{M}_{n,N_n}^{(m_n)}$$

будет называть *регулярным*, если

1) $$\lg_2 m_n \sim \lg_2 n; \quad m_n \leqslant \frac{n}{2}; \tag{5.1}$$

2) существуют такие k_n, что каждое из множеств $\mathfrak{M}_{n,i}^{(m_n)}$, $1 \leqslant i \leqslant k_n$, содержит одно и то же число M_n наборов и является ε_n-регулярным, причем

а) $$k_n \sim \frac{2^{m_n}}{M_n}, \tag{5.2}$$

б) $$\frac{M_n}{\lg_2 n} \to \infty, \tag{5.3}$$

в) $$\varepsilon_n \to 0, \tag{5.4}$$

г) число M наборов, содержащихся во всех множествах $\mathfrak{M}_{n,i}^{(m_n)}$, $i > k_n$, (в совокупности), удовлетворяет условию

$$M = o\left(\frac{2^{m_n}}{n \lg_2 n}\right). \tag{5.5}$$

Основная лемма 1. *Пусть для последовательности*

$$m_1, \ldots, m_n, \ldots$$

существует регулярное разбиение. Тогда

$$L_{\Phi}(n) \lesssim \varrho \frac{2^n}{\lg_2 n}.$$

Доказательство. Пусть $f(x_1, \ldots, x_n)$, где n достаточно велико, произвольная функция алгебры логики и $\chi_i(x_1, \ldots, x_{m_n})$ характеристическая функция множества $\mathfrak{M}_{n,i}^{(m_n)}$ регулярного разбиения (множество $\mathfrak{M}_{n,i}^{(m_n)}$ содержит наборы длины m_n). Разобьем аргументы функции f на две группы:

$\tilde{x}_1$ (включает аргументы $x_1, \ldots, x_{m_n}$),

$\tilde{x}_2$ (включает аргументы $x_{m_n+1}, \ldots, x_n$).

Рассмотрим функции

$$f_i(\tilde{x}_1, \tilde{x}_2) = \chi_i(\tilde{x}_1) f(\tilde{x}_1, \tilde{x}_2) \tag{5.6}$$

и

$$f_{i,\tilde{\sigma}}(\tilde{x}_1) = f_i(\tilde{x}_1, \tilde{\sigma}). \tag{5.7}$$

Очевидно, что

$$f = \bigvee_i f_i. \tag{5.8}$$

В силу ε_n-регулярности множества $\mathfrak{M}_{n,i}^{(m_n)}$, $i \leqslant k_n$, существуют функции $\varphi_{i,\widetilde{\sigma}}(\widetilde{x}_1)$, $i \leqslant k_n$, такие, что

$$f_{i,\widetilde{\sigma}}(\widetilde{x}_1) = \chi_i(\widetilde{x}_1)\,\varphi_{i,\widetilde{\sigma}}(\widetilde{x}_1) \tag{5.9}$$

и

$$L(\varphi_{i,\widetilde{\sigma}}) \leqslant \varrho(1+\varepsilon_n)\frac{M_n}{\lg_2 m_n}. \tag{5.10}$$

Из (5.6), (5.7), (5.8) и (5.9) следует

$$f_i(\widetilde{x}_1, \widetilde{x}_2) = \bigvee_{\widetilde{\sigma}} K_{\widetilde{\sigma}}(\widetilde{x}_2)\,\chi_i(\widetilde{x}_1)\varphi_{i,\widetilde{\sigma}}(\widetilde{x}_1) =$$

$$= \chi_i(\widetilde{x}_1)\Big(\bigvee_{\widetilde{\sigma}} K_{\widetilde{\sigma}}(\widetilde{x}_2)\,\varphi_{i,\widetilde{\sigma}}(\widetilde{x}_1)\Big),\ 1 \leqslant i \leqslant k_n. \tag{5.11}$$

Из (4.5) следует, что

$$L(\chi_i) \leqslant m_n M_n C, \tag{5.12}$$

где C — некоторая константа (определяемая индексами простоты $P_\vee$, $P_\&$, P_-).

Из (5.10), (5.11), (5.12) и леммы 2 вытекает, что при $i \leqslant k_n$

$$L(f_i) \leqslant P_\& + m_n M_n C + 2^{n-m_n}\left(2P_\& + P_\vee + P_- + \varrho(1+\varepsilon_n)\frac{M_n}{\lg_2 m_n}\right),$$

откуда в силу (5.1), (5.3), (5.4) и $\frac{m_n \lg_2 m_n}{2^{n-m_n}} \to 0$ (последнее следует из (5.1)) имеем

$$L(f_i) \leqslant \varrho\, 2^{n-m_n}\frac{M_n}{\lg_2 n}, \quad i \leqslant k_n. \tag{5.13}$$

Далее, пусть множество $\mathfrak{M}_{n,i}^{(m_n)}$, $i > k_n$, содержит $M_{(i)}$ наборов. Тогда, поскольку функция f_i принимает значение 1 не более, чем на $2^{n-m_n}M_{(i}$ наборах, в силу (4,5) *)

$$L(f_i) \leqslant M_{(i)}2^{n-m_n}nC, \quad i > k_n. \tag{5.14}$$

Очевидно, что число функций f_i не превосходит 2^{m_n}. Отсюда и из (5.8), (4.2), (5.13), (5.14), (5.1), (5.2), (5,5) следует

$$L(f) \leqslant \varrho 2^{n-m_n}\frac{k_n M_n}{\lg_2 n} + M\cdot 2^{n-m_n}nC + 2^{m_n}P_\vee \leqslant \varrho\frac{2^n}{\lg_2 n}\left(1 + M\frac{Cn\lg_2 n}{2^{m_n}}\right) \lesssim \varrho\frac{2^n}{\lg_2 n}.$$

Лемма доказана.

§ 6

Мы будем рассматривать наборы $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ из нулей и единиц; α_i будем называть *значением* i-го разряда. *Расстоянием* между двумя наборами $\widetilde{\alpha}$ и $\widetilde{\beta}$ будем называть число разрядов, в которых эти наборы различаются; это число будем обозначать $\varrho(\widetilde{\alpha}, \widetilde{\beta})$. Множество наборов $\widetilde{\alpha}$ таких, что $\varrho(\widetilde{\alpha}, \widetilde{\alpha}_0) = 1$, будем называть (единичной) *сферой* с центром $\widetilde{\alpha}_0$

*) Если $f_i \equiv 0$, то $f_i = x_1 \& \bar{x}_1$ и $L(f_i) \leqslant P_\& + P_-$. Очевидно, что можно подобрать константу C таким образом, чтобы (5. 14) было справедливо и для функций, тождественно равных нулю.

и обозначать $\widetilde{S}(\alpha_0)$. Объединение сферы и ее центра будем называть *шаром*; центр шара есть центр сферы.

Пусть $\chi(x_1, \ldots, x_n)$ — характеристическая функция сферы с центром $(\alpha_1, \ldots, \alpha_n)$. Тогда

$$\chi(x_1, \ldots, x_n) x_i^{\overline{\alpha}_i} = x_1^{\alpha_1} \ldots x_{i-1}^{\alpha_{i-1}} x_i^{\overline{\alpha}_i} x_{i+1}^{\alpha_{i+1}} \ldots x_n^{\alpha_n}.$$

Это свойство сферы будет существенно использоваться в дальнейшем (§ 8).

Будем рассматривать наборы длины $n_m = 2^m - 1$. Разряду с номером i, $1 \leqslant i \leqslant n_m$, сопоставим набор $\widetilde{\delta} = (\delta_1, \ldots, \delta_m)$ длины m из нулей и единиц, являющийся двоичной записью числа i, так что набор $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_{n_m})$ может быть записан в виде

$$(\alpha_{(0, \ldots, 0, 1)}, \ \alpha_{(0, \ldots, 1, 0)}, \ \ldots, \ \alpha_{(1, \ldots, 1, 1)}).$$

Разряды, занумерованные наборами $\widetilde{\delta}$ с одной единицей (m штук), будем называть *выделенными*, остальные — *невыделенными* ($2^m - m - 1$ штук).

Таблица 1

	1*	2*	3	4*	5	6	7
δ_3	1	0	1	0	1	0	1
δ_2	0	1	1	0	0	1	1
δ_1	0	0	0	1	1	1	1
	0	0	0	0	0	0	0
	1	1	0	1	0	0	1
	0	1	0	1	0	1	0
	1	0	0	0	0	1	1
	1	0	0	1	1	0	0
	0	1	0	0	1	0	1
	1	1	0	0	1	1	0
	0	0	0	1	1	1	1
	1	1	1	0	0	0	0
	0	0	1	1	0	0	1
	1	0	1	1	0	1	0
	0	1	1	0	0	1	1
	0	1	1	1	1	0	0
	1	0	1	0	1	0	1
	0	0	1	0	1	1	0
	1	1	1	1	1	1	1

Определим теперь следующее множество $\mathfrak{M}_m$ наборов длины n_m (кодовое множество Хэмминга [7]). Значения невыделенных разрядов этих наборов произвольны; значение выделенного разряда $\alpha_{(0, \ldots, 0, 1_i, 0, \ldots, 1)}$ (т. е. разряда, которому соответствует набор с единственной единицей на i-м месте) равно сумме по mod 2 значений невыделенных разрядов, у которых $\delta_i = 1$. Другими словами, набор $\widetilde{\alpha}$ принадлежит множеству $\mathfrak{M}_m$ тогда и только тогда, когда выполнены условия *)

$$\dot{\sum_{\substack{\delta_1, \ldots, \delta_{i-1}, \delta_{i+1}, \ldots, \delta_m \\ \delta_i = 1}}} \alpha_{(\delta_1, \ldots, \delta_m)} = 0 \qquad (6.1)$$

$$(1 \leqslant i \leqslant m).$$

Заметим еще, что множество $\mathfrak{M}_m$ содержит набор, состоящий из одних нулей.

На табл. 1 приводится множество $\mathfrak{M}_3$. В верхней части таблицы выписаны номера разрядов (числа и наборы $\widetilde{\delta} = (\delta_1, \delta_2, \delta_3)$, записанные в виде столбцов); номера выделенных разрядов помечены звездочками.

Пусть теперь $n = qs$ и разряды набора $\widetilde{\alpha}$ длины n разбиты на q групп (одинаковой длины) и занумерованы следующим образом:

$$\widetilde{\alpha} = (\alpha_{11}, \ldots, \alpha_{1s}, \alpha_{21}, \ldots \ldots \alpha_{qs}).$$

Определим оператор A_s следующим образом:

$$A_s \widetilde{\alpha} = (\alpha_1^{(s)}, \ \ldots, \ \alpha_q^{(s)}), \text{ где } \alpha_i^{(s)} = \dot{\sum_{j=1}^{s}} \alpha_{ij} \qquad (1 \leqslant i \leqslant q).$$

Обозначим $\varrho(A_s \widetilde{\alpha}, A_s \widetilde{\beta})$ через $\varrho_s(\widetilde{\alpha}, \widetilde{\beta})$.

*) Здесь и в дальнейшем знаки $\dot{+}$ и $\dot{\Sigma}$ означают сложение по mod 2.

Введем оператор B_t, отбрасывающий первые t разрядов набора, т. е.

$$B_t(\alpha_1, \ldots, \alpha_t, \alpha_{t+1}, \ldots, \alpha_n) = (\alpha_{t+1}, \ldots, \alpha_n).$$

Лемма 3. *Если* $\tilde{\alpha} \in \mathfrak{M}_m$, *то*

$$\tilde{\beta} = A_{2^k} B_{2^k-1} \tilde{\alpha} \in \mathfrak{M}_{m-k}.$$

Доказательство. Очевидно, что длина набора $\tilde{\beta}$ равна

$$\frac{(2^m-1)-(2^k-1)}{2^k} = 2^{m-k} - 1.$$

Далее, из определения набора $\tilde{\beta}$ следует, что

$$\beta_{(\delta_1, \ldots, \delta_{m-k})} = \dot{\sum_{\varepsilon_1, \ldots, \varepsilon_k}} (B_{2^k-1}\tilde{\alpha})_{(\delta_1, \ldots, \delta_{m-k}, \varepsilon_1, \ldots, \varepsilon_k)}. \tag{6.2}$$

Поскольку для всех отбрасываемых оператором B_{2^k-1} разрядов $\delta_i = 0$ $(1 \leqslant i \leqslant m-k)$, то из (6.2) следует:

$$\dot{\sum_{\substack{\delta_1, \ldots, \delta_{i-1}, \delta_{i+1}, \ldots, \delta_{m-k} \\ \delta_i = 1}}} \beta_{(\delta_1, \ldots, \delta_{m-k})} =$$

$$= \dot{\sum_{\substack{\delta_1, \ldots, \delta_{i-1}, \delta_{i+1}, \ldots, \delta_{m-k} \\ \delta_i = 1}}} \ \dot{\sum_{\varepsilon_1, \ldots, \varepsilon_k}} \alpha_{(\delta_1, \ldots, \delta_{m-k}, \varepsilon_1, \ldots, \varepsilon_k)},$$

т. е. что условие (6.1) для наборов $\tilde{\beta}$ выполнено.

Лемма доказана.

Лемма 4 (Теорема Хэмминга)*). *Если* $\tilde{\alpha}$ *и* $\tilde{\beta}$ — *два различных набора из множества* $\mathfrak{M}_m$, *то* $\varrho(\tilde{\alpha}, \tilde{\beta}) \geqslant 3$

Доказательство. Пусть $\varrho^*(\tilde{\alpha}, \tilde{\beta})$ (соответственно $\varrho'(\tilde{\alpha}, \tilde{\beta})$) есть число выделенных (соответственно невыделенных) разрядов, в которых различаются наборы $\tilde{\alpha}$ и $\tilde{\beta}$. Ясно, что $\varrho(\tilde{\alpha}, \tilde{\beta}) = \varrho^*(\tilde{\alpha}, \tilde{\beta}) + \varrho'(\tilde{\alpha}, \tilde{\beta})$.

Рассмотрим теперь два произвольных различных набора $\tilde{\alpha}$ и $\tilde{\beta}$. В силу определения множества $\mathfrak{M}_m$ в этом случае $\varrho'(\tilde{\alpha}, \tilde{\beta}) \neq 0$.

Если $\varrho'(\tilde{\alpha}, \tilde{\beta}) = 1$, то поскольку номеру (невыделенного) разряда, в котором различаются $\tilde{\alpha}$ и $\tilde{\beta}$ соответствует набор $\tilde{\delta}$ по крайней мере с двумя единицами, то $\varrho^*(\tilde{\alpha}, \tilde{\beta}) \geqslant 2$ и $\varrho(\tilde{\alpha}, \tilde{\beta}) \geqslant 3$.

Если $\varrho'(\tilde{\alpha}, \tilde{\beta}) = 2$, то наборы $\tilde{\delta}_1$ и $\tilde{\delta}_2$, соответствующие тем разрядам, в которых различаются наборы $\tilde{\alpha}$ и $\tilde{\beta}$, различаются в некотором i-м разряде, и, следовательно, $\tilde{\alpha}$ и $\tilde{\beta}$ различаются также в разряде с номером $(0, \ldots, 0, 1_i, 0, \ldots, 0)$, т. е. $\varrho^*(\tilde{\alpha}, \tilde{\beta}) \geqslant 1$ и $\varrho(\tilde{\alpha}, \tilde{\beta}) \geqslant 3$.

Если же $\varrho'(\tilde{\alpha}, \tilde{\beta}) \geqslant 3$, то и $\varrho(\tilde{\alpha}, \tilde{\beta}) \geqslant 3$.

Лемма доказана.

Лемма 5. *Если* $n = 2^m$, *то существует такое разбиение множества всех наборов длины* n *на попарно не пересекающиеся сферы с центрами* $\tilde{\alpha}'_i$, *что для любого* λ

$$\varrho_{2\lambda}(\tilde{\alpha}'_i, \tilde{\alpha}'_j) \neq 2,$$

причем в разбиение входит сфера с центром $(0, \ldots, 0)$.

---

*) По существу, доказательство этого утверждения содержится в уже упомянутой работе Хэмминга [7].

Доказательство. Определим множество $\mathfrak{M}'_m$ наборов длины 2^m следующим образом: набор $\widetilde{\alpha}'=(\alpha_0, \alpha_1, \ldots, \alpha_{2^m-1})$ принадлежит множеству $\mathfrak{M}'_m$ тогда и только тогда, когда $\widetilde{\alpha}=B_1\widetilde{\alpha}'\in\mathfrak{M}_m$. Покажем, что сферы с центрами $\widetilde{\alpha}'$ из $\mathfrak{M}'_m$ обладают требуемыми свойствами.

Во-первых, эти сферы попарно не пересекаются. В самом деле, пусть $\widetilde{\alpha}'$ и $\widetilde{\beta}'$ $(\widetilde{\alpha}'\neq\widetilde{\beta}')$ центры двух сфер. Если $\widetilde{\alpha}\neq\widetilde{\beta}$, то на основании леммы 4, $\varrho(\widetilde{\alpha}, \widetilde{\beta})\geqslant 3$, поэтому $\varrho(\widetilde{\alpha}', \widetilde{\beta}')\geqslant 3$ и шары с центрами $\widetilde{\alpha}'$ и $\widetilde{\beta}'$ не пересекаются. Если $\widetilde{\alpha}=\widetilde{\beta}$, то $\alpha_0\neq\beta_0$. Сфера $S(\widetilde{\alpha}')$ состоит из наборов

$$(\beta_0, \alpha_1, \ldots, \alpha_{2^m-1}),\ (\alpha_0, \bar{\alpha}_1, \alpha_2, \ldots, \alpha_{2^m-1}),\ \ldots,\ (\alpha_0, \alpha_1, \ldots, \alpha_{2^m-2}, \bar{\alpha}_{2^m-1}).$$

Сфера $S(\widetilde{\beta}')$ состоит из наборов

$$(\alpha_0, \alpha_1, \ldots, \alpha_{2^m-1}),\ (\beta_0, \bar{\alpha}_1, \alpha_2, \ldots, \alpha_{2^m-1}),\ \ldots,\ (\beta_0, \alpha_1, \ldots, \alpha_{2^m-2}, \bar{\alpha}_{2^m-1}).$$

Отсюда видно, что эти сферы не пересекаются.

Далее, сферы содержат все наборы, так как они попарно не пересекаются, каждая из них содержит 2^m наборов и всего сфер $2\cdot 2^{2^m-m-1}$

Наконец, по определению множества $\mathfrak{M}'_m$, если $\widetilde{\alpha}'\in\mathfrak{M}'_m$, то $B_1\widetilde{\alpha}'\in\mathfrak{M}_m$. На основании леммы 3

$$A_{2\lambda}B_{2\lambda}\widetilde{\alpha}'=A_{2\lambda}B_{2\lambda-1}B_1\widetilde{\alpha}'\in\mathfrak{M}_{m-\lambda}.$$

Поэтому, если $\widetilde{\alpha}', \widetilde{\beta}'\in\mathfrak{M}'_m$, то $\varrho_{2\lambda}(B_{2\lambda}\widetilde{\alpha}', B_{2\lambda}\widetilde{\beta}')$ либо равно 0, либо не менее 3. Далее, так как

$$\varrho_{2\lambda}(B_{2\lambda}\widetilde{\alpha}', B_{2\lambda}\widetilde{\beta}')\leqslant\varrho_{2\lambda}(\widetilde{\alpha}', \widetilde{\beta}')\leqslant\varrho_{2\lambda}(B_{2\lambda}\widetilde{\alpha}', B_{2\lambda}\widetilde{\beta}')+1,$$

то

$$\varrho_{2\lambda}(\widetilde{\alpha}', \widetilde{\beta}')\neq 2.$$

Последнее утверждение леммы выполнено в силу того, что $(0, \ldots, 0)\in\mathfrak{M}_m$.

Лемма доказана.

§ 7

Пусть теперь $\varphi(x_1, \ldots, x_{m_0})$ есть функция базиса, существенно зависящая по крайней мере от двух переменных, для которой достигается минимум выражения $\frac{L(\varphi_i(x_1, \ldots, x_{k_i}))}{k_i-1}$. Этот минимум был обозначен через ϱ.

Пусть k — некоторое натуральное число и k' — максимальное натуральное число такое, что

$$k'\leqslant\frac{k-1}{m_0-1}. \tag{7.1}$$

Тогда

$$k-[(m_0-1)k'+1]\leqslant m_0-2. \tag{7.2}$$

Введем обозначение

$$\widetilde{\psi}_k(y_1, \ldots, y_{(m_0-1)k'+1})=\varphi(\varphi(\ldots\varphi(\varphi(y_1, \ldots, y_{m_0}), y_{m_0+1}, \ldots, y_{2m_0-1}), \ldots)).$$

Пусть, далее,

$$\psi_k(y_1, \ldots, y_k) = \widetilde{\psi}_k(y_1, \ldots, y_{(m_0-1)k'}, y_{(m_0-1)k'+1} \vee \ldots \vee y_k)$$

(т. е. последний аргумент функции $\widetilde{\psi}_k$ замещается дизъюнкцией). Тогда, используя (7.1) и (7.2), получаем

$$L(\psi_k) \leqslant L(\widetilde{\psi}_k) + (m_0 - 2) P_\vee = k' L(\varphi) + (m_0 - 2) P_\vee \leqslant$$
$$\leqslant (k-1)\varrho + (m_0 - 2) P_\vee \leqslant \varrho k (1 + \widetilde{R}_k), \tag{7.3}$$

где

$$\widetilde{R}_k \leqslant \frac{(m_0 - 2) P_\vee}{k\varrho}.$$

Очевидно, что функция $\psi_k(y_1, \ldots, y_k)$ существенно зависит от всех своих аргументов. Поэтому существуют константы α_{ij}, $1 \leqslant i, j \leqslant k$ такие, что для любого i, $1 \leqslant i \leqslant k$, имеет место равенство *)

$$\psi_k(\alpha_{i1}, \ldots, \alpha_{i,i-1}, y_i, \alpha_{i,i+1}, \ldots, \alpha_{i,k}) = y_i + \alpha_{ii}. \tag{7.4}$$

Опишем теперь некоторое разбиение всех наборов длины n из нулей и единиц на подмножества, удовлетворяющие определенным условиям.

Будем рассматривать матрицы, имеющие n столбцов, элементами которых являются нули и единицы. Каждой матрице будем ставить в соответствие множество наборов, образующих ее строки.

Множество матриц будем называть *полным*, если каждый набор длины n является строкой некоторой матрицы множества, и *простым*, если все строки в совокупности матриц попарно различны.

Очевидно, что если множество матриц является полным и простым, то оно определяет разбиение множества всех наборов длины n на попарно непересекающиеся подмножества.

Введем следующие обозначения. Пусть M—матрица. Тогда $(M)_\alpha$ (соответственно $(M)^\alpha$) есть строка (соответственно столбец) с номером α матрицы M.

Пусть $k = 2^\varkappa$ и $A = \|\alpha_{ij}\|$ — квадратная матрица (порядка k), элементы которой—константы α_{ij}, соответствующие функции ψ_k. Определим матрицу A^* порядка kl, где $l = 2^\lambda$, $\lambda \geqslant 1$. Матрица A^* имеет строение

$$A^* = \left\| \begin{matrix} B_{11} & \ldots & B_{1k} \\ \cdot & \cdot & \cdot \\ B_{k1} & \ldots & B_{kk} \end{matrix} \right\|.$$

Все блоки B_{ij} суть квадратные матрицы порядка l; все элементы блока B_{ij} равны α_{ij}.

Пусть наборы $\widetilde{\gamma}_p \left(0 \leqslant p \leqslant N - 1,\ N = \frac{2^{kl}}{kl}\right)$ длины $kl = 2^{\varkappa+\lambda}$ являются центрами сфер, удовлетворяющих условиям леммы 5, причем $\gamma_0 = (0, \ldots, 0)$. Обозначим через C_p^* квадратную матрицу порядка kl, каждая строка которой есть $\widetilde{\gamma}_p$. Рассмотрим множество $\mathfrak{C}$ матриц C_p **)

$$C_p = C_p^* \dotplus E,$$

где

$$E = \left\| \begin{matrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 \end{matrix} \right\|.$$

---

*) То есть путем соответствующей подстановки констант эта функция превращается в функцию, существенно зависящую от любого одного аргумента.

**) Символ $\dotplus$ означает здесь поэлементное сложение по mod 2.

(единичная матрица). Множество $\mathfrak{C}$ определяет разбиение множества всех наборов на сферы, удовлетворяющие лемме 5.

Определим множество $\mathfrak{D}$ матриц D_p:

$$D_p = C_p \dot{+} A^* \qquad (0 \leqslant p \leqslant N-1).$$

Множество $\mathfrak{D}$ содержит $\frac{2^{kl}}{kl}$ матриц.

Пример. $k=2,\ l=2$.

$$A = \left\| \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix} \right\|, \qquad A^* = \left\| \begin{matrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix} \right\|,$$

$$C_0 = \left\| \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\|, \quad C_1 = \left\| \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \right\|, \quad C_2 = \left\| \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{matrix} \right\|, \quad C_3 = \left\| \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix} \right\|,$$

$$D_0 = \left\| \begin{matrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{matrix} \right\|, \quad D_1 = \left\| \begin{matrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{matrix} \right\|, \quad D_2 = \left\| \begin{matrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \right\|, \quad D_3 = \left\| \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\|.$$

Замечание 1. Так как каждый столбец матриц C_p^* состоит либо сплошь из нулей, либо сплошь из единиц, то в любой матрице D, $D \in \mathfrak{D}$, i-й столбец матрицы D либо совпадает с i-м столбцом матрицы D_0, либо является дополнением к нему, т. е. на соответствующем месте имеет противоположное значение.

Определим теперь множество $\mathfrak{E}$ матриц

$$E_{D, \widetilde{\zeta}}\ (D \in \mathfrak{D},\ \widetilde{\zeta} = (\zeta_{11}, \ldots, \zeta_{1, t-1}, \zeta_{2, 1}, \ldots, \zeta_{kl, t-1})),$$

имеющих каждая kl строк и klt столбцов. Пусть столбцы матрицы занумерованы парами чисел

$$(1, 0), (1, 1), \ldots, (1, t-1), (2, 0), \ldots, (kl, t-1).$$

Матрица $E_{D, \widetilde{\zeta}}$ определяется следующим образом:

$$\left. \begin{aligned} &(E_{D, \widetilde{\zeta}})^{(i, 0)} = (D)^i \qquad (1 \leqslant i \leqslant kl), \\ &(E_{D, \widetilde{\zeta}})^{(i, j)} = (D)^i \dot{+} \left\| \begin{matrix} \zeta_{i,j} \\ \vdots \\ \zeta_{i,j} \end{matrix} \right\| \qquad (1 \leqslant i \leqslant kl,\ 1 \leqslant j \leqslant t-1). \end{aligned} \right\} \tag{7.5}$$

Множество $\mathfrak{E}$ содержит $\frac{2^{kl}}{kl} \cdot 2^{(t-1)\,kl} = \frac{2^{klt}}{kl}$ матриц.

Пример. Пусть $t=2$, $D=D_2$ (см. предыдущий пример), $\zeta=(0, 1, 1, 0)$. Тогда

$$E = E_{D, \widetilde{\zeta}} = \left\| \begin{matrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{matrix} \right\|.$$

Рассмотрим теперь множество $\mathfrak{F}$ матриц $F_1, \ldots, F_h$, определенных следующим образом. F_1 — матрица, строками которой являются всевозможные (различные) наборы длины $\varkappa$ (она имеет $k=2^{\varkappa}$ строк); матрица F_{i+1} получается из матрицы F_i путем циклической перестановки строк.

Определим матрицы F_i^* $(1 \leqslant i \leqslant k)$. Матрица F_i^* имеет блочное строение

$$F_i^* = \left\| \begin{matrix} G_{i1} \\ \cdot \\ \cdot \\ \cdot \\ G_{ik} \end{matrix} \right\|.$$

Блок G_{ij} имеет l строк, каждая из которых совпадает с j-й строкой матрицы F_i.

Замечание 2. Для каждого набора $\widetilde{\sigma}=(\sigma_1, \ldots, \sigma_\varkappa)$ и каждого r, $1 \leqslant r \leqslant kl$, можно указать матрицу F_i^* такую, что $(F_i^*)_{(r)}=\widetilde{\sigma}$.

Определим, наконец, множество $\mathfrak{H}$ матриц $H_{E,F}$, имеющих kl строк и $klt+\varkappa$ столбцов: $H_{E,F}=\|H, F^*\|$, где $E \in \mathfrak{E}$, $F \in \mathfrak{F}$, F^* порождена матрицей F; т. е. первые klt столбцов образуют матрицу E, последние $\varkappa$ столбцов — матрицу F^*. Множество $\mathfrak{H}$ содержит $\frac{2^{klt}}{kl}k=\frac{2^{klt+\varkappa}}{kl}$ матриц.

Пример. Для матрицы E, построенной в предыдущем примере, и

$$F=\left\| \begin{matrix} 0 \\ 1 \end{matrix} \right\|,$$

имеем

$$H_{E,F}=\left\| \begin{matrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{matrix} \right\|.$$

Матрицу H будем называть *хорошей*, если для любого столбца матрицы D_0 существует совпадающий с ним столбец матрицы H.

Пусть $\widetilde{\beta}_1, \ldots, \widetilde{\beta}_p$ суть строки некоторых матриц. Если их номера (в матрицах, которым они принадлежат) $i_1, \ldots, i_p$ удовлетворяют условию

$$(q-1)\,l < i_j \leqslant ql \qquad (1 \leqslant j \leqslant p),$$

то будем говорить, что эти строки *принадлежат q-й полосе*.

Лемма 6. 1) *Множество $\mathfrak{H}$ определяет разбиение множества всех наборов длины $klt+\varkappa$ на попарно не пересекающиеся подмножества.*

2) *Доля хороших матриц в множестве $\mathfrak{H}$ (т. е. отношение числа хороших матриц к числу всех матриц) не менее* $\left(1-\frac{1}{2^{t-1}}\right)^{kl}$.

Доказательство. 1) Для доказательства пункта 1 достаточно показать, что множество $\mathfrak{H}$ является полным и простым. На основании леммы 5 этими свойствами обладает множество $\mathfrak{C}$. Ниже будет показано, что эти свойства сохраняются при переходе а) от $\mathfrak{C}$ к $\mathfrak{D}$, б) от $\mathfrak{D}$ к $\mathfrak{E}$, в) от $\mathfrak{E}$ к $\mathfrak{H}$.

а) Докажем сначала простоту $\mathfrak{D}$. Обозначим через $\widetilde{\eta}_j$ набор длины kl, имеющий 1 на j-м месте и 0 на всех остальных местах. Покажем, что если $(i_1, j_1) \neq (i_2, j_2)$, то $(D_{i_1})_{j_1} \neq (D_{i_2})_{j_2}$.

Если j_1-я и j_2-я строки принадлежат одной полосе, то $(A^*)_{j_1}=(A^*)_{j_2}$, и, поскольку $(C_{i_1})_{j_1} \neq (C_{i_2})_{j_2}$ (в силу простоты $\mathfrak{C}$), то $(D_{i_1})_{j_1} \neq (D_{i_2})_{j_2}$.

Пусть теперь j_1-я и j_2-я строки не принадлежат одной полосе. Тогда

$$\varrho_l(\widetilde{\eta}_{j_1}, \widetilde{\eta}_{j_2}) = 2. \tag{7.6}$$

Кроме того, поскольку в результате применения к $(A^*)_j$ оператора A_l получается набор $(0, \ldots, 0)$, то

$$\varrho_l((A^*)_{j_1}, (A^*)_{j_2}) = 0. \tag{7.7}$$

Но

$$(D_i)_j = \widetilde{\alpha}'_i \dotplus \widetilde{\eta}_j \dotplus (A^*)_j, \tag{7.8}$$

где $\widetilde{\alpha}'_i$ — центр сферы, определяемой матрицей C_i. Поэтому, если бы при рассматриваемых j_1 и j_2 было $(D_{i_1})_{j_1} = (D_{i_2})_{j_2}$, то $\varrho_l((D_{i_1})_{j_1}, (D_{i_2})_{j_2}) = 0$ и, в силу (7.6), (7.7) и (7.8) $\varrho_l(\widetilde{\alpha}'_{i_1}, \widetilde{\alpha}'_{i_2}) = 2$, что противоречит лемме 5.

Полнота системы $\mathfrak{D}$ матриц следует из ее простоты и того, что каждая матрица содержит kl строк и в $\mathfrak{D}$ имеется $\frac{2^{kl}}{kl}$ матриц.

б) Установим сначала полноту $\mathfrak{E}$. Пусть

$$\widetilde{\sigma} = (\sigma_{10}, \sigma_{11}, \ldots, \sigma_{1, t-1}, \sigma_{20}, \ldots, \sigma_{kl, t-1})$$

— произвольный набор длины klt. Так как множество $\mathfrak{D}$ полно, то набор $(\sigma_{10}, \sigma_{20}, \ldots, \sigma_{kl, 0})$ является строкой некоторой матрицы D. Поэтому $\widetilde{\sigma}$ является строкой матрицы $E_{D, \widetilde{\zeta}'}$, где $\zeta'_{ij} = \sigma_{i0} \dotplus \sigma_{ij}$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant t-1)$.

Простота $\mathfrak{E}$ следует из полноты и из того, что число матриц в $\mathfrak{D}$ равно $\frac{2^{klt}}{kl}$, а каждая матрица имеет kl строк.

в) Полнота множества $\mathfrak{H}$ следует из полноты $\mathfrak{E}$ и замечания 2. Простота — из полноты и того, что число матриц в $\mathfrak{H}$ равно $\frac{2^{klt+\varkappa}}{kl}$, а число строк в каждой из них равно kl.

2) Из замечания 1 и (7.5) следует, что столбец с номером (i, j), $1 \leqslant j \leqslant t-1$ либо совпадает с i-м столбцом матрицы D_0, либо является дополнением к нему. Поэтому для каждого i доля матриц E из $\mathfrak{E}$, у которых хотя бы один столбец с номером (i, j) совпадает с $(D_0)^i$ не менее $1 - \frac{1}{2^{t-1}}$, а доля всех хороших матриц в $\mathfrak{E}$ не менее $\left(1 - \frac{1}{2^{t-1}}\right)^{kl}$. Очевидно, что доля хороших матриц в $\mathfrak{H}$ не может быть меньше, чем в $\mathfrak{E}$.

Лемма доказана.

§ 8

Рассмотрим функцию

$$\psi_{kq}(y_{11}, \ldots, y_{kq}) = \psi_k(y_{11}, \ldots, y_{k1}) \vee \ldots \vee \psi_k(y_{1q}, \ldots, y_{kq})$$

(все переменные y_{ip}, $1 \leqslant i \leqslant k$, $1 \leqslant p \leqslant q$ попарно различны). На основании (4.2) и (7.3)

$$L(\psi_{kq}) \leqslant qP_{\vee} + \varrho kq(1 + \widetilde{R}_k) \leqslant \varrho kq(1 + R_k), \tag{8.1}$$

где

$$R_k \leqslant \frac{(m_0 - 1)P_{\vee}}{\varrho k}.$$

Из (7.4) следует

$$\psi_{kq}(\alpha_{i1}, \ldots, \alpha_{i,i-1}, y_{i1}, \alpha_{i,i+1}, \ldots, \alpha_{ik}, \alpha_{i1}, \ldots, \alpha_{i,i-1}, y_{i2}, \alpha_{i,i+1}, \ldots, \alpha_{ik}, \alpha_{i1}, \ldots, \alpha_{ik}) =$$

$$= (y_{i1} \dotplus \alpha_{ii}) \vee (y_{i2} \dotplus \alpha_{ii}) \vee \ldots \vee (y_{ik} \dotplus \alpha_{ii}) \qquad (1 \leqslant i \leqslant k) \quad (8.2)$$

(в функции ψ_{kq} аргументы y_{hp} при $h \neq i$ замещаются константой α_{ip} и при $h = i$ ничем не замещаются).

Лемма 7. *Пусть $\chi(x_1, \ldots, x_{klt+\varkappa})$ — характеристическая функция хорошей матрицы H из $\mathfrak{H}$ и*

$$B = \{\widetilde{\beta}_{11}, \widetilde{\beta}_{12}, \ldots, \widetilde{\beta}_{1q_1}, \ldots, \widetilde{\beta}_{k1}, \ldots, \widetilde{\beta}_{kq_k}\},$$

где $q_i \leqslant q$, — подмножество строк этой матрицы, причем $\widetilde{\beta}_{ir}$ принадлежит i-й полосе матрицы H. Тогда существуют

а) *расстановка некоторых из аргументов $x_1, \ldots, x_{klt+\varkappa}$ в функцию ψ_{kq} (вместо $y_{i,p}$ подставляется $x_{\nu(i,p)}$);*

б) *конъюнкции $K^{(i)}(x_{klt+1}, \ldots, x_{klt+\varkappa})$ такие, что*

$$\chi(x_1, \ldots, x_{klt+\varkappa})\, \psi_{kq}(x_{\nu(1,1)}, \ldots, x_{\nu(k,q)})\, K^{(i)}(x_{klt+1}, \ldots, x_{klt+\varkappa})$$

есть характеристическая функция множества $\{\widetilde{\beta}_{i1}, \ldots, \widetilde{\beta}_{iq_i}\}$, $1 \leqslant i \leqslant k$.

Доказательство. 1. Покажем сначала, что функция

$$\chi(x_1, \ldots, x_{klt+\varkappa})\, \psi_{kq}(x_{\nu(1,1)}, \ldots, x_{\nu(k,q)})$$

является характеристической функцией множества B.

Будем нумеровать строки матрицы H парами чисел (a, b), где a — номер полосы, которой принадлежит набор, и b — номер набора в этой полосе, называя также пары «номерами» (в кавычках), так что обычный номер строки с «номером» (a, b) есть $(a-1)l + b$.

Пусть целочисленная функция $\theta_i(r)$ такова, что при $1 \leqslant r \leqslant q_i$ пара $(i, \theta_i(r))$ есть «номер» набора $\widetilde{\beta}_{i,r}$ и $\theta_i(r) = \theta_i(1)$ при $r > q_i$.

В силу того, что матрица H — хорошая, для каждого ξ, $1 \leqslant \xi \leqslant kl$, можно указать столбец матрицы H, совпадающий с ξ-м столбцом матрицы D_0. Обозначим номер этого столбца (в матрице H) через $\pi(\xi)$.

Покажем, что функцию $\nu(g, h)$, определяющую расстановку аргументов, можно определить так

$$\nu(g, h) = \pi((g-1)l + \theta_g(h)), \quad 1 \leqslant g \leqslant k, \quad 1 \leqslant h \leqslant q. \qquad (8.3)$$

В самом деле, пусть набор $\widetilde{\beta}$ есть произвольная строка матрицы H и (a, b) — ее «номер». Тогда в силу (8.3)

$$\beta_{\nu(g,h)} = \delta_{(a-1)l+b,\ (g-1)l+\theta_g(h)},$$

где $\delta_{u,v}$ означает элемент матрицы D_0, стоящий в u-й строке и v-м столбце. Отсюда и из определения матрицы D_0 следует, что

$$\left.\begin{array}{l} \beta_{\nu(g,h)} = \alpha_{a,g}, \text{ если } g \neq a \qquad (1 \leqslant h \leqslant q), \\ \text{а} \\ \beta_{\nu(a,h)} = \delta_{(a-1)l+b,\ (a-1)l+\theta_a(h)} = \alpha_{a,a} \dotplus \varepsilon_{a,b,h}, \\ \text{где} \\ \varepsilon_{a,b,h} = \begin{cases} 1, & \text{если } \theta_a(h) = b, \\ 0, & \text{если } \theta_a(h) \neq b. \end{cases} \end{array}\right\} \qquad (8.4)$$

Далее, из (8.2) и (8.4) для набора $\widetilde{\beta}$ имеем

$$\psi_{kq}(\beta_{\nu(1,1)}, \ldots, \beta_{\nu(k,q)}) =$$
$$= \psi_{kq}(\alpha_{a1}, \alpha_{a2}, \ldots, \alpha_{a,a-1}, \alpha_{a,a} \dotplus \varepsilon_{a,b,1}, \alpha_{a,a+1}, \ldots, \alpha_{a,k},$$
$$\alpha_{a1}, \alpha_{a2}, \ldots, \alpha_{a,a-1}, \alpha_{a,a} + \varepsilon_{a,b,2}, \alpha_{a,a+1}, \ldots, \alpha_{a,k},$$
$$\alpha_{a1}, \alpha_{a2}, \ldots, \alpha_{a,a-1}, \alpha_{a,a} \dotplus \varepsilon_{a,b,q}, \alpha_{a,a+1}, \ldots, \alpha_{a,k}) =$$
$$= \varepsilon_{a,b,1} \vee \varepsilon_{a,b,2} \vee \ldots \vee \varepsilon_{a,b,q}.$$

Далее,

а) если $\widetilde{\beta} \in B$, то для некоторого c, $1 \leqslant c \leqslant q_a$, $b = \theta_a(c)$; поэтому $\varepsilon_{a,b,c} = 1$ и $\psi_{kq}(\beta_{\nu(1,1)}, \ldots, \beta_{\nu(k,q)}) = 1$;

б) если же $\widetilde{\beta} \,\overline{\in}\, B$, то для любого c, $1 \leqslant c \leqslant q$, имеет место $\theta_a(c) \neq b$ и поэтому $\varepsilon_{a,b,c} = 0$ при $1 \leqslant c \leqslant q$ и $\psi_{kq}(\beta_{\nu(1,1)}, \ldots, \beta_{\nu(k,q)}) = 0$. Так как на рассматриваемых наборах $\widetilde{\beta}$ функция χ обращается в единицу, то утверждение 1 доказано.

2. Покажем теперь, что можно подобрать надлежащим образом конъюнкции $K^{(i)}(x_{klt+1}, \ldots, x_{klt+\varkappa})$.

Пусть матрица H получена из матрицы F. Определим $K^{(i)}$ следующим образом: $K^{(i)}$ равна 1 на i-й строке матрицы F и равна 0 на всех остальных наборах (длины $\varkappa$). Тогда, если $\widetilde{\beta}$ принадлежит j-й полосе, то $K^{(i)}$ равна 1 на наборе $\widetilde{\beta}$ тогда и только тогда, когда $i = j$, и, следовательно,

$$\chi(x_1, \ldots, x_{klt+\varkappa})\, \psi_{kq}(x_{\nu(1,1)}, \ldots, x_{\nu(k,q)})\, K^{(i)}(x_{klt+1}, \ldots, x_{klt+\varkappa})$$

есть характеристическая функция множества $\{\widetilde{\beta}_{i1}, \ldots, \widetilde{\beta}_{iq_i}\}$.

Лемма полностью доказана.

§ 9

Пусть $\mathfrak{A}$ — некоторое множество наборов длины p. Множество $\mathfrak{B}$ всех наборов $\widetilde{\beta} = (\beta_1, \ldots, \beta_p, \beta_{p+1}, \ldots, \beta_{p+d})$ таких, что $(\beta_1, \ldots, \beta_p) \in \mathfrak{A}$, будем называть *цилиндром порядка d над множеством $\mathfrak{A}$*.

Основная лемма 2. *Если*

$$\left.\begin{array}{lll} \varkappa = [\lg_2 \lg_2 n], & \lambda = [\lg_2 n - 4 \lg_2 \lg_2 n], & t = [2 \lg_2 n], \\ q = [\lg_2^2 n], & d = [2 \lg_2 \lg_2 n], & \end{array}\right\} \quad (9.1)$$

то цилиндры порядка d над множествами строк матриц H из $\mathfrak{H}$ образуют регулярное разбиение.

Доказательство. Рассмотрим цилиндр $\mathfrak{C}$ порядка d над множеством строк некоторой хорошей матрицы H. Пусть функция $f(\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3)$, где

$\widetilde{x}_1$ есть набор аргументов $x_1, \ldots, x_{klt}$,

$\widetilde{x}_2$ есть набор аргументов $x_{klt+1}, \ldots, x_{klt+\varkappa}$,

$\widetilde{x}_3$ есть набор аргументов $x_{klt+\varkappa+1}, \ldots, x_{klt+\varkappa+d}$,

принимает значение 0 вне множества $\mathfrak{C}$ (а на остальных наборах произвольна).

Функция f может быть задана табл. 2, в которой строки соответствуют наборам $\widetilde{\sigma}_3$, а столбцы—наборам $\widetilde{\beta}_u^{(v)} = (\widetilde{\sigma}_1, \widetilde{\sigma}_2)$, являющимся строками матрицы H. Столбцы матрицы, определяющей значения функции, разбиты на вертикальные полосы, по l столбцов в каждой, в соответствии с распределением наборов $\widetilde{\beta}$ по полосам матрицы H $(1 \leqslant u \leqslant k)$.

Таблица 2

$x_{klt+\varkappa+1}$	$\ldots$	$x_{klt+\varkappa+d-1}$	$x_{klt+\varkappa+d}$	$\widetilde{\beta}_1^{(1)} \ldots \widetilde{\beta}_1^{(l)}$	$\ldots \widetilde{\beta} = (\widetilde{\sigma}_1, \widetilde{\sigma}_2) \ldots$	$\widetilde{\beta}_k^{(1)} \ldots \widetilde{\beta}_k^{(l)}$	
0 0	$\ldots$	0 0	0 1				s
$\widetilde{\sigma}_3 = (\sigma_1$	$\ldots$	σ_{d-1}	$\sigma_d)$		$\square$ $f(\widetilde{\sigma}_1, \widetilde{\sigma}_2, \widetilde{\sigma}_3)$		
1	$\ldots$	1	1				$s' \leqslant s$

Разобьем строки матрицы, определяющей значения функции f, на горизонтальные полосы $A_1, \ldots, A_N$ по s строк в каждой полосе, кроме, быть может, последней, содержащей меньшее число строк; поэтому

$$N \leqslant \frac{2^d}{s} + 1. \tag{9.2}$$

Пусть $f_{\xi,\eta}$—функция, совпадающая с f на пересечении ξ-й горизонтальной и η-й вертикальной полос и равная 0 в остальных случаях. Столбцы матрицы, соответствующей этой функции, разбиваются на группы одинаковых между собой столбцов (число групп не превосходит 2^s). Столбцы, соответствующие одной группе, разобьем на подгруппы по q столбцов каждая, кроме, быть может, одной, содержащей меньшее число столбцов. Очевидно, что число $\mu(\xi, \eta)$ подгрупп (для одной функции $f_{\xi,\eta}$) не превосходит

$$\frac{l}{q} + 2^s \doteq \mu. \tag{9.3}$$

Будем считать, что число подгрупп для всех функций $f_{\xi,\eta}$ равно μ, присвоив недостающие номера $\mu(\xi, \eta)+1, \ldots, \mu$ дополнительно, например, подгруппе с номером 1. Занумеруем теперь все подгруппы (для одной функции $f_{\xi,\eta}$) натуральными числами от 1 до μ. Обозначим через $f_{\xi,\eta,\zeta}$ функцию, совпадающую с $f_{\xi,\eta}$ на ζ-й подгруппе столбцов и равную 0 в остальных случаях (таким образом, все ненулевые столбцы матрицы для $f_{\xi,\eta,\zeta}$ одинаковы между собой). Тогда

$$f_{\xi,\eta,\zeta}(\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3) = f^{(1)}_{\xi,\eta,\zeta}(\widetilde{x}_1, \widetilde{x}_2)\, f^{(2)}_{\xi,\eta,\zeta}(\widetilde{x}_3),$$

где $f^{(1)}_{\xi,\eta,\zeta}$ есть характеристическая функция множества наборов $(\widetilde{\sigma}_1, \widetilde{\sigma}_2)$, соответствующих ζ-й подгруппе столбцов в матрице для функции $f_{\xi,\eta}$; $f^{(2)}_{\xi,\eta,\zeta}$ равна дизъюнкции конъюнкций, соответствующих ненулевым строкам матрицы для $f_{\xi,\eta,\zeta}$.

На основании леммы 7 существует подстановка $\widetilde{x}^{(\xi,\zeta)}$ аргументов (из множества $\widetilde{x}_1, \widetilde{x}_2$) в функцию ψ_{kq} (не зависящая от η) и конъюнкция $K^{(\xi,\eta,\zeta)}(\widetilde{x}_2)$ такие, что

$$f^{(1)}_{\xi,\eta,\zeta}(\widetilde{x}_1,\widetilde{x}_2)=\chi(\widetilde{x}_1,\widetilde{x}_2)\,\psi_{kq}(\widetilde{x}^{(\xi,\zeta)})\,K^{(\xi,\eta,\zeta)}(\widetilde{x}_2),$$

где $\chi(\widetilde{x}_1,\widetilde{x}_2)$ — характеристическая функция множества наборов матрицы H (функция $\chi(\widetilde{x}_1,\widetilde{x}_2)$ будет также характеристической функцией цилиндра $\mathfrak{C}$, если добавить к ней несущественные переменные $\widetilde{x}_3$).

Из сказанного выше следует, что

$$\begin{aligned} f(\widetilde{x}_1,\widetilde{x}_2,\widetilde{x}_3)&=\bigvee_{\xi=1}^{N}\bigvee_{\eta=1}^{k}\bigvee_{\zeta=1}^{\mu} f^{(1)}_{\xi,\eta,\zeta}(\widetilde{x}_1,\widetilde{x}_2)\,f^{(2)}_{\xi,\eta,\zeta}(\widetilde{x}_3)=\\ &=\bigvee_{\xi=1}^{N}\bigvee_{\eta=1}^{k}\bigvee_{\zeta=1}^{\mu}\chi(\widetilde{x}_1,\widetilde{x}_2)\,\psi_{k,q}(\widetilde{x}^{(\xi,\zeta)})\,K^{(\xi,\eta,\zeta)}(\widetilde{x}_2)\,f^{(2)}_{\xi,\eta,\zeta}(\widetilde{x}_3)=\\ &=\chi(\widetilde{x}_1,\widetilde{x}_2)\,\varphi(\widetilde{x}_1,\widetilde{x}_2,\widetilde{x}_3), \end{aligned}$$

где

$$\varphi(\widetilde{x}_1,\widetilde{x}_2,\widetilde{x}_3)=\underbrace{\bigvee_{\xi=1}^{N}\bigvee_{\zeta=1}^{\mu}\underbrace{\psi_{k,q}(\widetilde{x}^{(\xi,\zeta)})}_{\mathfrak{A}_4}\underbrace{\left(\bigvee_{\eta=1}^{k}\underbrace{K^{(\xi,\eta,\zeta)}(\widetilde{x}_2)\,\underbrace{f^{(2)}_{\xi,\eta,\zeta}(\widetilde{x}_3)}_{\mathfrak{A}_1}}_{\mathfrak{A}_2}\right)}_{\mathfrak{A}_3}}_{\mathfrak{A}_5}. \qquad (9.4)$$

Положим теперь

$$s=[\lg_2 n-7\lg_2\lg_2 n]. \qquad (9.5)$$

Оценим индекс простоты правой части (9.4). Для этого будут последовательно оцениваться индексы простоты подформул $\mathfrak{A}_1-\mathfrak{A}_5$ (в (9.4) они отмечены снизу фигурными скобками).

Функция $f^{(2)}_{\xi,\eta,\zeta}$ принимает значение 1 не более чем на s наборах. Поэтому на основании (4.5)

$$L(\mathfrak{A}_1)\leqslant sd\,(P_-+P_\&+P_\vee)=L_1. \qquad (9.6)$$

Из (4.4), (9,5), (9.6) (см. также (9.1)) следует, что

$$\left.\begin{aligned} L(\mathfrak{A}_2)\leqslant\varkappa(P_-+P_\&)+L_1\leqslant(\varkappa+sd)(P_-+P_\&+P_\vee)=L_2;\\ L_2=O(\lg_2 n\cdot\lg_2\lg_2 n). \end{aligned}\right\} \qquad (9.7)$$

Далее, из (4.2) и (9.7) (напомним, что $k=2^\varkappa$ — см. стр. 71)

$$L(\mathfrak{A}_3)\leqslant k(L_2+P_\vee)=L_3;\quad L_3=O(\lg_2^2 n\cdot\lg_2\lg_2 n). \qquad (9.8)$$

Из (8.1) следует, что

$$L(\mathfrak{A}_4)=\varrho kq\left(1+O\left(\frac{1}{\lg_2 n}\right)\right)=L_4. \qquad (9.9)$$

Из (9.8) и (9.9)

$$\begin{aligned} L(\mathfrak{A}_5)\leqslant L_3+L_4+P_\&=\varrho kq\left(1+O\left(\frac{1}{\lg_2 n}\right)+O\left(\frac{\lg_2^2 n\cdot\lg_2\lg_2 n}{kq}\right)\right)=\\ =\varrho kq\left(1+O\left(\frac{\lg_2\lg_2 n}{\lg_2 n}\right)\right)=L_5. \end{aligned}$$

Из предыдущего неравенства и из (9.2), (9.3) и (9.4) имеем (так как $l = 2^\lambda$)

$$L(\varphi) \leqslant (L_5 + P_\vee)\left(\frac{2^d}{s} + 1\right)\left(\frac{l}{q} + 2^s\right) =$$
$$= L_5 \cdot \frac{2^d}{s}\frac{l}{q}\left(1 + O\left(\frac{1}{kq}\right)\right)\left(1 + O\left(\frac{s}{2^d}\right)\right)\left(1 + O\left(\frac{2^s q}{l}\right)\right) =$$
$$= L_5 \cdot \frac{2^d}{s}\frac{l}{q}\left(1 + O\left(\frac{1}{\lg_2^3 n}\right)\right)\left(1 + O\left(\frac{1}{\lg_2 n}\right)\right)\left(1 + O\,\frac{1}{\lg_2 n}\right) =$$
$$= \varrho\,\frac{2^d kl}{s}\left(1 + O\left(\frac{\lg_2 \lg_2 n}{\lg_2 n}\right)\right). \qquad (9.10)$$

Так как на основании (9.1) и (9.5)

$$s = \lg_2 n \cdot \left(1 + O\left(\frac{\lg_2 \lg_2 n}{\lg_2 n}\right)\right)$$

и для длины $m_n = klt + \varkappa$ строк из H имеет место соотношение

$$\lg_2 m_n = \varkappa + \lambda + \lg_2 t + \lg_2\left(1 + \frac{\varkappa}{klt}\right) = \lg_2 n \cdot \left(1 + O\left(\frac{\lg_2 \lg_2 n}{\lg_2 n}\right)\right),$$

то из (9.10) следует

$$L(\varphi) \leqslant \varrho\,\frac{2^d kl}{\lg_2 m_n}\left(1 + O\left(\frac{\lg_2 \lg_2 n}{\lg_2 n}\right)\right).$$

Поскольку в произведенной выше оценке никак не использовались индивидуальные особенности матрицы H, то все множества $\mathfrak{C}$, построенные для хороших матриц H, являются ε_n-регулярными, причем ε_n — одно и то же для всех этих множеств и $\varepsilon_n \to 0$ с ростом n, т. е. выполнено условие 2в) регулярности.

Проверим теперь выполнение остальных условий регулярности. Очевидно, что все цилиндры разбиения содержат одно и то же число наборов. Выполнение условий 1) (см. стр. 66) и 2б) непосредственно вытекает из (9.1). Далее, согласно лемме 6 доля нехороших матриц из $\mathfrak{H}$ составляет не более

$$\alpha = 1 - \left(1 - \frac{1}{2^{t-1}}\right)^{kl} = 1 - \left(1 - \frac{kl}{2^{t-1}} + o\left(\frac{kl}{2^{t-1}}\right)\right) = O\left(\frac{kl}{2^{t-1}}\right).$$

Из (9.1) имеем

$$\alpha = O\left(\frac{\lg_2 n \cdot n}{\lg_2^4 n \cdot n^2}\right) = O\left(\frac{1}{n \lg_2^3 n}\right).$$

Поэтому число M наборов, принадлежащих нехорошим матрицам, не превосходит $O\left(\frac{2^{m_n}}{n \lg_2^3 n}\right)$, т. е. выполнено условие 2г). Выполнение условия 2а) следует из того, что α стремится к 0.

Лемма доказана.

Итак, основная теорема, которая была сформулирована в § 1, полностью доказана, так как неравенство (1.2) является непосредственным следствием основных лемм 1 и 2.

ЛИТЕРАТУРА

[1] Riordan J., Shannon C. E., The number of two-terminal series-parallel networks, Journ. of Math. and Phys. 21, 2 (1942), 83—93.

[2] Shannon C. E., The synthesis of two-terminal switching circuits, Bell. Syst. Techn. J. 28, 1 (1949), 59—98.

[3] Кричевский Р. Е., О реализации функций суперпозициями. Сб. Проблемы кибернетики, вып. 2, М., Физматгиз, 1959, 123—138.

[4] Лупанов О. Б., О вентильных и контактно-вентильных схемах ДАН СССР **111**, 6 (1956), 1171—1174.
[5] Лупанов О. Б., Об одном методе синтеза схем, Изв. ВУЗ, Радиофизика, 1958, 1, 120—140.
[6] Лупанов О. Б., О синтезе контактных схем, ДАН СССР **119**, 1 (1958), 23—26.
[7] Hamming R. W., Error detecting and error correcting codes, Bell. Syst. Techn. J. **29**, 1 (1950), 147—160. (Есть русский перевод в сб. «Коды с обнаружением и исправлением ошибок», ИЛ, 1956, стр. 7—22).
[8] Post E. L., Introduction to a general theory of elementary propositions, Amer. J. Math. **43**, 1 (1921), 163—185.
[9] Яблонский С. В., О суперпозициях функций алгебры логики, Матем. сб. **30** (72), 2 (1952), 329—345.
[10] Яблонский С. В., Функциональные построения в k-значной логике, Труды Матем. ин-та АН СССР **51** (1958), 5—142.
[11] Жегалкин И. И., Арифметизация символической логики, Матем. сб. **35**, 3—4 (1928), 311—377.

Поступило в редакцию 31 III 1958.