ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
им. М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ

ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

СБОРНИК ЛЕКЦИЙ

VI

Москва 2011

Институт прикладной математики им. М. В. Келдыша
Российской Академии Наук
Московский государственный университет им. М.В. Ломоносова
Механико-математический факультет

ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

СБОРНИК ЛЕКЦИЙ МОЛОДЕЖНЫХ НАУЧНЫХ ШКОЛ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

VI

Москва 2011

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 11–01–06838

М34 Дискретная математика и ее приложения: Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск VI. Под редакцией А. В. Чашкина. 2011. — 50 с.

Шестой выпуск лекций содержит лекции, прочитанные на VIII молодежной научной школе по дискретной математике и ее приложениям, проходившей в Москве в ИПМ им. М. В. Келдыша РАН с 24 по 29 октября 2011 г. при поддержке Российского фонда фундаментальных исследований (проект 11–01–06838). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

ДИСКРЕТНАЯ МАТЕМАТИКА
И ЕЕ ПРИЛОЖЕНИЯ
Сборник лекций
Выпуск VI

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *О. С. Дудакова*

О НАДЕЖНОСТИ СХЕМ В ПОЛНОМ КОНЕЧНОМ БАЗИСЕ И О СВОЙСТВАХ ФУНКЦИЙ И СХЕМ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ СХЕМ

М. А. Алехина

Пензенский государственный университет,
Пенза, ул. Красная д. 40

e-mail: alehina@pnzgu.ru

Введение

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе B. Считаем, что *схема из ненадежных элементов* реализует функцию $f(x_1, \ldots, x_n)$, если она реализует ее при отсутствии неисправностей в схеме. Предполагается, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon \in (0, 1/2)$) подвержены *инверсным неисправностям на выходах*, когда функциональный элемент с приписанной функцией φ в неисправном состоянии реализует функцию $\bar{\varphi}$.

Ненадежность $P(S)$ схемы S, реализующей функцию f, определяется как максимальная вероятность ошибки $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ ($\tilde{a} = (a_1, \ldots, a_n)$) при всевозможных входных наборах $\tilde{a}$ схемы S. *Надежность* схемы S равна $1 - P(S)$.

Схема A из ненадежных элементов, реализующая функцию f, называется *асимптотически оптимальной по надежности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, где $P_\varepsilon(f) = \inf\limits_S P(S)$, инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(\tilde{x})$.

Впервые инверсные неисправности на выходах элементов рассматривал Дж. фон Нейман [10], для повышения надежности схем используя схему, реализующую функцию голосования (медиану) $m(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$. Позднее для повышения надежности использовались также схемы, реализующие функции $x_1x_2 \vee x_3x_4$ или $(x_1 \vee x_2)\&(x_3 \vee x_4)$. С. И. Аксенов [1] расширил множество функций, схемы которых могут быть использованы для повышения надежности, а именно, ввел два класса функций

$$G_1 = \{x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3} | a_i \in \{0, 1\},\ i = 1, 2, 3\},$$
$$G_4 = \{(x_1^{a_1}x_2^{a_2} \vee x_3^{a_3}x_4^{a_4})^{a_5} | a_i \in \{0, 1\},\ i = 1, 2, 3, 4, 5\}$$

и показал, что наличие любой из функций множества $G_1 \cup G_4$ в заданном базисе B, гарантирует реализацию произвольной булевой функции схемой с ненадежностью не больше $\varepsilon + c_1\varepsilon^2$ при всех $\varepsilon \in (0, \varepsilon_1]$, где ε_1, c_1 – некоторые

положительные константы, зависящие только от базиса. Обозначим эти базисы как B_ε.

Оказалось, что наличие и некоторых других функций в базисе дает такой же результат. Опишем далее (раздел 2) свойства этих функций.

С. И. Аксенов [1] также доказал, что в произвольном полном конечном базисе любую функцию f можно реализовать такой схемой S, что при всех $\varepsilon \in (0, \varepsilon_2]$ верно неравенство $P(S) \le 5\varepsilon + c_2\varepsilon^2$, причем $\varepsilon_2 = 1/3600,\ c_2 = 10584$.

В разделе 1 приведем другое, отличное от данного в работе [1] доказательство этого утверждения (теорема 2). В работе [5] доказано, что в качестве констант $\varepsilon_2,\ c_2$ можно взять $1/960$ и 182 соответственно. Оказалось, что (см. теорему 2) константу $c_2 = 182$ можно еще уменьшить до значения 99.

В дальнейшем будем использовать ранее доказанную [5] теорему 1.

Теорема 1 [5]. *В произвольном полном конечном базисе любую функцию можно реализовать такой схемой S, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(S) \le 24\varepsilon$.*

Замечание 1. Известно [10], что любая схема, содержащая хотя бы один элемент, имеет ненадежность не меньше ε.

1. Верхняя оценка ненадежности схем в произвольном полном конечном базисе

Теорема 2. *В произвольном полном конечном базисе любую функцию можно реализовать такой схемой S, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(S) \le 5,2\varepsilon$ (точнее $P(S) \le 5\varepsilon + 99\varepsilon^2$).*

Чтобы доказать теорему 2, введем необходимые понятия и сформулируем вспомогательные утверждения.

Пусть $g_1(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$. Наборы (a_1, a_2, a_3) и $(\bar a_1, \bar a_2, \bar a_3)$ будем называть *характеристическими* для данной функции g_1.

Пусть $g_2(x_1, x_2, x_3, x_4) = x_1^{a_1}x_2^{a_2} \vee x_3^{a_3}x_4^{a_4}$ или $(x_1^{a_1} \vee x_2^{a_2})\&(x_3^{a_3} \vee x_4^{a_4})$. Наборы (a_1, a_2, a_3, a_4) и $(\bar a_1, \bar a_2, \bar a_3, \bar a_4)$ будем называть *характеристическими* для функции g_2.

Лемма 1 [2]. *Допустим, что произвольную функцию f можно реализовать схемой S с ненадежностью не более p. Пусть S_g — схема, реализующая некоторую функцию $g \in G_1 \cup G_4$ с ненадежностью $P(S_g)$, причем $v_0,\ v_1$ — вероятности ошибок схемы S_g на характеристических наборах (a_1, a_2, a_3) и $(\bar a_1, \bar a_2, \bar a_3)$ соответственно, если $g \in G_1$, и на характеристических наборах (a_1, a_2, a_3, a_4) и $(\bar a_1, \bar a_2, \bar a_3, \bar a_4)$, если $g \in G_4$. Тогда можно построить схему $\Phi(S)$, которая реализует функцию f с ненадежностью*

$$P(\Phi(S)) \le \max\{v_0, v_1\} + 3pP(S_g) + 3p^2, \ \text{если } g \in G_1,$$
$$P(\Phi(S)) \le \max\{v_0, v_1\} + 4pP(S_g) + 6p^2, \ \text{если } g \in G_4.$$

Теорема 3 [8]. *В полном базисе из двухвходовых функциональных элементов любую булеву функцию f можно реализовать такой схемой S, что при всех $\varepsilon \in (0, 1/600]$ верно неравенство $P(S) \leq 5\varepsilon + 99\varepsilon^2$.*

Лемма 2 [9]. 1) *Если полный конечный базис содержит линейную функцию двух или трех переменных, то в нем любую булеву функцию можно реализовать такой схемой D, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(D) \leq 2\varepsilon + 200\varepsilon^2$.*

2) *Если полный конечный базис содержит функции $x_1 \vee x_2$ и $x_1 \& x_2$, то в нем любую булеву функцию можно реализовать такой схемой D, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(D) \leq 3\varepsilon + 225\varepsilon^2$.*

Обозначим T_0 — множество функций, сохраняющих константу 0, T_1 — множество функций, сохраняющих константу 1, L — множество линейных функций, а M — множество монотонных функций.

Лемма 3 [12]. *Пусть $f_0(x_1, \ldots, x_k) \notin T_0$, $f_1(x_1, \ldots, x_m) \notin T_1$. Тогда либо $\bar{x} \in \{f_0(x, \ldots, x), f_1(x, \ldots, x)\}$, либо $f_0(x, \ldots, x) \equiv 1$, $f_1(x, \ldots, x) \equiv 0$.*

Булевы функции $x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$ где $a_i \in \{0, 1\}$, $i \in \{0, 1, 2, 3\}$, будем называть *особенными* [11].

Лемма 4 [11]. *Из всякой нелинейной и неособенной функции от трех или более переменных подстановкой переменных можно получить либо особенную функцию, либо нелинейную функцию от двух переменных.*

Из леммы 4 получаем очевидное следствие.

Следствие 1. *Из всякой нелинейной функции f_L подстановкой переменных можно получить функцию, равную либо некоторой особенной функции: $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$, либо некоторой нелинейной функции двух переменных: $\psi(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$, где $a_i \in \{0, 1\}$, $i = 0, 1, 2, 3$.*

Лемма 5 [1]. *Пусть $f(x_1, \ldots, x_n) \notin M$ $(n \geq 3)$. Тогда из f подстановкой переменных можно получить такую функцию $\phi(x_1, x_2, x_3) \notin M$, что $\phi(x, 0, 1) = \bar{x}$.*

Доказательство. Доказательство этой леммы отличается от доказательства, приведенного в работе [1]. Пусть $f(x_1, \ldots, x_n) \notin M$ $(n \geq 3)$. Тогда [12] найдутся i $(i \in \{1, \ldots, n\})$ и два соседние по i-ой компоненте набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ и $\tilde{\beta} = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$ такие, что $f(\tilde{\alpha}) = 1, f(\tilde{\beta}) = 0$. Переименуем переменные $x_1, \ldots, x_n$ следующим образом: 1) переменную x_i назовем x_1; 2) переменную x_j $(j \in \{1, \ldots, n\}, j \neq i)$ назовем переменной x_2 тогда и только тогда, когда $\alpha_j = 0$; 3) переменную x_k $(k \in \{1, \ldots, n\}, k \neq i)$ назовем переменной x_3 тогда и только тогда, когда $\alpha_k = 1$. В результате из функции f получим такую функцию $\phi(x_1, x_2, x_3) \notin M$, что $\phi(x, 0, 1) = \bar{x}$. Лемма 5 доказана.

Замечание 2. Переменная $x_i (i = 2, 3)$ для функции $\phi(x_1, x_2, x_3)$ из леммы 5 может быть как существенной, так и фиктивной.

Замечание 3. Отличие леммы 5 от известной леммы о немонотонной функции [12] в том, что используется только подстановка переменных, которая не влияет на вероятности ошибок функционального элемента.

Обозначим $M_0 = \{\bar{x}_1\bar{x}_2, \bar{x}_1 \vee x_2, x_1 \oplus x_2 \oplus 1\}$, $M_1 = \{\bar{x}_1 \vee \bar{x}_3, \bar{x}_1 x_3, x_1 \oplus x_3\}$.

Лемма 6. *Пусть* $\phi(x_1, x_2, x_3) \notin M$ *и* $\phi(x, 0, 1) = \bar{x}$. 1) *Если* $\phi(x_1, x_2, x_3)$ *существенно зависит только от переменной* x_1, *то* $\phi(x_1, x_2, x_3) = \bar{x}_1$; 2) *если* $\phi(x_1, x_2, x_3)$ *существенно зависит только от переменных* x_1, x_2, *то* $\phi(x_1, x_2, x_3) \in M_0$; 3) *если* $\phi(x_1, x_2, x_3)$ *существенно зависит только от переменных* x_1, x_3, *то* $\phi(x_1, x_2, x_3) \in M_1$.

Доказательство. 1) Очевидно, следует из условия леммы.

2) Поскольку функция $\phi(x_1, x_2, x_3)$ существенно зависит только от двух переменных x_1, x_2, представим ее многочленом:

$$\phi(x_1, x_2, x_3) = a_1x_1x_2 \oplus a_2x_1 \oplus a_3x_2 \oplus a_4.$$

По условию $\phi(x, 0, 1) = \bar{x}$, следовательно, выполняются два равенства $a_2 = 1$, $a_4 = 1$. Получаем четыре решения: $a_1 = a_2 = a_3 = a_4 = 1$; $a_1 = 0$, $a_2 = a_3 = a_4 = 1$; $a_1 = a_2 = a_4 = 1, a_3 = 0$; $a_1 = a_3 = 0, a_2 = a_4 = 1$. Каждому из этих решений соответствует одна из функций $\bar{x}_1\bar{x}_2$, $\bar{x}_1 \vee x_2$, $x_1 \oplus x_2 \oplus 1$, $\bar{x}_1$. Переменные x_1, x_2 — существенные для функции $\phi(x_1, x_2, x_3)$, поэтому $\phi(x_1, x_2, x_3) \in M_0$.

3) Доказательство такое же как в пункте 2. Лемма 6 доказана.

Теперь докажем теорему 2.

Доказательство. Пусть B — произвольный полный конечный базис, а f — любая булева функция. По теореме 1 функцию f можно реализовать такой схемой D, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(D) \leq 24\varepsilon$.

Поскольку базис B полный, в нем содержится нелинейная функция f_L. Из функции f_L (см. лемму 4 и следствие 1) подстановкой переменных можно получить функцию, равную либо

$$\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0,$$

либо

$$\psi(x_1, x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0,$$

где $a_i \in \{0, 1\}$, $i = 0, 1, 2, 3$.

1. Пусть $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_0$.

1.1. Пусть функция $\varphi(x_1, x_2, x_3)$ конгруэнтна функции

$$\varphi_1(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus a_4(x_2 \oplus x_3) \oplus a_0.$$

Тогда $\varphi_1(x_1,x_2,x_3) = x_1^{\bar{a}_0 \oplus a_4} x_2^{\bar{a}_0} \oplus x_1^{\bar{a}_0 \oplus a_4} x_3^{\bar{a}_0} \oplus x_2^{\bar{a}_0} x_3^{\bar{a}_0}$, т. е.

$$\varphi_1(x_1,x_2,x_3) = g(x_1,x_2,x_3) \in G_1.$$

Таким образом, в качестве S_g можно взять элемент E_{φ_1}, поэтому выполняются равенства $v_1 = v_0 = P(S_g) = \varepsilon$.

Применяя лемму 1, по схеме D с использованием элемента E_g построим такую схему $\Phi(D)$, реализующую функцию f, что

$$P(\Phi(D)) \le \varepsilon + 3 \cdot 24\varepsilon \cdot \varepsilon + 3(24\varepsilon)^2 \le \varepsilon + 1800\varepsilon^2 < 2,875\varepsilon < 3\varepsilon.$$

Схема $\Phi(D) = A$ — искомая.

1.2. Пусть функция $\varphi(x_1,x_2,x_3)$ конгруэнтна функции

$$\varphi_2(x_1,x_2,x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 \oplus a_4(x_1 \oplus x_2) \oplus a_0.$$

После отождествления переменных x_1 и x_2 получим функцию

$$\varphi_2(x_1,x_1,x_3) = x_1 \oplus x_3 \oplus a_0.$$

По лемме 2 утверждение верно.

2. Пусть $\psi(x_1,x_2) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$, т. е. функция $\psi(x_1,x_2)$ конгруэнтна одной из функций $\bar{x}_1\bar{x}_2, \bar{x}_1 \vee \bar{x}_2, x_1x_2, x_1 \vee x_2, \bar{x}_1x_2, \bar{x}_1 \vee x_2$.

Если базис B содержит хотя бы одну из функций $\bar{x}_1\bar{x}_2, \bar{x}_1 \vee \bar{x}_2$, то по теореме 3 утверждение верно. Поэтому будем рассматривать только случаи, когда $\psi(x_1,x_2)$ конгруэнтна одной из функций $x_1x_2, x_1 \vee x_2, \bar{x}_1x_2, \bar{x}_1 \vee x_2$.

По условию базис B — полный, поэтому в нем содержатся функции $f_0 \notin T_0$ и $f_1 \notin T_1$, из которых по лемме 3 отождествлением переменных получим либо $\bar{x} \in \{f_0(x,\dots,x), f_1(x,\dots,x)\}$, либо $f_0(x,\dots,x) \equiv 1,\ f_1(x,\dots,x) \equiv 0$.

2.1. Пусть $\bar{x} \in \{f_0(x,\dots,x), f_1(x,\dots,x)\}$. Тогда имеем четыре полных базиса $\{x_1x_2, \bar{x}_1\},\ \{x_1 \vee x_2, \bar{x}_1\},\ \{\bar{x}_1x_2, \bar{x}_1\},\ \{\bar{x}_1 \vee x_2, \bar{x}_1\}$, в каждом из которых по теореме 3 утверждение верно.

2.2. Пусть $f_0(x,\dots,x) \equiv 1,\ f_1(x,\dots,x) \equiv 0$.

В полных базисах $\{\bar{x}_1x_2, 1\},\ \{\bar{x}_1 \vee x_2, 0\}$ по теореме 3 утверждение верно. Поэтому далее будем считать, что нелинейная функция $\psi(x_1,x_2)$ равна x_1x_2 или $x_1 \vee x_2$.

Базис B — полный, поэтому в нем содержится немонотонная функция f_M. Если функция f_M зависит не более чем от двух переменных, то она конгруэнтна одной из функций множества M_2, где $M_2 = M_0 \cup M_1 \cup \{\bar{x}_1\}$. Добавим к каждому из множеств $\{x_1x_2, 0, 1\},\ \{x_1 \vee x_2, 0, 1\}$ любую немонотонную функцию из M_2 и получим полный базис из двухвходовых элементов, к которому применима теорема 3.

Пусть функция f_M зависит не менее чем от трех переменных. По лемме 5 из функции f_M подстановкой переменных можно получить такую немонотонную функцию $\phi(x_1,x_2,x_3)$, что $\phi(x_1,0,1) = \bar{x}_1$. Представим ее многочленом:

$$\phi(x_1,x_2,x_3) = a_1x_1x_2x_3 \oplus a_2x_1x_2 \oplus a_3x_1x_3 \oplus a_4x_2x_3 \oplus a_5x_1 \oplus a_6x_2 \oplus a_7x_3 \oplus a_8.$$

После подстановки констант 0, 1 в многочлен получим два равенства $a_3 \oplus a_5 = 1$, $a_7 \oplus a_8 = 1$. Решая эти уравнения, получим четыре решения: 1) $a_3 = 1$, $a_5 = 0$, $a_7 = 0$, $a_8 = 1$; 2) $a_3 = 0$, $a_5 = 1$, $a_7 = 0, a_8 = 1$; 3) $a_3 = 1$, $a_5 = 0$, $a_7 = 1$, $a_8 = 0$; 4) $a_3 = 0$, $a_5 = 1$, $a_7 = 1$, $a_8 = 0$. Подставим каждую из этих четверок в многочлен и исследуем полученные функции.

2.2.1. Пусть $\phi(x_1, x_2, x_3) = a_1x_1x_2x_3 \oplus a_2x_1x_2 \oplus x_1x_3 \oplus a_4x_2x_3 \oplus a_6x_2 \oplus 1$. Отождествим переменные x_1 и x_3 и получим

$$\phi(x_1, x_2, x_1) = x_1x_2(a_1 \oplus a_2 \oplus a_4) \oplus x_1 \oplus a_6x_2 \oplus 1.$$

Если $a_1 \oplus a_2 \oplus a_4 = 0,\ a_6 = 0$, то $\phi(x_1, x_2, x_1) = \bar{x}_1$; если $a_1 \oplus a_2 \oplus a_4 = 0,\ a_6 = 1$, то $\phi(x_1, x_2, x_1) = x_1 \oplus x_2 \oplus 1$; если $a_1 \oplus a_2 \oplus a_4 = 1,\ a_6 = 0$, то $\phi(x_1, x_2, x_1) = \bar{x}_1 \vee x_2$; если $a_1 \oplus a_2 \oplus a_4 = 1,\ a_6 = 1$, то $\phi(x_1, x_2, x_1) = \bar{x}_1 \& \bar{x}_2$. Таким образом, в каждом случае получаем полный базис из двухвходовых элементов, к которому применима теорема 3.

2.2.2. Пусть $\phi(x_1, x_2, x_3) = a_1x_1x_2x_3 \oplus a_2x_1x_2 \oplus a_4x_2x_3 \oplus x_1 \oplus a_6x_2 \oplus 1$. Отождествим переменные x_2 и x_3 и получим

$$\phi(x_1, x_2, x_2) = x_1x_2(a_1 \oplus a_2 \oplus a_4) \oplus x_1 \oplus a_6x_2 \oplus 1.$$

Далее рассуждаем как в п. 2.2.1.

2.2.3. Пусть $\phi(x_1, x_2, x_3) = a_1x_1x_2x_3 \oplus a_2x_1x_2 \oplus x_1x_3 \oplus a_4x_2x_3 \oplus a_6x_2 \oplus x_3$. Отождествим переменные x_1 и x_2 и получим

$$\phi(x_1, x_1, x_3) = x_1x_3(a_1 \oplus a_4 \oplus 1) \oplus x_1(a_2 \oplus a_6) \oplus x_3.$$

1) Если $a_1 \oplus a_4 \oplus 1 = 0,\ a_2 \oplus a_6 = 1$, то $\phi(x_1, x_1, x_3) = x_1 \oplus x_3$; 2) если $a_1 \oplus a_4 \oplus 1 = 1,\ a_2 \oplus a_6 = 0$, то $\phi(x_1, x_1, x_3) = \bar{x}_1 \& x_3$; 3) если $a_1 \oplus a_4 \oplus 1 = 0$, $a_2 \oplus a_6 = 0$, то $\phi(x_1, x_1, x_3) = x_3$; 4) если $a_1 \oplus a_4 \oplus 1 = 1$, $a_2 \oplus a_6 = 1$, то $\phi(x_1, x_1, x_3) = x_1 \vee x_3$. В первых двух случаях получаем полный базис из двухвходовых элементов, к которому применима теорема 3. Подробнее остановимся на двух последних случаях.

2.2.3.1. Пусть $a_1 \oplus a_4 \oplus 1 = 0,\ a_2 \oplus a_6 = 0$. Возможны четыре варианта.

2.2.3.1.1. $a_1 = 0, a_4 = 1, a_2 = 0, a_6 = 0$. Тогда $\phi(x_1, x_2, x_3) = x_1x_3 \oplus x_2x_3 \oplus x_3$. Вместо переменной x_3 подставим константу 1 и получим линейную функцию $\phi(x_1, x_2, 1) = x_1 \oplus x_2 \oplus 1$, которую, очевидно можно реализовать схемой из двух элементов. По лемме 2 утверждение верно.

2.2.3.1.2. $a_1 = 1, a_4 = 0, a_2 = 0, a_6 = 0$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_3 \oplus x_3.$$

Поскольку $\phi(x_3, x_4, 1) = \bar{x}_3 \vee x_4$, функцию

$$g(x_1, x_2, x_3, x_4) = \phi(x_1, x_2, \phi(x_3, x_4, 1)) = (\bar{x}_1 \vee x_2)(\bar{x}_3 \vee x_4) \in G_4$$

можно реализовать схемой S_g из трех элементов. Поэтому $v_0, v_1, P(S_g) \leq 3\varepsilon$. Применяя лемму 1, по схеме D с использованием схемы S_g построим такую схему $\Phi(D)$, реализующую функцию f, что

$$P(\Phi(D)) \leq 3\varepsilon + 4 \cdot 24\varepsilon \cdot 3\varepsilon + 6(24\varepsilon)^2 \leq 3\varepsilon + 3744\varepsilon^2 \leq 6,9\varepsilon$$

при всех $\varepsilon \in (0, 1/960]$. Воспользуемся леммой 1 еще раз: по схеме $\Phi(D)$ с использованием схемы S_g построим такую схему $\Phi^2(D)$, реализующую функцию f, что

$$P(\Phi^2(D)) \leq 3\varepsilon + 4 \cdot 6,9\varepsilon \cdot 3\varepsilon + 6(6,9\varepsilon)^2 \leq 3\varepsilon + 368,46\varepsilon^2 \leq 3,4\varepsilon$$

при всех $\varepsilon \in (0, 1/960]$.

Схема $\Phi^2(D) = A$ — искомая.

2.2.3.1.3. $a_1 = 0, a_4 = 1, a_2 = 1, a_6 = 1$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3.$$

Эта функция — особенная, она рассмотрена в п.1.1 этого доказательства.

2.2.3.1.4. $a_1 = 1, a_4 = 0, a_2 = 1, a_6 = 1$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_3 \oplus x_1x_2 \oplus x_2 \oplus x_3.$$

Тогда линейную функцию $\phi(0, x_2, x_3) = x_2 \oplus x_3$ можно реализовать схемой из двух элементов. По лемме 2 утверждение верно.

2.2.3.2. Пусть $a_1 \oplus a_4 \oplus 1 = 1$, $a_2 \oplus a_6 = 1$. В этом случае $\phi(x_1, x_2, x_1) = x_1 \vee x_3$. Следовательно, в базисе $\{x_1 \& x_2, 0, 1, \phi(x_1, x_2, x_3)\}$ утверждение теоремы верно. Убедимся в верности теоремы для базиса $\{x_1 \vee x_2, 0, 1, \phi(x_1, x_2, x_3)\}$, получив из $\phi(x_1, x_2, x_3)$ подстановкой $x_1 \& x_2$.

Для набора значений a_1, a_4, a_2, a_6 возможны четыре варианта.

2.2.3.2.1. $a_1 = 0, a_4 = 0, a_2 = 0, a_6 = 1$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_3 \oplus x_2 \oplus x_3.$$

Из этой функции при отождествлении переменных x_2 и x_3 получим $x_1 \& x_3$.

2.2.3.2.2. $a_1 = 0, a_4 = 0, a_2 = 1, a_6 = 0$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_3.$$

Из этой функции при отождествлении переменных x_1 и x_3 получим $x_1 \& x_2$.

2.2.3.2.3. $a_1 = 1, a_4 = 1, a_2 = 1, a_6 = 0$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3.$$

Из этой функции при отождествлении переменных x_2 и x_3 получим $x_1 \& x_2$.

2.2.3.2.4. $a_1 = 1, a_4 = 1, a_2 = 0, a_6 = 1$. Тогда

$$\phi(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3 = \bar{x}_1x_3 \vee x_2.$$

Тогда функцию $g(x_1, x_2, x_3, x_4) = \phi(x_1, \phi(x_2, 0, x_4), x_3) = \bar{x}_1x_3 \vee \bar{x}_2x_4 \in G_4$ можно реализовать схемой S_g из трех элементов. Поэтому $v_0, v_1, P(S_g) \leq 3\varepsilon$.

Далее рассуждаем как в п. 2.2.3.1.2.

Теорема 2 доказана.

Известно [9], что в общем случае константу 5 в оценке ненадежности понизить нельзя. Например, в базисах $\{x_1x_2, \bar{x}_1\}$, $\{\bar{x}_1 \vee x_2, 0\}$ для почти всех функций асимптотически оптимальные по надежности схемы функционируют с ненадежностью, асимптотически равной 5ε при $\varepsilon \to 0$.

2. Свойства функций и схем, используемых для повышения надежности схем

В этом разделе будем считать, что неисправности элементов схемы произвольные.

Пусть булева функция $m(x_1, \ldots, x_k)$ $(k \geq 3)$ обладает свойством: найдется такой набор $(b_1, \ldots, b_k)$, что на нем и всех соседних с ним наборах функция m принимает значение 0, а на наборе $(\bar{b}_1, \ldots, \bar{b}_k)$ и всех соседних с ним наборах — значение 1. Наборы $(b_1, \ldots, b_k)$ и $(\bar{b}_1, \ldots, \bar{b}_k)$ будем называть *характеристическими* наборами функции $m(x_1, \ldots, x_k)$. Обозначим через M_k множество всех функций $m(x_1, \ldots, x_k)$ с названным свойством.

Нетрудно проверить, что $2^{2^k-2k-1} \leq |M_k| \leq 2^{2^k-k-2}$. Заметим также, что: 1) $M_{k-1} \subset M_k$ $(k \geq 4)$; 2) $M_3 = G_1$; 3) $(G_1 \cup G_4) \subset M_4$ и $|M_4| = 992$.

Теорема 4 [2]. *Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, а схема S реализует f с ненадежностью $P(S) \leq p$. Пусть $m(x_1, \ldots, x_k)$ — функция из M_k, схема S_m реализует ее с ненадежностью $P(S_m) \leq p$. Пусть v^1 и v^0 — вероятности ошибок схемы S_m на характеристических наборах. Тогда функцию f можно реализовать такой схемой A, что будет выполнено неравенство $P(A) \leq \max\{v^0, v^1\} + cp^2$, где положительная константа $c \leq kC_k^{[k/2]}$.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, схема S реализует f с ненадежностью $P(S) \leq p$, а схема S^0 реализует функцию $\bar{f}$ с ненадежностью $P(S^0) \leq p$. Пусть $(b_1, \ldots, b_k)$ — характеристический набор функции $m(x_1, \ldots, x_k)$ и $m(b_1, \ldots, b_k) = 0$. Предположим в этом наборе компоненты $b_{i_1}, \ldots, b_{i_t}$ равны нулю, а остальные — единице. Возьмем t экземпляров схемы S и $k - t$ экземпляров S^0. Соединим i_1-й, $\ldots$, i_t-й входы схемы S_m с выходами схем S, а остальные $k-t$ входов — с выходами схем S^0. Построенная схема, обозначим ее D, реализует функцию f. Вычислим вероятности ошибок на выходе схемы D.

Пусть входной набор $\tilde{a}$ схемы S таков, что $f(\tilde{a}) = 0$. Вероятность ошибки $P_1(D, \tilde{a})$ на выходе схемы D в этом случае удовлетворяет неравенству

$$P_1(D, \tilde{a}) \le v_1 + kpP(S_m) + \sum_{i=2}^{k} C_k^i p^i \le v^1 + kpP(S_m) + (k-1)C_k^{[k/2]} p^2.$$

Но $P(S_m) \le p$, поэтому

$$P_1(D, \tilde{a}) \le v^1 + kp^2 + (k-1)C_k^{[k/2]} p^2 \le v^1 + kC_k^{[k/2]} p^2.$$

Аналогично получается неравенство для наборов $\tilde{a}$, на которых $f(\tilde{a}) = 1$. Таким образом, $P(D) \le \max\{v_1, v_0\} + kC_k^{[k/2]} p^2$. Теорема 4 доказана.

Следствие 2 [2]. *Пусть базис B содержит функцию $m(x_1, \ldots, x_k) \in M_k$, f — произвольная булева функция, а S — схема, ее реализующая с ненадежностью $P(S) \le 5,2\varepsilon$ при всех $\varepsilon \in (0, 1/960]$. Тогда функцию f можно реализовать такой схемой A в базисе B, что $P(A) \le \varepsilon + c\varepsilon^2$ (c — положительная константа, $c \le 28kC_k^{[k/2]}$).*

Доказательство следует из равенств $v^1 = v^0 = \varepsilon$ и теоремы 4.

Таким образом, если базис $B \cap M_k \ne \emptyset$, то базис B является базисом B_ε.

Оказалось, что класс функций M_k можно расширить.

Пусть $\hat{\alpha} = (\alpha_1, \ldots, \alpha_k)$, $\hat{\beta} = (\beta_1, \ldots, \beta_k)$ — некоторые двоичные наборы длины k. Обозначим через $\rho(\hat{\alpha}, \hat{\beta})$ расстояние Хэмминга между ними, равное $\rho(\hat{\alpha}, \hat{\beta}) = \sum\limits_{i=1}^{k} |\alpha_i - \beta_i|$.

Пусть булева функция $m(x_1, \ldots, x_k)$, $k \ge 3$, обладает следующим свойством: существуют наборы $\hat{\alpha}, \hat{\beta}$ длины k такие, что 1) $3 \le \rho(\hat{\alpha}, \hat{\beta}) = \rho \le k$, 2) для любого набора $\hat{x}$ такого, что $\rho(\hat{\alpha}, \hat{x}) \le 1$, верно $m(\hat{x}) = 0$, и 3) для любого набора $\hat{y}$ такого, что $\rho(\hat{\beta}, \hat{y}) \le 1$, верно $m(\hat{y}) = 1$. Обозначим через $M_k(\rho)$ класс функций с названным свойством, а наборы $\hat{\alpha}, \hat{\beta}$ также как раньше будем называть *характеристическими*. Полагаем $\tilde{M}_k = \bigcup\limits_{\rho=3}^{k} M_k(\rho)$. Очевидно, что 1) $M_k(k) = M_k$, 2) $M_k \subset \tilde{M}_k$.

Теорема 5 [4]. *Допустим, что любую булеву функцию можно реализовать схемой с ненадежностью не больше $p \le 1/2$. Пусть схема S_m реализует функцию $m(x_1, \ldots, x_k) \in \tilde{M}_k$ с ненадежностью $P(S_m) \le p$, причем v_1 и v_0 вероятности ошибок схемы S_m на характеристических наборах. Тогда произвольную функцию $f(x_1, \ldots, x_n)$ можно реализовать такой схемой A, что $P(A) \le max\{v_1, v_0\} + cp^2$, где положительная константа $c \le k + 2C_k^{[k/2]}$.*

Доказательство. Пусть функция $m(x_1,\ldots,x_k) \in \tilde{M}_k$ имеет характеристические наборы $\hat{\alpha},\hat{\beta}$ такие, что $m(\hat{\alpha})=0$ и $m(\hat{\beta})=1$. Не ограничивая общности, будем считать, что для характеристических наборов $\hat{\alpha},\hat{\beta}$ выполняются соотношения:

$$\begin{aligned}
&\alpha_1 \neq \beta_1,\ldots,\alpha_d \neq \beta_d,\\
&\alpha_1=\alpha_2=\ldots=\alpha_t=0, \quad \alpha_{t+1}=\alpha_{t+2}=\ldots=\alpha_d=1,\\
&\alpha_{d+1}=\alpha_{d+2}=\ldots=\alpha_l=\beta_{d+1}=\beta_{d+2}=\ldots=\beta_l=0,\\
&\alpha_{l+1}=\alpha_{l+2}=\ldots=\alpha_k=\beta_{l+1}=\beta_{l+2}=\ldots=\beta_k=1.
\end{aligned}$$

Пусть $f(x_1,\ldots,x_n)$ — произвольная булева функция. Возьмем t экземпляров схемы S, реализующей функцию f с ненадежностью $P(S)\le p$ и $d-t$ экземпляров схемы S^0, реализующей функцию $\bar{f}$ с ненадежностью $P(S^0)\le p$. Соединим первые t из d входов схемы S_m с выходами t экземпляров схемы S соответственно, а последние $d-t$ входов схемы S_m с выходами $d-t$ экземпляров схемы S^0 соответственно. Поскольку любую булеву функцию можно реализовать схемой с ненадежностью не больше $p\le 1/2$, возьмем $l-d$ экземпляров схемы O, реализующей константу 0 с ненадежностью $P(O)\le p$. Соединим $(d+1)$-й, $\ldots,l$-й входы схемы S_m с выходами $l-d$ экземпляров схемы O соответственно. Возьмем $k-l$ экземпляров схемы I, реализующей константу 1 с ненадежностью $P(I)\le p$, и последние $k-l$ входов схемы S_m соединим с выходами $k-l$ экземпляров схемы I соответственно. Построенная таким образом схема D реализует функцию f.

Вычислим вероятности ошибок на выходе схемы D. Пусть входной набор $\tilde{a}$ схемы S является нулевым для функции f, т. е. $f(\tilde{a})=0$. Вероятность ошибки на выходе схемы D в этом случае удовлетворяет неравенству

$$\begin{aligned}
P_1(D,\tilde{a}) &\le v_1 + kpP(S_m) + \sum_{i=2}^{k} C_k^i p^i \le v_1 + kp^2 + \sum_{i=2}^{k} C_k^i p^i \le\\
&\le v_1 + kp^2 + C_k^{[k/2]} \sum_{i=2}^{k} p^i = v_1 + kp^2 + C_k^{[k/2]} p^2 (1-p^{k-1})/(1-p) \le\\
&\le v_1 + p^2(k + C_k^{[k/2]}/(1-p)) \le v_1 + (k+2C_k^{[k/2]})p^2.
\end{aligned}$$

Аналогично получается неравенство для наборов $\tilde{a}$, на которых $f(\tilde{a})=1$. Таким образом, $P(D)\le \max\{v_1,v_0\} + (k+2C_k^{[k/2]})p^2$. Теорема 5 доказана.

Следствие 3 [4]. *Пусть полный конечный базис B содержит функцию $m(x_1,\ldots,x_k)\in \tilde{M}_k$, а базисные элементы с вероятностью ε подвержены инверсным неисправностям на выходах. Тогда любую булеву функцию можно реализовать такой схемой S, что при всех $\varepsilon\in(0,1/960]$ верно неравенство $P(S)\le \varepsilon + c\varepsilon^2$, где $c\le k+2C_k[k/2]$.*

Доказательство следует из равенств $v^1 = v^0 = \varepsilon$ и теоремы 5.

Теорема 6 [4]. $|\tilde{M}_k| \le 2^{2^k-2} - (k^2+k+2)2^{2^k-k-3}$.

Доказательство. Пусть функция $m(x_1,\dots,x_k) \in \tilde{M}_k$. Характеристический набор $\hat{\alpha}$, $m(\hat{\alpha}) = 0$, этой функции можно выбрать 2^k способами, тогда характеристический набор $\hat{\beta}$, $m(\hat{\beta}) = 1$, можно выбрать $2^k - 1 - k - k(k-1)/2$ способами, остальные $2^k - 2k - 2$ значений функции произвольны. Поэтому $|\tilde{M}_k| \le 2^k(2^k - 1 - k - k(k-1)/2)(2^{2^k-2k-2}) = 2^{2^k-2} - (k^2+k+2)2^{2^k-k-3}$. Теорема 6 доказана.

Замечание 4. Известно, что число всех функций от 4-х переменных равно $2^{2^4} = 65536$. В работе [6] найдено $|\tilde{M}_4| = 3152$.

Класс M_k мы расширили до класса $\tilde{M}_k$. Является ли множество $\tilde{M}_k$ исчерпывающим, критериальным? Или существуют другие функции, при наличии которых рассматриваемый базис B является базисом B_ε? Ответы на эти вопросы получены в следующем разделе.

3. Специальный класс функций

В этом разделе снова считаем, что все элементы подвержены инверсным неисправностям на выходах.

Пусть G_2 — множество функций, конгруэнтных одной из функций вида $x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3}$, G_3 — множество функций, конгруэнтных одной из функций вида $x_1^{\sigma_1}x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2}x_3^{\sigma_3}$, где $\sigma_1,\sigma_2,\sigma_3 \in \{0,1\}$. Полагаем $G = G_1 \cup G_2 \cup G_3$.

Замечание 5. Пусть B_3 – множество булевых функций, зависящих от переменных x_1, x_2 и x_3. Нетрудно проверить, что $|G_1 \cap B_3| = 8$, $|G_2 \cap B_3| = 24$, $|G_3 \cap B_3| = 24$. Таким образом, $|G \cap B_3| = 56$.

В синтезе схем с интересующими нас свойствами особое место будет отведено операциям над схемами.

Пусть функция $g \in G_1$, т. е. $g(x_1,x_2,x_3) = x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}$. Напомним, что наборы $(\sigma_1,\sigma_2,\sigma_3)$, $(\bar{\sigma}_1,\bar{\sigma}_2,\bar{\sigma}_3)$ для функции $g(x_1,x_2,x_3)$ являются характеристическими.

Обозначим f^σ функцию $\bar{f}$, если $\sigma = 0$ и функцию f, если $\sigma = 1$. Возьмем схемы $S^{\sigma_1}, S^{\sigma_2}, S^{\sigma_3}$, реализующие функции $f^{\sigma_1}, f^{\sigma_2}, f^{\sigma_3}$ соответственно, и соединим их выходы со входами схемы S_g, реализующей функцию g. Построенную таким образом схему обозначим $\Phi(S^0,S^1)$. Нетрудно проверить, что в результате применения операции Φ к схемам S^0, S^1, реализующим функции $\bar{f}$, f соответственно, получается схема, реализующая функцию f. Результат n-кратного применения ($n \in \mathbf{N}$) операции Φ к схемам S^0, S^1 будем обозначать $\Phi^n(S^0,S^1)$.

Результат теоремы 7 известен и принадлежит Дж. фон Нейману [10]. Здесь он приводится для полноты изложения и отличается от оригинала [10] константами, ограничивающими ε и коэффициент при ε^2.

Теорема 7. *Пусть базис B содержит функцию $\varphi \in G_1$. Тогда любую функцию f в этом базисе можно реализовать такой схемой A, что с при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(A) \leq \varepsilon + 8\varepsilon^2$.*

Доказательство. Пусть в базисе B содержится функция $\varphi \in G_1$. Без ограничения общности можно считать, что

$$\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} \& x_2^{\sigma_2} \vee x_2^{\sigma_2} \& x_3^{\sigma_3} \vee x_1^{\sigma_1} \& x_3^{\sigma_3} \in G_1,$$

где $\sigma_i \in \{0, 1\}$, $i = 1, 2, 3$. Ясно, что в качестве схемы S_g берем базисный элемент E_g, реализующий функцию $x_1^{\sigma_1} \& x_2^{\sigma_2} \vee x_2^{\sigma_2} \& x_3^{\sigma_3} \vee x_1^{\sigma_1} \& x_3^{\sigma_3}$. Вероятности ошибок v^1 и v^0 на характеристических наборах $\tilde{\alpha} = (\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3)$ и $\tilde{\beta} = (\sigma_1, \sigma_2, \sigma_3)$ соответственно равны $v^1 = \varepsilon = v^0$.

Возьмем три схемы S^{σ_i} $(i = 1, 2, 3)$, каждая из которых реализует функцию f^{σ_i} и удовлетворяет теореме 2, а также схему S_g и построим схему $\Phi(S^0, S^1)$. Используя лемму 1, оценим ненадежность схемы $\Phi(S^0, S^1)$ и получим $P(\Phi(S^0, S^1)) \leq \varepsilon + 3\varepsilon \cdot 5, 2\varepsilon + 3(5, 2\varepsilon)^2 \leq \varepsilon + 97\varepsilon^2 \leq 1, 11\varepsilon$ при $\varepsilon \in (0, 1/960]$. По схеме $\Phi(S^0, S^1)$ построим схему $\Phi^2(S^0, S^1)$. По замечанию 1 получим $P(\Phi^2(S^0, S^1)) \leq \varepsilon + 3\varepsilon \cdot 1, 11\varepsilon + 3(1, 11\varepsilon)^2 \leq \varepsilon + 7, 03\varepsilon^2 \leq \varepsilon + 8\varepsilon^2$. Теорема 7 доказана.

Теорема 8 [9]. *Пусть полный конечный базис B содержит функцию $\varphi \in G_2$. Тогда любую функцию f в этом базисе можно реализовать такой схемой A, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(A) \leq \varepsilon + 200\varepsilon^2$.*

Доказательство. Пусть $\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} x_2^{\sigma_2} \oplus x_3^{\sigma_3} \in G_2$, где $\sigma_i \in \{0, 1\}$, $i = 1, 2, 3$. Поскольку B — полный базис, функции $(x_1 \oplus x_2)^{\sigma} \in [B]$ $(\sigma \in \{0, 1\})$. Реализуем функции $(x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}$ и $(x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}$ такими схемами D_1 и D_2 соответственно, что $P(D_1) \leq 5, 2\varepsilon$ и $P(D_2) \leq 5, 2\varepsilon$ (см. теорему 2). Моделируя формулу $\varphi((x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}, (x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}, x_1)$ и используя схемы D_1, D_2 и элемент E_φ, строим схему S_g, которая реализует функцию

$$\begin{aligned}
&\varphi((x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3}, (x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3}, x_1) = \\
&\quad = ((x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3})^{\sigma_1} ((x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3})^{\sigma_2} \oplus x_1^{\sigma_3} = \\
&\quad = ((x_1 \oplus x_2)^{\bar{\sigma}_1 \oplus \sigma_3} \oplus \bar{\sigma}_1)((x_1 \oplus x_3)^{\bar{\sigma}_2 \oplus \sigma_3} \oplus \bar{\sigma}_2) \oplus x_1^{\sigma_3} = \\
&\quad = (x_1 \oplus x_2 \oplus \bar{\sigma}_1 \oplus \sigma_3 \oplus 1 \oplus \bar{\sigma}_1)(x_1 \oplus x_3 \oplus \bar{\sigma}_2 \oplus \sigma_3 \oplus 1 \oplus \bar{\sigma}_2) \oplus x_1^{\sigma_3} = \\
&\quad = (x_1 \oplus x_2 \oplus \bar{\sigma}_3)(x_1 \oplus x_3 \oplus \bar{\sigma}_3) \oplus x_1^{\sigma_3} = \\
&\quad = (x_1^{\sigma_3} \oplus x_2)(x_1^{\sigma_3} \oplus x_3) \oplus x_1^{\sigma_3} = x_1^{\sigma_3} x_2 \vee x_1^{\sigma_3} x_3 \vee x_2 x_3
\end{aligned}$$

из множества G_1.

Для схемы S_g (очевидно, $P(S_g) \leq 11, 4\varepsilon$) вычислим вероятности ошибок v^1 и v^0 на наборах $(\bar{\sigma}_3, 0, 0)$ и $(\sigma_3, 1, 1)$ соответственно. Вероятность ошибки v^1 удовлетворяет неравенству: $v^1 \leq \varepsilon + 2(5, 2\varepsilon)\varepsilon + (5, 2\varepsilon)^2 \leq \varepsilon + 37, 5\varepsilon^2$.

Аналогично получается 2-е неравенство:

$$v^0 \le \varepsilon + 2(5,2\varepsilon)\varepsilon + (5,2\varepsilon)^2 \le \varepsilon + 37,5\varepsilon^2.$$

Пусть f — произвольная булева функция. Возьмем два экземпляра схемы S, реализующей функцию f, схему S_{σ_3}, которая реализует функцию f^{σ_3}, причем $P(S) \le 5,2\varepsilon$, $P(S_{\sigma_3}) \le 5,2\varepsilon$ (см. теорему 2). Используя схему S_g, построим схему $\Phi(S_{\sigma_3}, S) = A$. Тогда по лемме 1 функцию f можно реализовать схемой A с ненадежностью $P(A) \le \varepsilon + 37,5\varepsilon^2 + 3 \cdot 5,2\varepsilon \cdot 11,4\varepsilon + 3(5,2\varepsilon)^2 \le \varepsilon + 200\varepsilon^2$. Теорема 8 доказана.

Теорема 9 [9]. *Пусть базис B содержит функцию $\varphi \in G_3$. Тогда любую функцию f в этом базисе можно реализовать схемой A с ненадежностью $P(A) \le \varepsilon + 18\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$.*

Доказательство. Пусть в базисе B содержится функция

$$\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} \& x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2} \& x_3^{\sigma_3} \in G_3,$$

где $\sigma_i \in \{0,1\}$, $i = 1,2,3$. Без ограничения общности можно считать, что $\sigma_2 = 1$, т. е. $\varphi(x_1, x_2, x_3) = x_1^{\sigma_1} \& \bar{x}_2 \vee x_2 \& x_3^{\sigma_3}$.

Покажем, что $\varphi(x_1, \varphi(x_1, x_2, x_3), x_3) = x_1^{\sigma_1} \& x_2 \vee x_1^{\sigma_1} \& x_3^{\sigma_3} \vee x_2 \& x_3^{\sigma_3}$.

Действительно,

$$\begin{aligned}
&\varphi(x_1, \varphi(x_1, x_2, x_3), x_3) = \varphi(x_1, (x_1^{\sigma_1}\bar{x}_2 \vee x_2 x_3^{\sigma_3}), x_3) = \\
&= x_1^{\sigma_1}\overline{(x_1^{\sigma_1}\bar{x}_2 \vee x_2 x_3^{\sigma_3})} \vee (x_1^{\sigma_1}\bar{x}_2 \vee x_2 x_3^{\sigma_3}) x_3^{\sigma_3} = \\
&= x_1^{\sigma_1}(\overline{(x_1^{\sigma_1}\bar{x}_2)}\,\overline{(x_2 x_3^{\sigma_3})}) \vee x_1^{\sigma_1}\bar{x}_2 x_3^{\sigma_3} \vee x_2 x_3^{\sigma_3} = \\
&= x_1^{\sigma_1}(x_1^{\bar{\sigma}_1} \vee x_2)(\bar{x}_2 \vee x_3^{\bar{\sigma}_3}) \vee (x_1^{\sigma_1}\bar{x}_2 \vee x_2) x_3^{\sigma_3} = \\
&= (x_1^{\sigma_1} x_1^{\bar{\sigma}_1} \vee x_1^{\sigma_1} x_2)(\bar{x}_2 \vee x_3^{\bar{\sigma}_3}) \vee (x_1^{\sigma_1} \vee x_2) x_3^{\sigma_3} = \\
&= x_1^{\sigma_1} x_2 \bar{x}_2 \vee x_1^{\sigma_1} x_2 x_3^{\bar{\sigma}_3} \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2 x_3^{\sigma_3} = \\
&= x_1^{\sigma_1}(x_2 x_3^{\bar{\sigma}_3} \vee x_3^{\sigma_3}) \vee x_2 x_3^{\sigma_3} = x_1^{\sigma_1}(x_2 \vee x_3^{\sigma_3}) \vee x_2 x_3^{\sigma_3} = \\
&= x_1^{\sigma_1} x_2 \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2 x_3^{\sigma_3}.
\end{aligned}$$

Моделируя формулу $\varphi(x_1, \varphi(x_1, x_2, x_3), x_3)$, построим схему S_g из двух элементов, реализующую функцию $x_1^{\sigma_1} x_2 \vee x_1^{\sigma_1} x_3^{\sigma_3} \vee x_2 x_3^{\sigma_3}$. Очевидно, $P(S_g) \le 2\varepsilon$.

Вычислим вероятности ошибок v^1 и v^0 этой схемы на наборах $(\bar{\sigma}_1, 0, \bar{\sigma}_3)$ и $(\sigma_1, 1, \sigma_3)$ соответственно. Получаем $v^1 = \varepsilon = v^0$.

Пусть f — произвольная булева функция. Возьмем схемы S, S^{σ_1}, S^{σ_3}, реализующие соответственно функции f, f^{σ_1}, f^{σ_3}, причем ненадежности всех трех схем не больше $5,2\varepsilon$ (см. теорему 2). Используя схему S_g, построим схему $\Phi(S^0, S)$. Тогда по лемме 1 функцию f можно реализовать схемой A с ненадежностью $P(\Phi(S^0, S)) \le \varepsilon + 3 \cdot 2\varepsilon \cdot 5,2\varepsilon + 3(5,2\varepsilon)^2 \le \varepsilon + 112,32\varepsilon^2 \le 1,117\varepsilon$ при $\varepsilon \in (0, 1/960]$. По схеме $\Phi(S^0, S)$ построим схему $\Phi^2(S^0, S)$. По лемме 1 получим $P(\Phi^2(S^0, S)) \le \varepsilon + 8,2\varepsilon^2 \le \varepsilon + 17,94\varepsilon^2$. Теорема 9 доказана.

Из теорем 7, 8 и 9 и замечания 1 получаем следующий результат [9]: если в полном конечном базисе B содержится функция из множества G, то в этом базисе любую булеву функцию можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

В [9] для полных базисов $B \subseteq B_3$ доказано, что в базисе B почти все булевы функции можно реализовать асимптотически оптимальными схемами с ненадежностью ε (при $\varepsilon \to 0$) тогда и только тогда, когда $G \cap B \neq \emptyset$.

Подобный критерий неизвестен для полных базисов, содержащих функции четырех переменных. Пусть T_4 – множество функций $f(x_1, x_2, x_3, x_4)$, из которых при отождествлении некоторых двух переменных (с последующим переименованием переменных) можно получить функцию множества G. Очевидно, что при наличие в базисе B функции из T_4, он является базисом B_ε.

С помощью ПЭВМ [7] найдены $|T_4| = 46672$, $|T_4 \cap \tilde{M}_4| = 2824$. А затем с помощью формулы вычислено значение $|T_4 \cup \tilde{M}_4| = 46980$. Отметим, что $2^{2^4} = 65536$, $|T_4 \cup \tilde{M}_4|/2^{2^4} = 0,7168579$.

Таким образом, 1) если базис содержит некоторую функцию из множества $\tilde{M}_k \cup T_4 \cup G_2 \cup G_3$ $(k \geq 3)$, то он является базисом B_ε, 2) чтобы в заданном базисе (не содержащем функцию из множества $\tilde{M}_k \cup T_4 \cup G_2 \cup G_3$) получить "хорошие" верхние оценки ненадежности схем для произвольных функций, следует искать схемы, реализующие функции из множества $\tilde{M}_k \cup T_4 \cup G_2 \cup G_3$ с наименьшими возможными вероятностями ошибок всего на двух наборах.

Работа выполнена при финансовой поддержке РФФИ, номер проекта 11-01-00212а.

Литература

1. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — № 6 (21), — 2005. — С. 42–55.
2. Алехина М.А. Синтез асимптотически оптимальных по надежности схем. Монография. – Пенза: Инф.-издат. центр ПГУ, 2006. — 156 с.
3. Алехина М.А. О надежности схем в базисах, содержащих медиану // Труды VIII международной конференции "Дискретные модели в теории управляющих систем". — М.: Издат. отдел ф-та ВМиК МГУ им. М. В. Ломоносова; МАКС Пресс, 2009. — С. 13–17.
4. Алехина М. А., Аксенов С. И., Васин А. В. О функциях и схемах, применяемых для повышения надежности схем // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — № 3. — 2008. — С. 30–38.

5. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // Ученые записки казанского государственного университета. Серия Физико-математические науки. — Казань: Изд-во Казанского университета, 2009. — Том 151, кн. 2. — С. 25–36.

6. Алехина М. А., Заваровский К. Ю., Спиридонов Н. С. О числе функций, используемых для повышения надежности схем // Труды международного симпозиума "Надежность и качество, 2008". — Пенза: ИИЦ ПГУ. — 2008. — Том 1. — С. 363.

7. Алехина М. А., Спиридонов Н. С., Черепанова О. Ю. О числе хороших функций // Материалы седьмой международной молодежной школы по дискретной математике и ее приложениям. — М.: Изд-во механико-матем. ф-та МГУ им. М. В. Ломоносова. — 2009. — С. 4–7.

8. Алехина М.А., Шилов А. В. Верхние оценки ненадежности схем в некоторых базисах при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — № 5 (26). — 2006. — С. 4–12.

9. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов. — Дисс. ... кандидата физ.-мат. наук. — Пенза, 2010. — 100 с.

10. von Neuman J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata studies, edited by Shannon C., Mc. Carthy J. Princeton University Press, 1956. (Русский перевод: Автоматы. — М.: ИЛ, 1956. — С. 68–139.)

11. Редькин Н.П. О полных проверяющих тестах // Математические вопросы кибернетики. — Вып. 2: Сборник статей / Под ред. С. В. Яблонского — М.: Наука, 1989. — С. 198–222.

12. Яблонский С.В. Введение в дискретную математику: Учеб. пособие для вузов. — М.: Высшая школа, 2001. — 384 с.

СОВЕРШЕННЫЕ РАСКРАСКИ И КОРРЕЛЯЦИОННО-ИММУННЫЕ ФУНКЦИИ В q-ЗНАЧНОМ ГИПЕРКУБЕ

В. Н. Потапов

Институт математики им. С. Л. Соболева СОРАН, Новосибирск, пр. Акад. Коптюга д.4

e-mail: vpotapov@math.nsc.ru

1. Совершенные раскраски

Пусть $E_q = \{0, 1, \ldots, q-1\}$. Обозначим через E_q^n множество упорядоченных q-ичных наборов (вершин) длины n (q-*значный* n-*мерный куб*). *Расстоянием Хэмминга* $d(x, y)$ между вершинами $x, y \in E_q^n$ называется число позиций, в которых наборы x и y различаются. *Шаром радиуса* ρ с центром в вершине $x \in E_q^n$ называется множество $B_\rho(x) = \{y \in E_q^n \mid d(x, y) \le \rho\}$. $L_\rho(x) = \{y \in E_q^n \mid d(x, y) = \rho\}$ — сфера радиуса ρ.

ρ-*Совершенным кодом* в E_q^n называется такое множество C, $|C| \ge 2$, что[1] $|C \cap B_\rho(x)| = 1$ для любого $x \in E_q^n$.

Утверждение 1. *Если в* E_q^n *имеется* ρ-*совершенный код, то число* $\nu(q, n) = \frac{q^n}{1+(q-1)\binom{n}{1}+\cdots+(q-1)^\rho\binom{n}{\rho}}$ *целое, где* $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Утверждение 2. *Множество* $C \subset E_q^n$ *является* ρ-*совершенным кодом тогда и только тогда, когда* $|C| = \nu(q, n)$ *и* $d(x, y) \ge 2\rho + 1$ *для любых различных* $x, y \in C$.

Заметим, что если $d(x, y) \ge 2\rho + 1$ для любых различных $x, y \in C$, то $|C| \le \nu(q, n)$.

Рассмотрим множество E_q^n как векторное пространство над полем $GF(q)$, где $q = p^s$ — степень простого числа. Код называется *линейным*, если он является аффинным подпространством в E_q^n.

Конструкция кода Хэмминга [13]

Пусть $q = 2$, $n = 2^t - 1$. Пусть β_i — двоичная запись длины t числа i, $i \in \{0, \ldots, 2^t - 1\}$. Пусть матрица $D_t = (\beta_1, \ldots, \beta_n)$ составлена из векторов $i = 1, \ldots, n$. Например, $D_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Утверждение 3. *Множество* $C = \{x \in E_2^n \mid D_t x = \overline{0}\}$ *является линейным* 1-*совершенным кодом.*

[1] Здесь и далее через $|C|$ обозначается мощность множества C.

Подобным образом можно построить линейный 1-совершенный код Хэмминга в E_q^n, где $q = p^s$ — степень простого, $n = \frac{q^t-1}{q-1}$.

Заметим, что при нечётном n множество $\{\overline{0}, \overline{1}\}$ является $(n-1)/2$-совершенным кодом в E_2^n. Такие коды называются тривиальными.

Теорема 1 (Зиновьев, Леонтьев, 1973 [3]; Тиетвайнен, 1973 [18]). *Нетривиальный совершенный код в E_q^n при $q = p^s$ (p — простое) должен иметь одни из следующих параметров*:

1) $q = p^s$, $\rho = 1$, $n = \frac{q^t-1}{q-1}$;
2) $q = 3$, $\rho = 2$, $n = 11$;
3) $q = 2$, $\rho = 2$, $n = 23$.

Коды с параметрами 2) и 3) построены М. Голеем [12]. Все коды с параметрами 2) и 3) являются линейными.

Проблема. *Существуют ли совершенные коды в гиперкубе E_q^n, если q — не степень простого числа?*

Через $|x| = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ обозначим *чётность* вершины $x \in E_2^n$.

Теорема 2 (Васильев, 1962 [2]). *Пусть $C \subset E_2^m$ — 1-совершенный код. Тогда множество $C_\lambda = \{(x, x \oplus y, |x| \oplus \lambda(y)) \mid x \in E_2^m, y \in C\}$, где $\lambda : C \to \{0,1\}$ — произвольная функция, является 1-совершенным кодом в E_2^{2m+1}.*

Доказательство. В соответствии с утверждением 2 достаточно доказать, что $|C_\lambda| = \frac{2^{2m+1}}{2m+2} = |C| \cdot 2^m$ и $d(z, z') \geq 3$ для любых $z, z' \in C_\lambda$. Первое сразу следует из определения кода C_λ, второе нетрудно получить непосредственной проверкой.

Из теоремы Васильева, сравнив число различных функций λ и число различных аффинных подпространств, нетрудно получить следующее

Утверждение 4. *Существуют нелинейные 1-совершенные коды.*

Дж. Шёнхейм [16] предложил подобную конструкцию для построения совершенных кодов в E_q^n, где $q = p^s$ — степень простого, $n = \frac{q^t-1}{q-1}$.

Совершенной раскраской куба E_q^n в k цветов называется отображение $Col : E_q^n \to \{1, \ldots, k-1, 0\}$, удовлетворяющее следующему условию: мощность пересечения $|Col^{-1}(i) \cap L_1(x)|$ зависит только от цветов i и $Col(x)$, но не от вершины $x \in E_q^n$. Каждой совершенной раскраске[2] соответствует матрица параметров $S = \{s_{ij}\}$, где s_{ij} — число вершин цвета j в сфере радиуса 1 с центром в вершине цвета i.

[2] Совершенные раскраски в два цвета также называются (c_0, c_1)-регулярными функциями [6].

Утверждение 5. *Множество $C \subset E_q^n$ является 1-совершенным кодом тогда и только тогда, когда χ^C — совершенная раскраска куба E_q^n в два цвета*[3] *с матрицей параметров* $\begin{pmatrix} 0 & n(q-1) \\ 1 & n(q-1)-1 \end{pmatrix}$.

Занумеруем вершины куба E_q^n. Определим $(0,1)$-матрицу $M(n,q) = \{m_{ij}\}$ так: $m_{ij} = 1$, если i-я и j-я вершины находятся на расстоянии 1, и $m_{ij} = 0$ в противном случае. Матрица $M = M(n,q)$ называется *матрицей смежности* куба E_q^n. Например, матрица смежности для E_2^2 имеет вид $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.

По произвольной раскраске Col куба E_q^n в k цветов определим матрицу F_{Col} размера $q^n \times k$, в которой i-я строка равна $\overline{e_j}$, если $Col(i) = j$. Наоборот, по любой $(0,1)$-матрице размера $q^n \times k$ с единственной единицей в каждой строке определяется раскраска куба в k цветов.

Теорема 3 (Августинович [14]). 1) *Если Col — совершенная раскраска куба E_q^n с матрицей S, то $MF_{Col} = F_{Col}S$.*

2) *Если для некоторой раскраски и матрицы S выполнено равенство $MF_{Col} = F_{Col}S$, то раскраска Col совершенная.*

Теорему Августиновича можно доказать непосредственной проверкой равенства в п. 1) и проверкой определения совершенной раскраски в п. 2). Теорема верна для произвольного регулярного графа.

Нетрудно доказать следующие утверждения о совершенных раскрасках и матрицах параметров.

Утверждение 6. *Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда $n(q-1)$ собственное число матрицы S.*

Для доказательства утверждения 6 достаточно заметить, что сумма элементов любой строки в матрице S равна мощности сферы $|L_1(x)|$ в E_q^n.

Утверждение 7. *Пусть S матрица параметров совершенной раскраски куба E_q^n, тогда собственные числа матрицы S являются собственными числами матрицы M смежности куба E_q^n.*

Доказательство. Пусть $v \in \mathbb{C}^k$ — собственный вектор матрицы S. Тогда $Sv = \lambda v$ и $MF_{Col}v = F_{Col}Sv = \lambda F_{Col}v$, причём $F_{Col}v \neq \overline{0}$, если $v \neq \overline{0}$. Таким образом, λ — собственное число матрицы M.

Утверждение 8. *Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — матрица параметров совершенной раскраски булева куба E_2^n. Тогда число $\frac{2^n b}{b+c}$ целое.*

[3] Здесь и далее через χ^C обозначается характеристическая функция множества C.

Для доказательства утверждения 8 достаточно заметить, что количества вершин разных цветов относятся друг к другу как b/c.

Для раскрасок в произвольное число цветов утверждение 8 можно обобщить следующим образом.

Утверждение 9. *Пусть S — матрица параметров совершенной раскраски E_q^n в k цветов. Тогда найдётся целочисленный вектор b размерности k удовлетворяющий условиям:*

(1) $Sb = n(q-1)b$; (2) $\sum\limits_{i=1}^{k} b_i = q^n$; (3) $s_{ij}b_j = s_{ji}b_i$ *для любых* $i, j \in \{1, \ldots, k\}$.

Утверждение 10. *Пусть* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *— матрица параметров совершенной раскраски булева куба E_2^n. Тогда существует совершенная раскраска булева куба E_2^{n+1} с матрицей параметров* $\begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix}$.

Для доказательства утверждения 10 заметим, что если $f : E_2^n \to \{0, 1\}$ — раскраска с матрицей параметров $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то раскраску куба E_2^{n+1} с требуемой матрицей параметров можно определить равенством

$$f'(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n).$$

Утверждение 11 (Конструкция удвоения). *Пусть $f : E_2^n \to E_2$ — совершенная раскраска булева куба с матрицей параметров* $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Тогда $g : E_2^{2n} \to E_2$, где $g(x, y) = f(x \oplus y)$, есть совершенная раскраска с матрицей параметров $2S$.*

Доказательство утверждения 11 получается непосредственной проверкой. Утверждение 11 можно обобщить следующим образом.

Утверждение 12. *Пусть* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *— матрица параметров совершенной раскраски булева куба E_2^n. Тогда существует совершенная раскраска с параметрами* $\begin{pmatrix} ta & tb \\ tc & td \end{pmatrix}$ *в E_2^{tn}.*

Следующая теорема обеспечивает свойство монотонности реализуемых параметров совершенных раскрасок в два цвета.

Теорема 4 (Августинович, Фрид [7]). *Для любой пары натуральных чисел b, c таких, что $\frac{b+c}{(b,c)} = 2^t$ найдётся такое $a_0 = a_0(b, c)$, что матрица* $\begin{pmatrix} a & b \\ c & a+b-c \end{pmatrix}$ *является матрицей параметров совершенной раскраски булева куба если и только если $a \geq a_0$.*

Теорема 5 (Шапиро, Злотник, 1959 [17]; Кротов, 2011 [14]). *Для любой совершенной раскраски* $Col : E^n \to \{1, \dots, k-1, 0\}$ *и* $t \in \mathbb{N}$ *мощность пересечения* $|Col^{-1}(i) \cap L_t(x)|$ *зависит только от цветов* i *и* $Col(x)$.

Доказательство. Без ограничения общности считаем, что $x = \overline{0}$. Пусть r_t — число вершин из $L_{t-1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$; l_t — число вершин из $L_{t+1}(\overline{0})$ смежных с одной вершиной из $L_t(\overline{0})$.

Пусть M_t — матрица смежности расстояний t в кубе E_q^n.

$$M_t M = M_{t+1} r_{t+1} + M_{t-1} l_{t-1},$$

$M_1 = M$, $M_0 = E$, $M_t = p_t(M)$.

$$M_t F_{Col} = p_t(M) F_{Col} = F_{Col} p_t(S).$$

F_{Col} — совершенная раскраска графа расстояний t по теореме 3.

По существу теорема 5 означает, что совершенная раскраска по расстоянию 1 всегда является совершенной раскраской по любому расстоянию. Из доказательства теоремы 5 можно извлечь более сильное утверждение.

Утверждение 13. *Если две совершенные раскраски по расстоянию* 1 *имеют одинаковую матрицу параметров* S*, то они имеют одинаковые матрицы параметров* $p_t(S)$ *как раскраски по расстоянию* t.

Подмножество $C \subseteq E_2^n$ называется *антиподальным*, если из $x \in C$ следует, что $x \oplus \overline{1} \in C$.

Утверждение 14. *Любой* 1*-совершенный код* $C \subseteq E_2^n$ *является антиподальным.*

Доказательство. Свойство антиподальности означает, что χ^C является совершенной раскраской по расстоянию n, причём вершины, находящиеся на расстоянии n, имеют одинаковый цвет. Таким образом, по утверждению 13 свойство антиподальности достаточно проверить для линейного 1-совершенного кода.

Теорема 6 (Августинович, 1995 [1]). *Пусть* C_1 *и* C_2 1*-совершенные коды в* E_2^n*. Если* $C_1 \cap L_{(n-1)/2}(\overline{0}) = C_2 \cap L_{(n-1)/2}(\overline{0})$*, то* $C_1 = C_2$.

Доказательство. Из утверждения 14 следует, что

$$C_1 \cap L_{(n+1)/2} = C_2 \cap L_{(n+1)/2}.$$

Тогда множество $C = (C_1 \cap B_{(n-1)/2}(\overline{0})) \cap (C_2 \cap B_{(n-1)/2}(\overline{1}))$ является 1-совершенным кодом по определению. Но из антиподальности совершенного кода имеем

$$C_2 \cap B_{(n-1)/2}(\overline{1}) = C \cap B_{(n-1)/2}(\overline{1}) = C_1 \cap B_{(n-1)/2}(\overline{1}),$$
$$C_2 \cap B_{(n-1)/2}(\overline{0}) = C \cap B_{(n-1)/2}(\overline{0}) = C_1 \cap B_{(n-1)/2}(\overline{0}).$$

Аналогичным образом можно доказать, что любая совершенная раскраска гиперкуба E_2^n при нечётном n восстанавливается по раскраске вершин среднего слоя $L_{(n-1)/2}(\overline{0})$.

Средний слой $L_{(n-1)/2}(\overline{0})$ гиперкуба и любое другое удовлетворяющее условию теоремы 6 называется *тестовым* для 1-совершенных кодов.

Проблема. *Найти тестовое множество меньшей мощности для* 1-*совершенных кодов.*

2. Корреляционно-иммунные функции

Будем рассматривать множество E_q как группу по $\bmod q$ и куб E_q^n как абелеву группу $E_q \times \cdots \times E_q$. Для $x, y \in E_q^n$ определим

$$\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n \pmod q.$$

Множество функций $f : E_q^n \to \mathbb{C}$ будем рассматривать как векторное пространство $\mathbb{V}$ над полем $\mathbb{C}$ со скалярным произведением

$$(f, g) = \frac{1}{q^n} \sum_{x\in E_q^n} f(x)\overline{g(x)}.$$

Пусть $\xi = e^{2\pi i/q}$. *Характером* группы E_q^n называется $\phi_z \in \mathbb{V}$, где $\phi_z(x) = \xi^{\langle x,z\rangle}$, $z \in E_q^n$. При $q = 2$ можно рассматривать векторное пространство над $\mathbb{R}$ или $\mathbb{Q}$, поскольку $\xi = -1$.

Непосредственно из определения характера нетрудно вывести следующие равенства.

Утверждение 15. 1) $\phi_z \cdot \phi_y = \phi_{z+y}$;

2) $\sum\limits_{j=0}^{q-1} \xi^{kj} = 0$ *при* $k \neq 0 \pmod q$;

3) $\sum\limits_{x\in E_q^n} \xi^{\langle x,z\rangle} = 0$ *при* $z \neq \overline{0}$.

Из утверждения 15 получаем

Утверждение 16. *Характеры образуют ортонормированный базис в* $\mathbb{V}$.

Преобразованием Фурье вектора f называется $\widehat{f}(z) = (f, \phi_z)$. Тогда $f(x) = \sum\limits_{z\in E_q^n} \widehat{f}(z)\phi_z(x)$.

В любом евклидовом пространстве справедливо *равенство Парсеваля*: $\sum\limits_{x\in E_q^n} |f(x)|^2 = \sum\limits_{z\in E_q^n} |\widehat{f}(z)|^2$.

Гранью размерности k называется подмножество куба E_q^n, состоящее из вершин с одинаковыми фиксированными значениями некоторых $n - k$ координат. В частности, *одномерная грань направления* i, проходящая через

вершину $(a_1, \ldots, a_n) \in E_q^n$, определяется как множество

$$\{(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) \mid x \in E_q\}.$$

Функция $f : E_q^n \to E_q$ называется *корреляционно-иммунной порядка* $n - m$, если для любого $a \in E_q$ величина $|f^{-1}(a) \cap \Gamma|$ не зависит от выбора m-мерной грани Γ.

Обозначим через $\mathrm{cor}(f)$ максимальный порядок иммунности функции f и через $wt(x)$ — число ненулевых координат набора $x \in E_q^n$.

Пример. Пусть $f(x_1, \ldots, x_n) = x_1 + \cdots + x_n \pmod q$, тогда $\mathrm{cor}(f) = n - 1$.

Утверждение 17. *Если f — корреляционно-иммунная функция порядка m, тогда $\widehat{f}(z) = 0$ при $0 < wt(z) \le m$.*

Доказательство. Рассмотрим $z = (z', \overline{0})$, $wt(z') \le m$.

$$\widehat{f}(z) = \frac{1}{q^n} \sum_{x \in E_q^n} f(x)\overline{\phi_z(x)} = \frac{1}{q^n} \sum_{x'} (\xi^{-\langle x', z' \rangle} \sum_{x''} f(x) \xi^{-\langle x'', \overline{0} \rangle}) =$$

$$= \frac{const}{q^n} \sum_{x'} \xi^{-\langle x', z' \rangle} = 0.$$

Утверждение 18. *Если $f \in \mathbb{V}$ такова, что $\widehat{f}(z) = 0$ при $0 \le wt(z) \le m$. Тогда $\sum\limits_{x \in \Gamma} f(x) = 0$ для любой грани Γ размерности $n - m$.*

Доказательство. Имеет место равенство $f(x) = \sum\limits_{wt(z) > m} \widehat{f}(z)\phi_z(x)$. Если $wt(z) > m$, то $\sum\limits_{x \in \Gamma} \phi_z(x) = 0$ для любой грани Γ размерности $n - m$.

Утверждение 19. *Если $f : E_q^n \to \{0, 1\}$ и $\widehat{f}(z) = 0$ при $0 < wt(z) \le m$, то f — корреляционно-иммунная функция порядка m.*

Доказательство. Из утверждения 18 следует, что величина $\sum\limits_{x \in \Gamma} f(x)$ не зависит от выбор грани Γ размерности $n - m$. Следовательно, число единиц функции во всех таких гранях одинаково.

Булеву функцию $f : E_2^n \to \{0, 1\}$ называют *уравновешенной*, если

$$|f^{-1}(0)| = |f^{-1}(1)|.$$

Теорема 7 (Фон-Дер-Флаасс, 2007 [11]). *Пусть $f : E_2^n \to \{0, 1\}$, f — неуравновешенная и $|f^{-1}(0)|, |f^{-1}(1)| \ne 0$. Тогда $\mathrm{cor}(f) < \frac{2n}{3}$.*

Доказательство. Пусть $c = |\{x \in E_2^n \mid f(x) = 0\}|$, $b = |\{x \in E_2^n \mid f(x) = 1\}|$, $c + b = 2^n$, $c \neq b$.

Определим функцию $g(x) = \begin{cases} -c, & \text{при } f(x) = 1, \\ b, & \text{при } f(x) = 0. \end{cases}$

Для любого $x \in E_2^n$ имеем $g^2(x) - (b-c)g(x) - bc = 0$.

Пусть $\widehat{f}(z) = 0$ при $0 < wt(z) \leq \frac{2n}{3} = m$. Тогда $\widehat{g}(z) = 0$ при $wt(z) \leq m$ и

$$\left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x)\right)\left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x)\right) = cb + (b-c)\left(\sum_{wt(z)>m} \widehat{g}(z)\phi_z(x)\right),$$

$$\sum_{z' \neq z''} \widehat{g}(z')\widehat{g}(z'')(-1)^{\langle x, z' \oplus z'' \rangle} = (b-c) \sum_{wt(z)>m} \widehat{g}(z)(-1)^{\langle x,z \rangle}.$$

Но $wt(z' \oplus z'') \leq 2n - wt(z') - wt(z'') < m$.

Утверждение 20. *Характеры $\phi_z(x)$ являются собственными векторами матрицы смежности куба E_q^n с собственными числами $(n-wt(z))(q-1)-wt(z)$.*

Доказательство.

$$M\phi_z(x) = \sum_{y, d(x,y)=1} \xi^{\langle y-x, z \rangle + \langle x, z \rangle} = \xi^{\langle x,z \rangle} \sum_{j=1}^{n} \sum_{k \neq 0} \xi^{k z_j} =$$

$$= ((n - wt(z))(q-1) - wt(z))\phi_z(x).$$

Утверждение 21. *Пусть $f : E_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда $f - \frac{b}{c+b}$ есть собственная функция матрицы смежности булева куба E_q^n с собственным числом $n(q-1) - (b+c)$.*

Утверждение 21 нетрудно доказать непосредственной проверкой.

Утверждение 22. 1) *Если $f : E_q^n \to \{0,1\}$ — совершенная раскраска с матрицей параметров $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $\widehat{f}(z) = 0$ при $wt(z) \neq 0, \frac{b+c}{q}$.*

2) *Если $\widehat{f}(z) = 0$ при $wt(z) \neq 0, s$ для некоторой функции $f : E_q^n \to \{0,1\}$, то f — совершенная раскраска.*

Доказательство. Пункт 1) следует из утверждений 16, 20 и 21. Докажем пункт 2). Функция $g = f + t$ является собственным вектором матрицы смежности гиперкуба E_q^n для некоторой константы $c \in \mathbb{Q}$. Пусть $g(x) = t$ и $b(x) = |L_1(x) \cap g^{-1}(1+t)|$. Тогда $b(x)(1+t) + (n(q-1) - b(x))t = \lambda t$, где λ — собственное число соответствующее характерам ϕ_z, $wt(z) = s$. Таким образом, число $b(x)$ не зависит от выбора $x \in E_q^n$.

Из утверждений 19 и 22 имеем

Утверждение 23. *Пусть* $f : E_q^n \to \{0,1\}$ — *совершенная раскраска с матрицей параметров* $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Тогда* $\mathrm{cor}(f) = \frac{c+b}{q} - 1$.

Из доказательства теоремы 8 видно, что если неуравновешенная булева функция имеет максимально возможную корреляционную иммунность, то её преобразование Фурье имеет ненулевые значения только в точках фиксированного веса. Тогда, используя утверждение 22, получаем следующую теорему.

Теорема 8 (Фон-Дер-Флаасс, 2007 [11]). *Пусть* $f : E_2^n \to \{0,1\}$ — *корреляционно-иммунная функция порядка* $\mathrm{cor}(f) = \frac{2n}{3} - 1$. *Тогда* f — *совершенная раскраска.*

Параметры совершенных раскрасок достигающих границы Фон-Дер-Флаасса: $\begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 5 \\ 3 & 3 \end{pmatrix}$.

С помощью конструкции удвоения (утверждение 11) можно построить совершенные раскраски, достигающие границы Фон-Дер-Флаасса, в гиперкубах сколь угодно большой размерности.

Пусть $f : E_q^n \to \{0,1\}$, будем называть *плотностью* $\varrho(f) = \frac{|\{x \in E_q^n \mid f(x)=1\}|}{q^n}$.

Теорема 9 (Фридман, 1992 [10]; Биербрауэр, 1995 [8]). *Для любой функции* $f : E_q^n \to \{0,1\}$ *справедливо неравенство* $\varrho(f) \geq 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Доказательство. Пусть $m = \mathrm{cor}(f)$, $\lambda(z)$ — собственное число, соответствующее характеру ϕ_z.

$$f(x) = \varrho(f) + \sum_{wt(z)>m} \widehat{f}(z)\phi_z(x), \ (f,f) = \varrho(f).$$

$$0 \leq (Mf, f) = \sum_{z',z''} \lambda(z')\widehat{f}(z')\widehat{f}(z'')(\phi_{z'}, \phi_{z''}) =$$

$$= \varrho^2(f)n(q-1) + \sum_{wt(z)>m} \lambda(z)|\widehat{f}(z)|^2 \leq$$

$$\leq \varrho(f)n(q-1) + ((n-(m+1))(q-1) - (m+1))(\varrho(f) - \varrho^2(f)). \quad (1)$$

Теорема 10 (Потапов, 2010 [4]). *Функция* $f : E_q^n \to \{1,0\}$ *является совершенной раскраской с параметром* $s_{11} = 0$ *тогда и только тогда, когда справедливо равенство* $\varrho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$.

Доказательство. Если функция f является совершенной раскраской в два цвета с параметром $s_{11} = 0$, то $(Mf, f) = 0$. Из утверждений 22 и 23 в цепочке неравенств (1) имеем равенства. Наоборот, если выполнено равенство $\varrho(f) = 1 - \frac{n(q-1)}{q(\mathrm{cor}(f)+1)}$, то в цепочке неравенств (1) имеем всюду равенства. Тогда по утверждению 22 функция f есть совершенная раскраска.

Следует отметить, что граница Биербрауэра – Фридмана достигается на счётчике чётности $S = \begin{pmatrix} 0 & n \\ n & 0 \end{pmatrix}$ и 1-совершенном коде $S = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix}$.

Частным случаем теоремы 10 является

Теорема 11 (Дельсарт, 1972 [9]; Пулатов, 1976 [5]; Остергард, Поттонен, Фелпс, 2010 [15]). *Булева функция f является характеристической функцией 1-совершенного кода тогда и только тогда, когда* $\mathrm{cor}(f) = \frac{n-1}{2}$, $\varrho(f) = \frac{1}{n+1}$.

Проблема. *Обобщить на q-значный гиперкуб теоремы* 7 *и* 8.

Проблема. *Существуют ли совершенные раскраски булева куба с матрицами параметров* $\begin{pmatrix} 1 & 23 \\ 9 & 15 \end{pmatrix}, \begin{pmatrix} 2 & 22 \\ 10 & 14 \end{pmatrix}, \begin{pmatrix} 3 & 21 \\ 11 & 13 \end{pmatrix}, \begin{pmatrix} 0 & 25 \\ 7 & 18 \end{pmatrix}$?

Литература

1. Августинович С. В. Об одном свойстве совершенных двоичных кодов // Дискретн. анализ и исслед. опер. — 1995. — Т. 2, № 1. — С. 4—6.
2. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. — 1962. — Вып. 8. — С. 337–339.
3. Зиновьев В. А., Леонтьев В. К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. — 1973. — Вып. 2. — С. 123–132.
4. Потапов В. Н. О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Сибирские электронные математические известия. — 2010. — Т. 7.— С. 372–382.
5. Пулатов А. К. О структуре плотно упакованных $(n, 3)$-кодов // Дискретный Анализ. — 1976. — Вып. 29. — С. 53–60.
6. Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. — 2002. — Вып. 11 — С. 91–148.
7. Фон-Дер-Флаасс Д. Г. Совершенные 2-раскраски гиперкуба // Сибирский математический журнал. — 2007. — Т. 48, № 4. — С. 923–930.
8. Bierbrauer J. Bounds on orthogonal arrays and resilient functions // Journal of Combinatorial Designs. — 1995. — V. 3. — P. 179–183.
9. Delsarte P. Bounds for unrestricted codes by linear programming // Philips Res. Reports. — 1972. — V. 27. — P. 272–289.

10. Friedman J. On the bit extraction problem // Proc. 33rd IEEE Symposium on Foundations of Computer Science. — 1992. — P. 314–319.

11. Fon-Der-Flaass D. G. A bound of correlation immunity // Siberian Electronic Mathematical Reports. — 2007. — V. 4. — P. 133–135.

12. Golay M. J. E. Notes on digital coding // Proc. IRE. — 1949. — V. 37. — P. 657.

13. Hamming R. W. Error detecting and error correcting codes // Bell System Tech. J. — 1950. — V. 29. — P. 147—160.

14. Krotov D. S. On weight distributions of perfect colorings and completely regular codes // Design, Codes and Cryptography. — 2011. — V. 61, №. 3. — P. 315–329.

15. Ostergard P. R. J., Pottonen O., Phelps K. T. The perfect binary one-error-correcting codes of length 15: Part II-Properties // IEEE Transactions on Information Theory. — 2010. — V. 56 — P. 2571–2582.

16. Schönheim J. On linear and nonlinear single-error-correcting q-nary perfect codes // Inform. and Control. — 1968. — V. 12, №. 1. — P. 23–26.

17. Shapiro G. S., Slotnik D. S. On the mathematical theory of error correcting codes // IBM Journal of Research Development. — 1959. — V. 3 — P. 68–72.

18. Tietäväinen A. On the nonexistance of perfect codes over finite fields // SIAM J. Appl. Math. — 1973. — V. 24— P. 88–96.

ВЫЧИСЛЕНИЕ НЕДООПРЕДЕЛЕННЫХ ФУНКЦИЙ

А. В. Чашкин

Московский государственный университет им. М. В. Ломоносова

e-mail: chashkin@inbox.ru

1. Недоопределенные функции

Пусть $\mathcal{P}(\mathbb{Z}_m)$ — множество всех непустых подмножеств множества $\mathbb{Z}_m$. Набор $\boldsymbol{\beta} = \{\beta_1, \ldots, \beta_n\}$ назовем недоопределенным m-ичным набором, если каждая его компонента $\beta_i \in \mathcal{P}(\mathbb{Z}_m)$. Набор $\boldsymbol{\alpha} \in \mathbb{Z}_m^n$ назовем доопределением недоопределенного набора $\boldsymbol{\beta}$, если $\alpha_i \in \beta_i$ для всех i. Множество $A \subseteq \mathbb{Z}_m^n$ назовем доопределением множества B недоопределенных m-ичных наборов, если для каждого недоопределенного набора $\boldsymbol{\beta}$ из B в A найдется элемент $\boldsymbol{\alpha}$, являющийся его доопределением.

Набор $\boldsymbol{k} = (k_1, k_2, \ldots, k_m)$ назовем характеристикой набора $\boldsymbol{\beta}$, если для каждого i число k_i равно количеству i-элементных компонент $\boldsymbol{\beta}$. На множестве недоопределенных наборов введем функцию I, показывающую степень определенности набора. Для набора $\boldsymbol{\beta}$ с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_m)$ положим

$$I(\boldsymbol{\beta}) = \log_2 \left(\left(\frac{m}{1}\right)^{k_1} \left(\frac{m}{2}\right)^{k_2} \cdots \left(\frac{m}{m}\right)^{k_m} \right),$$

т. е. чем сильнее определен набор $\boldsymbol{\beta}$, тем больше значение $I(\boldsymbol{\beta})$. Нетрудно видеть, что недоопределенный m-ичный набор $\boldsymbol{\beta}$ длины n с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_m)$ имеет ровно

$$1^{k_1} 2^{k_2} \cdots m^{k_m} = m^n 2^{-I(\boldsymbol{\beta})} \tag{1}$$

доопределений.

Функции из $\{0,1\}^n$ в $\mathcal{P}(\mathbb{Z}_m)$ будем называть n-местными недоопределенными m-ичными функциями. Функцию $h : \{0,1\}^n \to \mathbb{Z}_m$ назовем доопределением n-местной недопределенной m-ичной функции f, если вектор значений h является доопределением вектора значений f. Для недоопределенной m-ичной функции f через $I(f)$ обозначим значение введенной выше функции I на векторе значений f. Множество $D(f) = \{\boldsymbol{x} \in \{0,1\}^n \mid f(\boldsymbol{x}) \neq \mathbb{Z}_m\}$ назовем областью определения f. Размер области определения f обозначим через D_f. Легко видеть, что $D_f = k_1 + \cdots + k_{m-1}$, где $\boldsymbol{k} = (k_1, k_2, \ldots, k_m)$ — характеристика вектора значений f. Далее набор $\boldsymbol{k}$ будем называть характеристикой функции f.

Каждому элементу из $\mathbb{Z}_m$ поставим в соответствие набор из нулей и единиц длины $\lceil \log_2 m \rceil$, и далее под элементами из $\mathbb{Z}_m$ будем понимать соответству-

ющие им булевы наборы, а под функциями из $\{0,1\}^n$ в $\mathbb{Z}_m$ — функции из $\{0,1\}^n$ в $\{0,1\}^{\lceil \log_2 m \rceil}$. Будем рассматривать сложность вычисления функций из $\{0,1\}^n$ в $\mathcal{P}(\mathbb{Z}_m)$ схемами из функциональных элементов в базисе из всех двухместных булевых функций. Сложностью недоопределенной функции f назовем сложность самого простого ее доопределения.

Далее сложность вычисления недоопределенных функций рассматривается в "шенноновской" постановке, т. е. изучается сложность самой сложной функции среди всех тех функций f, для которых $I(f)$ ограничена сверху некоторой величиной.

2. Немного истории

Изучение сложности вычисления недоопределенных функций началось в работах Э. И. Нечипорука [4, 5], где впервые была применена простая и эффективная идея использования универсального множества, содержащего доопределения всех недоопределенных функций специального вида. Фактически Нечипорук рассмотрел частный случай с $m = 2$ и $I(f) \sim n$, для которого получил асимптотически неулучшаемый результат. Л. А. Шоломов [8] распространил этот результат на случай $m = 2$ и $I(f) \geq n \log_2^{1+\delta} n$, где δ — сколь угодно малое положительное число. Сделано это было при помощи инъективных и "почти инъективных" операторов, которые вкладывали область определения недоопределенной булевой функции в булев куб меньшей размерности, после чего задача сводилась к рассмотренному ранее случаю с $I(f) \sim n$. Шоломов рассматривал булевы наборы как двоичные чисел, а в качестве операторов использовал вычисление остатков от деления чисел на подходящие простые числа. Именно этим обстоятельством вызвано ограничение на размер области определения рассматриваемых им недоопределенных функций. Продолжая начатое в [7] изучение сложности систем недоопределенных булевых функций Шоломов в [9] получил решение для растущего m и $I(f) \sim n$. В своих работах Шоломов существенным образом опирался на разработанный О. Б. Лупановым [3] метод локального кодирования. Наконец в работах [1, 10] А. Е. Андреев получил окончательный результат (Теорема 1) сняв ограничения на величину $I(f)$. Это удалось сделать использовав вместо операторов Шоломова линейные булевы операторы [2], имеющие при малых значениях $I(f)$ линейную сложность.

Несмотря на то, что в своих работах Шоломов и Андреев использовали одни и те же результаты Нечипорука [5] и Лупанова [3], их методы вычисления недоопределенных функций существенно отличаются друг от друга. Приводимый ниже в доказательстве Теоремы 1 способ вычисления недоопределенных функций следует в основном по пути намеченному Шоломовым в [8], так как подход Андреева [10] выглядит более громоздким и менее прозрачным, требуя от читателя значительных усилий.

3. Основные результаты

Теорема 1. *Пусть f — n-местная недоопределенная m-ичная функция, $n \to \infty$ и $\log_2 m = o(\log_2 I(f))$. Тогда*

$$L(f) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)) + \mathcal{O}(n).$$

Утверждение теоремы следует из доказываемых ниже лемм 4, 7 и 8, в которых рассматривается вычисление недоопределенных функций с различными значениями $I(f)$.

Теорема 2. *Пусть $n \to \infty$. Множество $\{f_i\}$, состоящее из всех n-местных недоопределенных m-ичных функций с характеристикой $(k_1, k_2, \ldots, k_m)$ и $I(f_i) = R$, содержит такую функцию f, что*

$$L(f) \ge \frac{R}{\log_2 R}(1 + o(1)).$$

Теорема 2 доказывается стандартным мощностным методом [3], и ее неравенство легко следует из доказываемой ниже леммы 3.

Рассмотрим функцию Шеннона

$$L(n, m, R) = \max L(f),$$

где максимум берется по всем n-местным недоопределенным m-ичным функциям f с $I(f)$ не превосходящим R. Справедлива следующая теорема.

Теорема 3. *Пусть $n \to \infty$, $R \ge n$ и $\log_2 m = o(\log_2 R)$. Тогда*

$$L(n, m, R) = \frac{R}{\log_2 R}(1 + o(1)) + \mathcal{O}(n).$$

При $R \gg n \log_2 n$ утверждение теоремы 3 легко следует из теорем 1 и 2. Если же $R = \mathcal{O}(n \log_2 n)$, то справедливость теоремы следует из теоремы 1 и того факта, что среди функций с $I(f) = R$ найдется функция, существенно зависящая от n переменных.

4. Доопределения

Лемма 1. *Пусть $B = \{\boldsymbol{\beta}\}$ — множество всех недоопределенных m-ичных наборов длины n с $I(\boldsymbol{\beta}) \le R$. Тогда существует доопределение множества B, состоящее не более чем из $mn2^R$ наборов.*

Доказательство. Допустим, что любое N-элементное подмножество множества $\{0, 1, \ldots, m-1\}^n$ не является доопределением множества B. Тогда для каждого такого подмножества можно указать хотя бы один набор из B, для

которого в этом подмножестве нет доопределения. Поэтому число пар $(\boldsymbol{\beta}, A)$, где $\boldsymbol{\beta} \in B$, а A — N-элементное подмножество множества $\{0,1,\ldots,m-1\}^n$, таких, что в A нет доопределения $\boldsymbol{\beta}$, равно $\binom{m^n}{N}$. Так как B состоит менее чем из 2^{mn} элементов, то в B найдется такой набор $\boldsymbol{\beta}$, что более

$$\binom{m^n}{N} \Big/ 2^{mn}$$

N-элементных подмножеств множества $\{0,1,\ldots,m-1\}^n$ не содержат доопределение $\boldsymbol{\beta}$. С другой стороны, легко видеть, что для любого недоопределенного набора из B не более (см. (1))

$$\binom{m^n - m^n 2^{-R}}{N}$$

N-элементных подмножеств множества $\{0,1,\ldots,m-1\}^n$ не содержат его доопределение. Поэтому должно выполняться неравенство

$$\binom{m^n}{N} \Big/ \binom{m^n - m^n 2^{-R}}{N} < 2^{mn} \tag{2}$$

Оценивая левую часть (2), видим, что

$$2^{mn} > \frac{m^n \cdots (m^n - N + 1)}{(m^n - m^n 2^{-R}) \cdots (m^n - m^n 2^{-R} - N + 1)} \geq \left(\frac{m^n}{m^n - m^n 2^{-R}}\right)^N =$$
$$= \left(\frac{1}{1 - 2^{-R}}\right)^N \geq \left(1 + 2^{-R} + 2^{-2R}\right)^N \geq 2^{N(2^{-R}(1+2^{-R}))}.$$

Поэтому логарифмируя полученные неравенства, заключаем, что

$$N < mn2^R(1 + 2^{-R})^{-1} \leq mn2^R(1 - 2^{-R-1}) \leq mn2^R - 1. \tag{3}$$

Таким образом, из предположения, что любое N-элементное подмножество множества $\{0,1,\ldots,m-1\}^n$ не является доопределением множества B, следует неравенство (3). Поэтому при N больших или равных правой части (3) среди N-элементных подмножеств множества $\{0,1,\ldots,m-1\}^n$ найдется хотя бы одно доопределение множества B. Лемма доказана.

Лемма 2. *Пусть $B = \{\boldsymbol{\beta}\}$ — множество недоопределенных m-ичных наборов длины n таких, что $I(\boldsymbol{\beta}) \geq R$ и $I(\boldsymbol{\beta}') < R$, где $\boldsymbol{\beta}'$ — набор $\boldsymbol{\beta}$ без последней компоненты. Тогда существует доопределение множества B, состоящее не более чем из $nm^2 2^R$ наборов.*

Справедливость леммы 2 легко следует из леммы 1 и двух очевидных неравенств $2^{I(\boldsymbol{\beta}')} < 2^R$ и $2^{I(\boldsymbol{\beta})} \leq m2^{I(\boldsymbol{\beta}')}$.

Лемма 3. *Пусть $B = \{\boldsymbol{\beta}\}$ — множество всех недоопределенных m-ичных наборов длины n с характеристикой $\boldsymbol{k} = (k_1, k_2, \ldots, k_m)$ и $I(\boldsymbol{\beta}) = R$. Тогда любое доопределение множества B состоит не менее чем из 2^R наборов.*

Доказательство. Каждый недоопределенный набор из B имеет (1) ровно $m^n 2^{-R}$ доопределений. Поэтому число пар $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ таких, что $\boldsymbol{\beta} \in B$ и $\boldsymbol{\alpha} \in \mathbb{Z}_m^n$ и является доопределением β, равно $|B| m^n 2^{-R}$. Так как любые два m-ичных набора длины n являются доопределениями одного и того же числа недоопределенных наборов одинаковой характеристики $\boldsymbol{k}$, то каждый m-ичный набор длины n будет доопределением ровно $|B| 2^{-R}$ наборов из B. Следовательно, если множество A состоит менее чем из 2^R m-ичных наборов длины n, то оно содержит доопределения менее $|B|$ наборов и поэтому не может быть доопределением множества B. Лемма доказана.

5. Сильно определенные функции

Лемма 4. *Пусть $\log_2 I(f) \sim n$ и $\log_2 m = o(n)$. Тогда*

$$L(f) \leq \frac{I(f)}{\log_2 I(f)}(1 + o(1)).$$

Доказательство. Введем параметры R и k, значения которых определим позднее. Значения недоопределенной n-местной функции f запишем в таблице T_f из 2^k столбцов и 2^{n-k} строк, поставив в соответствие i-му столбцу таблицы двоичный набор $(\sigma_1, \ldots, \sigma_k)$, являющийся двоичным представлением числа $i-1$, а j-й строке — набор $(\sigma_{k+1}, \ldots, \sigma_n)$, являющийся двоичным представлением числа $j-1$. В таблице на пересечении i-го столбца и j-й строки поставим значение $f(\sigma_1, \ldots, \sigma_k, \sigma_{k+1}, \ldots, \sigma_n)$. Каждую строку таблицы представим в виде следующих друг за другом элементарных наборов $\boldsymbol{\beta}$, для каждого из которых, кроме быть может последнего, справедливы неравенства $I(\boldsymbol{\beta}) \geq R$ и $I(\boldsymbol{\beta}') < R$. Множество таких наборов разобьем на классы, поместив в класс P_{ij} наборы, начинающиеся в i-й и заканчивающиеся в j-й позициях. Нетрудно видеть, что число различных классов не превосходит величины 2^{2k-1}.

Из леммы 2 следует, что для множества элементарных наборов класса P_{ij} существует множество их доопределений, которое состоит не более чем из $2^k m^2 2^R$ наборов длины 2^k, в каждом из которых первые $i-1$ и последние $2^k - j$ компонент равны нулю. Следовательно, для множества всех элементарных наборов существует множество их доопределений $H = \{\boldsymbol{\alpha}\}$, которое состоит не более чем из $m^2 2^{2k-1}(2^k - 1)2^R$ наборов длины 2^k. Далее полагаем, что нулевой набор принадлежит H.

Преобразуем таблицу T_f, заменив в ней каждый элементарный набор $\boldsymbol{\beta}$ каким-либо его доопределением $\boldsymbol{\alpha}$ из H. Нетрудно видеть, что преобразованная таблица T_h будет таблицей значений некоторой n-местной функции h, являющейся доопределением функции f. Функцию h вычислим используя метод локального кодирования Лупанова [3].

Прежде всего оценим число наборов $\boldsymbol{\alpha}$, из которых состоит T_h. Заметим, что

$$I(f) = \sum_{\boldsymbol{\alpha}} I(\boldsymbol{\alpha}),$$

где сумма берется по всем наборам $\boldsymbol{\alpha}$, входящим в T_h. При этом число наборов с $I(\boldsymbol{\alpha}) < R$ не превосходит числа строк таблицы, т. е. не больше чем 2^{n-k}. Так как для каждого из оставшихся наборов $I(\boldsymbol{\alpha}) \geq R$, то очевидно, что их число не превосходит $I(f)/R$. Таким образом, общее наборов в T_h не превосходит

$$I(f)\Big/R + 2^{n-k}. \tag{4}$$

Перенумеруем наборы $\boldsymbol{\alpha}$ из H целыми числами от нуля до $m^2 2^{3k-1} 2^R - 1$, присвоив нулевому набору нулевой номер. Теперь из таблицы T_h построим вектор T следующим образом: в T_h заменим все наборы $\boldsymbol{\alpha}$ из H на которые разбиты ее строки их номерами $\boldsymbol{t}$ — двоичными наборами длины $p = \lceil \log_2 m^2 2^{3k-1} 2^R \rceil \leq 2\log_2 m + 3k + R$, и затем начиная с первой строки T_1 выпишем строки T_i новой таблицы одну за другой в виде вектора $T = T_1 \dots T_i \dots T_{2^{n-k}}$, где $T_i = \boldsymbol{t}_{i1} \dots \boldsymbol{t}_{ij} \dots \boldsymbol{t}_{il_i}$. Из (4) следует, что длина T удовлетворяет неравенству

$$\begin{aligned} |T| &\leq (I(f)/R + 2^{n-k})(2\log_2 m + 3k + R) = \\ &= I(f) + (2\log_2 m + 3k)(I(f)/R + 2^{n-k}) + 2^{n-k}R. \end{aligned}$$

При этом, так как значение функции I на любой строке таблицы T_h не превосходит $2^k \log_2 m$, нетрудно видеть, что каждый вектор T_i состоит не более чем из $q = \lceil 2^k \log_2 m / R \rceil$ номеров, а его длина $|T_i|$ не превосходит s, где

$$s \leq \frac{(2\log_2 m + 3k + R)(2^k \log_2 m + R)}{R}.$$

Положим $\boldsymbol{l} = (l_1, \dots, l_i, \dots, l_{2^{n-k}})$, где l_i — число номеров $\boldsymbol{t}_{ij}$ в векторе T_i, $\boldsymbol{r} = (r_1, \dots, r_i, \dots, r_{2^{n-k}})$, где r_i — номер позиции начиная с которой в векторе T располагается вектор T_i. Далее вектор T будем рассматривать как вектор значений $\lceil \log_2 |T| \rceil$-местной булевой функции t, а вектора $\boldsymbol{l}$ и $\boldsymbol{r}$ — как вектора значений функции $l : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 q \rceil}$ и функции $r : \{0,1\}^{n-k} \to \{0,1\}^{\lceil \log_2 |T| \rceil}$. Пусть $g : \{0,1\}^{\lceil \log_2 p \rceil} \to \{0,1\}^{2^k \lceil \log_2 m \rceil}$ — функция, преобразующая номер $\boldsymbol{t}$ в соответствующий ему вектор из H. Теперь покажем как при помощи функций t, l, r и g вычислить функцию h. Вычисляющую функцию h схему S представим в виде пяти независимых подсхем.

1. Подсхема S_1 вычисляет $\boldsymbol{y} = l(x_{k+1}, \dots, x_n)$ и $\boldsymbol{z} = r(x_{k+1}, \dots, x_n)$. Легко видеть, что

$$L(S_1) = \mathcal{O}\Big(\frac{2^{n-k}(\log_2 q + \log_2 |T|)}{n-k}\Big) = \mathcal{O}\Big(\frac{2^{n-k}\log_2 |T|}{n-k}\Big). \tag{5}$$

2. Подсхемы S_2 и S_3 по вычисленным значениям $\boldsymbol{y}$ и $\boldsymbol{z}$ находят вектор $T_i = \boldsymbol{t}_{i1} \ldots \boldsymbol{t}_{ij} \ldots \boldsymbol{t}_{il_i}$. Сначала подсхема S_2 вычисляет значения функции t на s последовательных наборах начиная с $\boldsymbol{z}$. Затем подсхема S_3 оставляет в вычисленном подсхемой S_2 векторе первые $\boldsymbol{y} \cdot p$ значений, заменяя оставшиеся нулями. Конструкции подобных схем подробно рассмотрены в [3], откуда следует, что

$$L(S_2) \le \frac{|T|}{\log_2 |T|}\Big(1 + o(1)\Big), \quad L(S_3) \le \mathcal{O}(s \log_2 s). \tag{6}$$

3. Подсхема S_4 вычисляет сумму $\sum_{j=1}^{l_i} g(\boldsymbol{t}_{ij})$ разбивая вычисленный подсхемой S_3 вектор на блоки длины $\lceil \log_2 p \rceil$, вычисляя значения функции g на каждом из этих блоков и складывая полученные значения. Нетрудно видеть, что

$$\begin{aligned} L(S_4) &= \mathcal{O}\Big(\frac{2^k \log_2 m (2^k \log_2 m / R + 1) m^2 2^{3k-1} 2^R}{\log_2 (m^2 2^{3k-1} 2^R)}\Big) = \\ &= \mathcal{O}\Big(\frac{(\log_2 m)^2 m^2 2^{5k} 2^R}{R(3k + 2\log_2 m + R)}\Big) = \mathcal{O}\Big(m^4 2^{5k} 2^R\Big). \end{aligned} \tag{7}$$

4. Подсхема S_5 по значениям переменных $x_1, \ldots, x_k$ выделяет из вычисленного подсхемой S_4 вектора $\sum_{j=1}^{l_i} g(\boldsymbol{t}_{ij})$ позицию, являющуюся значением $f(\boldsymbol{x})$. Нетрудно видеть, что

$$L(S_5) = \mathcal{O}\Big(2^k \log_2 m\Big). \tag{8}$$

Суммируя неравенства (5)–(8), видим, что

$$L(S) \le \frac{|T|}{\log_2 |T|}\Big(1 + o(1)\Big) + O\Big(\frac{2^{n-k} \log_2 |T|}{n-k} + m^4 2^{5k} 2^R + 2^k \log_2 m + s \log_2 s\Big), \tag{9}$$

где

$$|T| \le I(f) + (2\log_2 m + 3k)(I(f)/R + 2^{n-k}) + 2^{n-k} R.$$

Положим

$$\begin{aligned} k &= \lceil n - \log_2 I(f) + 2\log_2 \log_2 I(f) \rceil, \\ R &= \lfloor \log_2 I(f) - 4\log_2 m - 5k - 2\log_2 \log_2 I(f) \rfloor. \end{aligned}$$

Тогда, учитывая условия $\log_2 I(f) \sim n$ и $\log_2 m = o(n)$, имеем

$$\begin{aligned} R &\sim \log_2 I(f), \\ k &= o\big(\log_2 I(f)\big), \\ R + 4\log_2 m + 5k &\le \log_2 I(f) - 2\log_2 \log_2 I(f), \\ n - k &\le \log_2 I(f) - 2\log_2 \log_2 I(f), \\ |T| &\le I(f)(1 + o(1)), \\ s &= 2^{o(\log_2 I(f))}. \end{aligned} \tag{10}$$

Подставляя оценки из (10) в (9), после несложных преобразований получаем требуемую оценку сложности схемы S:

$$L(S) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)).$$

Лемма доказана.

6. "Почти" инъективные линейные операторы

Покажем, что для любого подмножества в $\{0,1\}^n$ найдется линейный булев оператор, действующий на большей части этого подмножества инъективно. Затем, используя такие операторы, оценим сложность средне и слабо определенных функций.

Лемма 5. *Пусть $A \subseteq \{0,1\}^n$, s — целое. Тогда существует линейный оператор $\mathcal{L} : \{0,1\}^n \to \{0,1\}^s$ такой, что*

$$|\{(\boldsymbol{x},\boldsymbol{y}) \,|\, \boldsymbol{x},\boldsymbol{y} \in A, \mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})\}| < 2^{-s-1}|A|^2.$$

Доказательство. Обозначим через $F(n,s)$ множество всех линейных операторов $\mathcal{L} : \{0,1\}^n \to \{0,1\}^s$. Очевидно, что $|F(n,s)| = 2^{ns}$. Так как для любых двух различных наборов $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\{0,1\}^n$ имеется ровно 2^{n-1} n-местных линейных функций f с нулевым свободным членом, значения которых на этих наборах совпадают, т. е. $f(\boldsymbol{x}) = f(\boldsymbol{y})$, то поэтому в $F(n,s)$ имеется 2^{ns-s} различных операторов $\mathcal{L}$ таких, что $\mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})$. Следовательно, величина

$$2^{-ns} \sum_{\boldsymbol{x},\boldsymbol{y} \in A} 2^{ns-s} < 2^{-s}|A|^2/2$$

является средним значением для числа таких пар $(\boldsymbol{x},\boldsymbol{y})$, на которых значения оператора из $F(n,s)$ одинаковы. Поэтому в $F(n,s)$ найдется оператор $\mathcal{L}$, для которого равенство $\mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})$ выполняется менее чем на $2^{-s-1}|A|^2$ парах $(\boldsymbol{x},\boldsymbol{y})$, $\boldsymbol{x},\boldsymbol{y} \in A$. Лемма доказана.

Лемма 6. *Пусть $A \subseteq \{0,1\}^n$, $s = \lfloor \log_2 |A| + k \rfloor$, где $k \ge 0$. Тогда существует линейный оператор $\mathcal{L} : \{0,1\}^n \to \{0,1\}^s$ такой, что*

$$|\{(\boldsymbol{x},\boldsymbol{y}) \,|\, \boldsymbol{x},\boldsymbol{y} \in A, \mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})\}| \le \frac{1}{2^k}|A|.$$

Доказательство. Из леммы 5 следует, что найдется такой линейный (n,s)-оператор $\mathcal{L}$, для которого равенство $\mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})$ выполняется не более чем на $2^{-s-1}|A|^2$ парах $(\boldsymbol{x},\boldsymbol{y})$ наборов из A. Так как $2^{m+1} \ge 2^k|A|$, то $2^{-s-1}|A|^2 \le \frac{1}{2^k}|A|$. Лемма доказана.

7. Средне определенные функции

Лемма 7. *Пусть* $\frac{1}{3}n \le \log_2 I(f) \ll n$ *и* $\log_2 m = o(\log_2 I(f))$. *Тогда*

$$L(f) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)).$$

Доказательство. Пусть $(k_1, k_2, \ldots, k_m)$ — характеристика f. Прежде всего заметим, что так как

$$\left(\frac{m}{m-1}\right)^{D_f} \le 2^{I(f)} = \left(\frac{m}{1}\right)^{k_1}\left(\frac{m}{2}\right)^{k_2}\cdots\left(\frac{m}{m}\right)^{k_m} \le m^{D_f}$$

и $\log_2 \frac{m}{m-1} = \frac{1}{m} + \mathcal{O}\left(\frac{1}{m^2}\right)$, то из неравенств

$$\log_2 D_f + \log_2\log_2 \frac{m}{m-1} \le \log_2 I(f) \le \log_2 D_f + \log_2\log_2 m$$

и условий леммы легко следует, что

$$D_f = \mathcal{O}(mI(f)), \tag{11}$$

$$\log_2 I(f) \sim \log_2 D_f, \tag{12}$$

$$D_f \ge \frac{2^{n/3}}{\log_2 m}. \tag{13}$$

Положим $k = 3\log_2 n + \log_2 m$. К области определения f применим лемму 6. В результате для $s = \lfloor \log_2 D_f + 3\log_2 n + \log_2 m \rfloor$ найдется такой линейный оператор $\mathcal{L} : \{0,1\}^n \to \{0,1\}^s$, что множество

$$B = \{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in D(f), \mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})\}$$

состоит не более чем из $D_f n^{-3} m^{-1}$ пар наборов. Далее введем недоопределенную s-местную функцию

$$g(\boldsymbol{y}) = \begin{cases} f(\boldsymbol{x}), & \text{если существует единственный } \boldsymbol{x} \in D(f) \text{ такой, что } \boldsymbol{y} = \mathcal{L}(\boldsymbol{x}), \\ \mathbb{Z}_m, & \text{в противном случае,} \end{cases}$$

для которой значения $g(\mathcal{L}(\boldsymbol{x}))$ не совпадают со значениями $f(\boldsymbol{x})$ не более чем на $2D_f n^{-3} m^{-1}$ наборах из $\{0,1\}^n$. Нетрудно видеть, что

$$\left(\frac{m}{m-1}\right)^{D_f(1-2n^{-3}m^{-1})} \le 2^{I(g)} \le m^{D_f}.$$

Следовательно,

$$\log_2 D_f + \log_2\left(1 - \frac{2}{n^3 m}\right) + \log_2\log_2 \frac{m}{m-1} \le \log_2 I(g) \le \log_2 D_f + \log_2\log_2 m.$$

Таким образом, в силу условий леммы и неравенств (12) и (13)

$$\log_2 I(g) \sim \log_2 I(f) \sim s.$$

Поэтому для вычисления функции g можно воспользоваться леммой 4. Из этой леммы следует существование такого доопределения $\hat{g}$ функции g, что

$$L(\hat{g}) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)).$$

Теперь заметим, что сложность линейного оператора $\mathcal{L}$ не превосходит n^2, и, следовательно, вычисление композиции $\hat{g} \circ \mathcal{L}$ асимптотически не сложнее вычисления функции $\hat{g}$:

$$L(\hat{g} \circ \mathcal{L}) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)).$$

Наконец определим на $\{0,1\}^n$ полностью определенную функцию $h(\boldsymbol{x})$ так, чтобы сумма $h(\boldsymbol{x}) + \hat{g}(\mathcal{L}(\boldsymbol{x}))$ была доопределением $f(\boldsymbol{x})$. Положим

$$h(\boldsymbol{x}) = \begin{cases} z, & \text{если } \boldsymbol{x} \in D(f), \text{ существует } \boldsymbol{y} \in D(f) \text{ такой,} \\ & \text{что } \mathcal{L}(\boldsymbol{y}) = \mathcal{L}(\boldsymbol{x}) \text{ и } z + \hat{g}(\mathcal{L}(\boldsymbol{x}) \in f(\boldsymbol{x}), \\ 0, & \text{в противном случае.} \end{cases}$$

Нетрудно видеть, что $h(\boldsymbol{x})$ отлична от нуля не более чем на $2D_f n^{-3} m^{-1}$ наборах из $\{0,1\}^n$. Поэтому вычисляя компоненты h в соответствии с их дизъюнктивными нормальными формами и учитывая условие $\log_2 m = o(n)$ с неравенством (11), имеем

$$L(h) = \mathcal{O}\Big(\frac{D_f n \log_2 m}{n^3 m}\Big) = \mathcal{O}\Big(\frac{I(f) n m \log_2 m}{n^3 m}\Big) = o\Big(\frac{I(f)}{\log_2 I(f)}\Big).$$

Лемма доказана.

8. Слабо определенные функции

Лемма 8. *Пусть* $\log_2 I(f) \le \frac{1}{2} n$ *и* $\log_2 m = o(\log_2 I(f))$. *Тогда*

$$L(f) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)) + \mathcal{O}(n).$$

Доказательство. К области $D(f)$ применим лемму 6 с $k = \log_2 D_f + 1$. В результате найдется такой линейный оператор $\mathcal{L} : \{0,1\}^n \to \{0,1\}^s$, что $s = \lfloor 2 \log_2 D_f + 1 \rfloor$ и при этом в области $D(f)$ нет таких элементов $\boldsymbol{x}$ и $\boldsymbol{y}$, что $\mathcal{L}(\boldsymbol{x}) = \mathcal{L}(\boldsymbol{y})$. Далее введем недоопределенную s-местную функцию

$$g(\boldsymbol{y}) = \begin{cases} f(\boldsymbol{x}), & \text{если существует } \boldsymbol{x} \in D_f \text{ такой, что } \boldsymbol{y} = \mathcal{L}(\boldsymbol{x}), \\ \mathbb{Z}_m, & \text{в противном случае.} \end{cases}$$

Нетрудно видеть, что $f(\boldsymbol{x}) = g(\mathcal{L}(\boldsymbol{y}))$ и $I(g) = I(f)$. Так как $s \sim 2\log_2 D_f$,

$$\log_2 D_f + \log_2\log_2 \frac{m}{m-1} \le \log_2 I(g) \le \log_2 D_f + \log_2\log_2 m$$

и $\log_2 \frac{m}{m-1} = \frac{1}{m} + \mathcal{O}\left(\frac{1}{m^2}\right)$, то $\log_2 I(g) \sim \log_2 D_f \sim s/2$ и при достаточно больших n имеет место неравенство $\log_2 I(g) \ge s/3$ и, следовательно, можно воспользоваться леммой 7. В силу этой леммы

$$L(g) \le \frac{I(f)}{\log_2 I(f)}(1 + o(1)). \tag{14}$$

Наконец заметим (см. например [6]), что для сложности линейного оператора $\mathcal{L}$ справедливо неравенство

$$L(\mathcal{L}) = \mathcal{O}\left(\frac{n(s + \log_2 n)}{\log_2 n}\right) = \mathcal{O}\left(\frac{n(\log_2 I(f) + \log_2 n)}{\log_2 n}\right). \tag{15}$$

Нетрудно видеть, что при $n \to \infty$ сумма правых частей неравенств (14) и (15) не превосходит $\frac{I(f)}{\log_2 I(f)}(1 + o(1)) + \mathcal{O}(n)$. Лемма доказана.

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508.

Литература

1. Андреев А. Е. О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискретная математика. — 1989. —Вып. 4. — С. 36–45.
2. Кричевский Р. Е. Сжатие и поиск информации. — М.: Радио и связь, 1989.
3. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования. — В кн.: Проблемы кибернетики. Вып. 14. — М.: Физматгиз, 1965. — С. 31–110.
4. Нечипорук Э. И. О топологических принципах самокорректирования. — В кн.: Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 5–102.
5. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. — 1965. — 163, 1. — С. 40–42.
6. Чашкин А. В. О сложности булевых матриц, графов и соответствующих им булевых функций // Дискретная математика. — 1994. — Вып. 2. — С. 43–73.
7. Шоломов Л. А. О функционалах, характеризующих сложность систем недоопределенных булевых функций. — В кн.: Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 123–140.

8. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов. — В кн.: Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.

9. Шоломов Л. А. Информационные свойства функционалов сложности для систем недоопределенных булевых функций. — В кн.: Проблемы кибернетики. Вып. 34. — М.: Наука, 1978. — С. 133–150.

10. Andreev A. E. Complexity of Nondetetministic Functions. BRICS Report Series, RS-94-2.

КОЛИЧЕСТВО ВЕРШИН НЕЯВНО ЗАДАННОГО ПОЛИЭДРА

А. Ю. Чирков

Нижегородский государственный университет им. Н.И.Лобачевского

e-mail: chir7@yandex.ru

Введение

Пусть R — множество вещественных чисел, Z — множество целых чисел, $\lfloor\alpha\rfloor$ — наибольшее целое число, не превосходящее α, $\lceil\alpha\rceil$ — наименьшее целое число, не меньше чем α.

Под полиэдром будем понимать множество решений конечной системы неравенств $P = \{x \mid Ax \le b\}$. Если не оговорено противное, то элементы матрицы A и компоненты вектора b суть целые числа ($A \in Z^{m\times d}$, $b \in Z^m$), ранг A равен d, и полиэдр P — телесен (т. е. содержит множество ненулевого объема).

Подматрицу матрицы A, расположенную на пересечении строк с номерами из I и столбцов с номерами из J, обозначим через A_{IJ}. При обозначении множеств строк (столбцов) используем следующие соглашения: $*$ — множество, содержащее все номера строк (столбцов); $\bar{I}$ — дополнение множества I до множества всех номеров строк (столбцов). Максимум из абсолютных значений миноров порядка k матрицы A обозначим через $\Delta_k(A)$.

Выпуклую оболочку точек из пересечения полиэдра P с целочисленной решеткой Z^d обозначим через P_I. Если полиэдр P ограничен или имеет рациональное описание, то P_I — полиэдр. Вопрос описания P_I является одним из основных в целочисленном линейном программировании. Здесь будет рассмотрен вопрос о количестве вершин P_I.

Число вершин полиэдра $P \subset R^d$, заданного системой из m неравенств, не превосходит $\xi(d,m) = \binom{m-\lceil\frac{d}{2}\rceil}{\lfloor\frac{d}{2}\rfloor} + \binom{m-\lceil\frac{d+1}{2}\rceil}{\lfloor\frac{d-1}{2}\rfloor}$ (см. [1]). Приведенная оценка достигается на полиэдрах, двойственных к циклическим (полиэдр называется циклическим, если все его вершины лежат на кривой $x_1 = t$, $x_2 = t^2, \ldots$, $x_d = t^d$). Таким образом, число вершин полиэдра оценивается сверху величиной, зависящей только от m и d.

В отличие от непрерывного случая, количество вершин неявно заданного полиэдра P_I нельзя ограничить функцией только от количества неравенств m и размерности d. Обозначим через ϕ_k числа Фибоначчи ($\phi_0 = \phi_1 = 1$, $\phi_k = \phi_{k-1} + \phi_{k-2}$ при $k \ge 2$). В [2] приведен пример треугольника T на плоскости, заданного системой неравенств $\phi_{2k}x_1 + \phi_{2k+1}x_2 \le \phi_{2k+1}^2 - 1$, $x_1 \ge 0$, $x_2 \ge 0$. Вершинами полиэдра T_I являются точки $(0,0)$, $(0,\phi_{2k+1})$, и $(\phi_{2j}, \phi_{2k+1} - \phi_{2j-1})$,

где $j = 1, \ldots, k+1$. Всего число вершин полиэдра T_I равно $k+3$.

1. Верхние оценки числа вершин P_I

Поскольку вершину полиэдра нельзя представить полусуммой других точек этого полиэдра, то из условий x — вершина P_I, а y — такая точка, что $2x - y \in P_I$, следует, что $x = y$. На этом замечании основано следующее понятие, введенное в работе [3]: множество $M \subseteq \{x|\ x \in Z^d, x \geq 0\}$ обладает *свойством разделенности*, если из условий $z,\ y \in M,\ 2z \geq y$ следует равенство $z = y$.

Для множества, обладающего свойством разделенности справедлива

Лемма 1 [3]. *Если координаты любой точки x множества M, обладающего свойством разделенности, удовлетворяют неравенствам $\psi_i \leq x_i \leq \omega_i$, $i \in \{1, 2, \ldots, d-1\}$, то $|M| \leq \prod_{i=1}^{d-1} \lceil \log_2 \frac{\omega_i+2}{\psi_i+1} \rceil$.*

Доказательство. Для набора t, составленного из $d-1$ неотрицательных целых чисел, определим множество точек

$$K(t) = \{x \in R^d \,|\, 2^{t_i}(\psi_i + 1) - 1 \leq x_i \leq 2^{t_i+1}(\psi_i + 1) - 2,\ i = 1, \ldots, d-1\}.$$

Покажем, что в множестве $K(t)$ содержится не более одной точки из M. Действительно, допустим, нашлись $x, y \in K(t) \cap M$ и $x_d \geq y_d$. Тогда $2x_d \geq y_d$, и $2x_i \geq 2(2^{t_i}(\psi_i + 1) - 1) \geq y_i$, при $i = 1, \ldots, d-1$. Неравенство $2x \geq y$ противоречит свойству разделенности M, а значит, в множестве $K(t)$ содержится не более одной точки из M.

Целые точки отрезка $[\psi, \omega]$ покрываются семейством отрезков вида

$$[2^t(\psi + 1) - 1,\ 2^{t+1}(\psi + 1) - 2],$$

где $t = 0, 1, \ldots, \lceil \log_2 \frac{\omega+2}{\psi+1} \rceil - 1$. Все точки множества M покрываются полосами $K(t)$, где компоненты наборов t для каждого $i = 1, \ldots, d-1$ удовлетворяют неравенству $0 \leq t_i \leq \lceil \log_2 \frac{\omega_i+2}{\psi_i+1} \rceil - 1$. Количество полос в покрытии равно $\prod_{i=1}^{d-1} \lceil \log_2 \frac{\omega_i+2}{\psi_i+1} \rceil$, тем самым лемма доказана.

Метод получения верхних оценок числа вершин, предложенный в [3], состоит в отображении множества вершин P_I в ограниченное множество, обладающее свойством разделенности. В качестве примера применения метода, следуя [3], получим верхние оценки количества вершин P_I.

Обозначим через $V(T)$ множество вершин полиэдра T, а через A' — матрицу $\begin{pmatrix} A & -b \\ 0 & -1 \end{pmatrix}$.

Положим $M = \{b - Ax \,|\, x \in V(P_I)\}$. Точки из M имеют неотрицательные целые компоненты, не превосходящие $d\Delta_{d+1}(A')$. Нетрудно убедиться,

что множество M обладает свойством разделенности и $|M| = |V(P_I)|$. Множество M удовлетворяет условиям леммы 1, и, следовательно, справедливо неравенство $|V(P_I)| \le \lceil \log_2(2 + d\Delta_{d+1}(A'))\rceil^{m-1}$.

При получении неравенства не использовался тот факт, что аффинная размерность множества M равна d. Следовательно, степень логарифма в оценке можно понизить. Возможность понижения степени в оценке показывает следующий комбинаторный результат [4] о количестве точек множества, лежащего на гиперплоскости, и обладающего свойством разделенности.

Лемма 2. *Пусть множество точек M обладает свойством разделенности и лежит на гиперплоскости $ax = b$ ($a \ge 0$). Если компоненты любой точки M по не превосходят ω, то $|M| \le d\lceil \log_2 d\rceil \lceil \log_2(2+\omega)\rceil^{d-2}$.*

Доказательство. Для $x \in M$ найдем j, при котором $a_j x_j = \max_{i=1}^{d} a_i x_i$. Из выбора j, равенства $ax = b$ и неотрицательности компонент векторов x и a следует $da_j x_j \ge b \ge a_j x_j$. Из полученных неравенств выводим $\lceil \frac{b}{da_j}\rceil \le x_j \le \lfloor \frac{b}{a_j}\rfloor$. Для $j \in \{1, \ldots, d\}$ определим множество

$$M(j) = \{x \in M \mid \lceil \frac{b}{da_j}\rceil \le x_j \le \lfloor \frac{b}{a_j}\rfloor\}.$$

Очевидно, $|M| \le \sum_{j=1}^{d} |M(j)|$. Множество $M(j)$ обладает свойством разделенности, как подмножество M.

Оценим количество элементов $M(j)$, используя лемму 1, перенумеровав предварительно компоненты так, чтобы j-я компонента стала первой. Поскольку $\frac{2+\lfloor \frac{b}{a_j}\rfloor}{1+\lceil \frac{b}{da_j}\rceil} \le d$, то $|M(j)| \le \lceil \log_2 d\rceil \lceil \log_2(2+\omega)\rceil^{d-2}$, и, значит, выполняется неравенство $|M| \le d\lceil \log_2 d\rceil \lceil \log_2(2+\omega)\rceil^{d-2}$, что и требовалось доказать.

В [5] предложен способ отображения множества вершин P_I в множества размерности d, обладающие свойством разделенности. Главная идея этого способа, применительно к ограниченному полиэдру P, состоит в покрытии P симплексами. В общем случае, полиэдр P представим как сечение в $d+1$-мерном пространстве конуса $K = \{x \in R^{d+1} \mid A'x \le 0\}$ гиперплоскостью $x_{d+1} = 1$.

Конус, натянутый на линейно независимую систему векторов, назовем *миниэдральным*. Покроем конус K миниэдральными конусами. Сечения миниэдральных конусов гиперплоскостью $x_{d+1} = 1$ образуют покрытие полиэдра P.

Пусть H — квадратная невырожденная матрица порядка d. Обозначим через $S(H)$ пересечение миниэдрального конуса, натянутого на столбцы H, с гиперплоскостью $x_d = 1$.

Лемма 3. *Пусть $H \in Z^{d\times d}$, $\det H \ne 0$, и элементы последней строки матицы H суть неотрицательные числа. Тогда справедливо неравенство $V(S(H)_I) \le d\lceil \log_2 d\rceil \lceil \log_2(2 + |\det H|)\rceil^{d-2}$.*

Доказательство. Пусть J — множество номеров столбцов матрицы H с нулевой последней компонентой. Нетрудно убедиться, что выполняется равенство $V(S(H)) = \{\frac{1}{h_{dj}} H_{*\{j\}} \,|\, j \in \bar{J}\}$ и конус рецессивных направлений $S(H)$ образован столбцами матрицы H с номерами из J. Пусть v — вершина $S(H)_I$. Поскольку $v \in S(H)$, то найдутся такие неотрицательные числа $\beta_1, \ldots, \beta_d$, что $v = \sum_{j \in \bar{J}} \frac{\beta_j}{h_{jd}} H_{*\{j\}} + \sum_{j \in J} \beta_j H_{*\{j\}}$ и $\sum_{j \in \bar{J}} \beta_j = 1$. При $j \in J$ выполнено неравенство $\beta_j < 1$, т. к. иначе, точки $v \pm H_{*\{j\}} \in S(H)_I$, что противоречит выбору v. Компоненты вектора $H^{-1}v$ равны либо β_j, при $j \in J$, либо $\frac{\beta_j}{h_{dj}}$, при $j \in \bar{J}$. В любом из этих случаев компоненты $H^{-1}v$ суть неотрицательные числа не превосходящие 1.

Положим $M = \{|det\, H| \cdot H^{-1}x \,|\, x \in V(S(H)_I)\}$. Множество M образовано точками с целыми (т. к. $|det\, H| \cdot H^{-1} \in Z^{d \times d}$) не отрицательными компонентами, не превосходящими $|det\, H|$. Множество точек M обладает свойством разделенности и лежит на гиперплоскости $\sum_{j=1}^{d} h_{dj} x_j = |det\, A|$. Воспользовавшись для оценки $|M|$ леммой 2, получим требуемое неравенство.

Задача покрытия острого конуса $K = \{x \in R^{d+1} \,|\, A'x \leq 0\}$ миниэдральными конусами сводится к задаче покрытия политопа симплексами. Положим $h \in R^{d+1}$ равным сумме строк матрицы A' и рассмотрим полиэдр $P' = \{x \in K \,|\, hx = -1\}$. Нетрудно убедиться, что полиэдр P' ограничен, и, следовательно, является политопом. Каждому симплексу S из покрытия политопа P' сопоставим миниэдральный конус C, являющийся конической оболочкой вершин S. Очевидно, что совокупность всех миниэдральных конусов, соответствующих симплексам из покрытия P', образует покрытие конуса K.

Не нарушая общности можно считать, что полиэдры P и P' имеют размерность d. Пусть v — вершина P', а F — множество граней размерности $d-1$ политопа P' не содержащих v. Через точку политопа P' проходит отрезок, соединяющий v с некоторой точкой грани $f \in F$. То есть, политоп P' покрывается пирамидами $conv(v \cup f)$, где $f \in F$. Задача покрытия симплексами пирамиды сводится к покрытию симплексами грани. Действительно, покрыв грань f симплексами, и добавив к каждому симплексу вершину v, получим покрытие симплексами пирамиды. Таким образом, задача покрытия симплексами политопа P' свелась к аналогичным задачам меньшей размерности. При покрытии симплексами грани f в качестве v выберем лексикографически наименьшую вершину, принадлежащую f (полиэдр P' считаем собственной гранью размерности d).

Рассмотрим симплекс S с вершинами $v_0, \ldots, v_d$ из покрытия P', построенного описанным выше способом. По построению, вершины $v_{d-i}, \ldots, v_d$, где $i = 0, \ldots, d$, лежат на i мерной грани g_i политопа P', причем, справедливо включение $g_i \subset g_{i+1}$, при $i = 1, \ldots, d-1$. Последнее включение означает, что грань g_i представляется в виде пересечения g_{i+1} с $d-1$ мерной гранью f_i политопа P'. Тем самым, симплексу S поставлена в соответствие последовательность $d-1$ мерных граней $f_1, \ldots, f_d$. Данное соответствие инъективно, так

как вершина v_i симплекса S является лексикографически минимальной среди вершин грани $\cap_{j=1}^{i} f_j$. Отметим полезный в дальнейшем факт, что вершина v_i принадлежит граням $f_1, \ldots, f_{i-1}$.

Политоп размерности d называется *простым*, если в каждой его вершине пересекается ровно d граней размерности $d-1$. Если политоп P' — простой, то количество симплексов в его покрытии не больше $d!|V(P)|$. Действительно, симплекс из покрытия определяется последовательностью $d-1$ мерных граней $f_1, \ldots, f_d$, причем все грани пересекаются в одной вершине. Количество различных таких наборов граней (с точностью до перестановок) совпадает с числом вершин P'. Поскольку количество гиперграней политопа P' не превосходит $m+1$, то число вершин P' не превосходит $\xi(d, m+1)$. Таким образом, количество симплексов в покрытии P' не больше $d!\xi(d, m+1)$. Если политоп P' не является простым, то в справедливости последней верхней оценки количества симплексов в покрытии легко убедиться, представив политоп P' как предел последовательности простых политопов, полученных из P' малым сдвигом гиперграней.

Для получения верхней оценки количества вершин P_I осталось оценить определитель матрицы $H \in Z^{(d+1)\times(d+1)}$, столбцы которой образованы ребрами миниэдрального конуса C из покрытия K. Поскольку ребро h конуса C является ребром K, то найдется такое d-элементное множество J номеров строк матрицы A', что $rg\, A'_{J*} = d$ и $A'_{J*}h = 0$. Вектор, i-я компонента которого равна $(-1)^i det\, A'_{J\,\{\bar{i}\}}$ при $i = 1, \ldots, d+1$, является базисом пространства решений однородной системы линейных уравнений $A'_{J*}x = 0$, и, следовательно, можно считать с точностью до знака h равным этому вектору. При таком выборе h справедливо $|A'_{k*}h| = |det A'_{J\cup\{k\}}| \le \Delta_{d+1}(A')$.

Из способа построения покрытия конуса K вытекает, что для любого миниэдрального конуса C из покрытия K найдется такая последовательность d-мерных граней $f_1, \ldots, f_d$ конуса K, что ребро $H_{*\{i\}}$ принадлежит граням $f_1, \ldots, f_{i-1}$. Возьмем в качестве f_{d+1} грань K, не содержащую ребро $H_{*\{d+1\}}$. Пусть I — множество номеров строк матрицы A', соответствующих граням $f_1, \ldots, f_{d+1}$. Произведение матриц $A_{I*}H$ — треугольная матрица, на главной диагонали которой стоят положительные целые числа, не превосходящие $\Delta_{d+1}(A')$. Следовательно, $|\det A_{I*}H| \le \Delta_{d+1}(A')^{d+1}$. Поскольку определитель матрицы A_{I*} — целое ненулевое число, то $|\det H| \le \Delta_{d+1}(A')^{d+1}$. Элементы последней строки матрицы H — неотрицательные числа (т. к. при задании K используется неравенство $x_{d+1} \ge 0$). Матрица H удовлетворяет условиям леммы 3, следовательно,

$$V(S(H)_I) \le (d+1)\lceil \log_2(d+1)\rceil \lceil \log_2(2 + \Delta_{d+1}(A')^{d+1})\rceil^{d-1}.$$

Поскольку полиэдры $S(H)$ (общим количеством не более $d!\xi(d, m+1)$) образуют покрытие P, то тем самым доказана

Теорема 1 [6]. *Пусть* $P = \{x \,|\, Ax \le b\}$, *где* $A \in Z^{m\times d}$, $b \in Z^m$. *Тогда* $|V(P_I)| \le (d+1)!\lceil \log_2(d+1)\rceil\, \xi(d, m+1) \lceil \log_2(2 + \Delta_{d+1}(A')^{d+1})\rceil^{d-1}$.

Максимальное расстояние между точками полиэдра P назовем диаметром полиэдра и обозначим через $d(P)$. Получим верхние оценки числа вершин полиэдра в зависимости от его диаметра. Для получения верхней оценки числа вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой, зависящей от диаметра политопа, потребуется лемма об аппроксимации неравенств.

Лемма 4. *Пусть $a \in R^d$, $\beta \in R$ и $\alpha \in R_+$. Тогда найдутся вектор $c \in Z^d$ и число $\gamma \in Z$, такие, что для любого вектора x с целыми компонентами, по модулю не превосходящими α,выполнены либо неравенства $ax \le \beta, cx \le \gamma$, либо $ax > \beta, cx > \gamma$. При этом $|c| \le (d+1)d^{\frac{d}{2}}\alpha^d$ и $|\gamma| \le (d+1)d^{\frac{d}{2}}\alpha^d$.*

Доказательство. Положим

$$M_1 = \{(-x, 1) \in Z^{d+1} | \, ax \le \beta, \ |x_i| \le \alpha, \ \text{где } i = 1, \ldots, d\},$$
$$M_2 = \{(x, -1) \in Z^{d+1} | \, ax > \beta, \ |x_i| \le \alpha, \ \text{где } i = 1, \ldots, d\}.$$

Построим конус $K \subset R^{d+1}$, заданный системой неравенств $xy \ge 0$, при $x \in M_1$, и $xy > 0$, при $x \in M_2$. Конус K не пуст, так как содержит вектор $(a, \beta)^T$. Замыкание конуса K обозначим через $\bar{K}$. Очевидно, что конус $\bar{K}$ — острый при $\alpha \ge 1$.

Для ребра g конуса $\bar{K}$ найдется d линейно независимых неравенств, обращающихся на этом ребре в равенство. То есть, найдутся такие точки $x_1, \ldots, x_d$ из $M_1 \cup M_2$, что $gx_i = 0$, где $i = 1, ..., d$. Поскольку вектор g образует фундаментальную систему решений системы линейных однородных уравнений с целыми коэффициентами, не превосходящими по абсолютной величине α, то можно считать компоненты g целыми числами, по абсолютной величине не превосходящими $d^{\frac{d}{2}}\alpha^d$ (верхняя оценка минора порядка d матрицы, составленной из коэффициентов неравенств). Вектор $(a, \beta)^T$ представим в виде конической комбинации $d+1$ ребер $g_1, \ldots, g_{d+1}$ конуса $\bar{K}$. Положим $c' = \sum_{i=1}^{d+1} g_i$ и $\gamma = c'_{d+1}$, $c = (c'_1, \ldots, c'_d)$. Очевидно, что $c' \in K$, а значит, вектор c и число γ удовлетворяют условиям леммы.

Пусть $P = \{x \,|\, Ax \le b\}$, где $A \in R^{m \times d}$, $b \in R^m$, и полиэдр P ограничен. Получим верхние оценки числа вершин выпуклой оболочки P_I в зависимости от диаметра полиэдра. Пусть $y \in P \cap Z^d$. Заменим каждое неравенство системы $Ax \le b - Ay$ на их аппроксимации, удовлетворяющие условиям леммы 4. В результате получим систему неравенств $Fx \le g$ с целочисленными коэффициентами, по абсолютной величине не превосходящими $(d+1)d^{\frac{d}{2}}d(P)^d$. Рассмотрим полиэдр $P' = \{x \,|\, Fx \le g, \ |x_i| \le d(P), \ \text{где } i = 1, ..., d\}$. По построению $y + \{P' \cap Z^d\} = P \cap Z^d$, и, следовательно, $|V(P'_I)| = |V(P_I)|$. Положим $F' = \begin{pmatrix} F & -g \\ 0 & -1 \end{pmatrix}$. Нетрудно убедиться в справедливости неравенства

$\Delta_{d+1}(F') \le (d+1)^{\frac{(d+2)^2}{2}} d(P)^{d^2+d}$. Из теоремы 1 выводим

$$|V(P_I)| \le (d+1)!\lceil\log_2(d+1)\rceil\, \xi(d, m+2d+1)\lceil\log_2(2+(d+1)^{\frac{(d+2)^3}{2}} d(P)^{d(d+1)^2})\rceil^{d-1}.$$

При фиксированной размерности d, полученная оценка имеет вид полинома со старшим членом $m^{d/2}\log_2^{d-1} d(P)$.

2. Достижимость верхних оценок

Положим $c \in Z^d$, $E_c = \begin{pmatrix} c_1 & c_2 & \dots & c_d \\ 0 & 1 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & 1 \end{pmatrix}$, $e = (1, 0, \dots, 0)^T$. Пусть $P = \{x \,|\, Ax \le b\}$ — простой политоп, $A \in Z^{m\times d}$, $b \in Z^m$, $rgA = d \le m$. Обозначим через $P(c,\alpha)$ политоп, получающийся из P аффинным преобразованием $x = \frac{1}{2d\delta\Delta_d(A)^2}(E_c y + \alpha e)$. Нетрудно получить явное описание $P(c,\alpha)$ как множества решений системы неравенств $AE_c y \le 2d\delta\Delta_d(A)^2 b - \alpha A_{*1}$. Положим $b' = 2d\delta\Delta_d(A)^2 b - \alpha A_{*1}$. Семейство политопов $P(c,\alpha)$, где $0 \le \alpha < \delta$, $\alpha \in Z$, и $c \in Z^d$, $c_1 = \delta$ и $0 \le c_i < \delta$ при $i \ge 2$, обозначим через $K_{P,\delta}$. Средним числом вершин назовем величину $\sigma(P,\delta) = \frac{1}{|K_{P,\delta}|}\sum_{T\in K_{P,\delta}} |V(T_I)|$.

С каждой вершиной w политопа P связан "угловой" полиэдр P_w, образованный неравенствами, которые обращаются в равенства в точке w. Множество номеров этих неравенств обозначим через J_w ($P_w = \{x \,|\, A_{J_w *} x \le b_{J_w}\}$). Покажем, что для полиэдра $P(c,\alpha) \in K_{P,\delta}$ имеет место равенство

$$V(P(c,\alpha)_I) = \cup_{w\in V(P)} V(P_w(c,\alpha)_I).$$

Действительно, пусть x — вершина $P_w(c,\alpha)_I$. Положим $y = b'_{J_w} - A_{J_w *}E_c x$. Полиэдр $P_w(c,\alpha)_I$ (в силу простоты P) является многогранником задачи групповой минимизации, и, следовательно, компоненты y не превосходят $|\det A_{J_w}E_c| = \delta|\det A_{J_w}|$. Покажем, что $x \in P(c,\alpha)$. Неравенства с номерами из J_w заведомо выполняются. Пусть $j \notin J_w$. Справедливо равенство $b'_j - A_{j*}E_c x = b'_j - A_{j*}A^{-1}_{J_w *}(b'_{J_w} - y)$. Компоненты вектора $a_{j*}A^{-1}_{J_w} y$ не превосходят $d\delta\Delta_d(A)$ и $b'_j - A_{j*}A^{-1}_{J_w} b'_{J_w} = 2d\delta\Delta_d(A)^2(b_j - A_{j*}w)$. Из простоты полиэдра P и условия $j \notin J_w$ вытекает неравенство $b_j - A_{j*}w \ge (\Delta_d(A))^{-1}$. Таким образом, $b'_j - A_{j*}E_c x > d\delta\Delta_d(A) > 0$, и включение $x \in P(c,\alpha)$ установлено. Поскольку x — вершина $P_w(c,\alpha)_I$ и $x \in P(c,\alpha)$, то x — вершина $P(c,\alpha)_I$. Тем самым доказано включение $\cup_{w\in V(P)} V(P_w(c,\alpha)_I) \subseteq V(P(c,\alpha)_I)$.

Для доказательства обратного включения рассмотрим вершину x полиэдра $P(c,\alpha)_I$. Найдется $u \in R^d$, что $u^\top x > u^\top y$ при всех $y \ne x$, $y \in P(c,\alpha) \cap Z^d$. Обозначим через w' вершину $P(c,\alpha)$, в которой достигается максимум линейной формы $u^\top x$. Положим $w = (2d\delta\Delta_d(A)^2)^{-1}(E_c w' + \alpha e)$. Точка w является вершиной P и $x \in P_w(c,\alpha)$. Если x не является вершиной $P_w(c,\alpha)_I$, то найдется вершина z полиэдра $P_w(c,\alpha)_I$, что $u^\top z \ge u^\top x$. По доказанному ранее, z

является вершиной $P(c,\alpha)_I$, что противоречит выбору u. Следовательно x — вершина выпуклой оболочки точек $P_w(c,\alpha)_I$ и равенство доказано.

Из проведенных рассуждений следует, что для любой вершины x полиэдра $P(c,\alpha)_I$ найдется ровно d номеров неравенств, $b'_j - a_{j*}E_c x < d\delta\Delta_d(A)$. Причем обратив эти неравенства в равенства, получим вершину $P(c,\alpha)$. Следовательно, все члены в правой части равенства попарно не пересекаются, и значит, $\sigma(P,\delta) = \sum_{w\in V(P)} \sigma(P_w,\delta)$.

Пусть $M = \{b'_{J_w} - A_{J_w*}E_c x \,|\, x \in P_w(c,\alpha)_I\}$, Λ — решетка, порожденная столбцами матрицы A_{J_w*}. Формула $y = b'_{J_w} - A_{J_w*}E_c x$ устанавливает взаимно однозначное соответствие между вершинами $P_w(c,\alpha)_I$ и M. Относительно решетки Λ множество точек Z^d разбивается на $|\det A_{J_w*}|$ смежных классов $\Lambda_x = x + \Lambda$. Если $p \in M$, то $p \in \Lambda_{b'_{J_w}}$. Обратно, если $p \in \Lambda_{b'_{J_w}}$, то найдется δ^{d-1} наборов c,α, при которых $p \in M$. Если $p \in \Lambda_{b'_{J_w}}$ и система неравенств $-p \le A_{J_w*}E_c x \le (d-1)p$ не имеет целочисленного решения, отличного от нулевого, то $p \in V(M)$. Количество векторов $f \in Z^d$, удовлетворяющих условиям $-p \le f \le (d-1)p$ и $f \in \Lambda_x$, обозначим через $h_x(p)$. Для каждого f, удовлетворяющего $-p \le f \le (d-1)p$ и $f \in \Lambda$, количество наборов c, при которых совместна в целых числах система уравнений $f = A_{J_w*}E_c x$, равно количеству решений сравнения $c_2u_2 + \ldots + c_du_d = u_1(\delta)$, где $f = A_{J_w*}u$. Пусть δ — простое число и $\delta > |\det A_{J_w*}|$. Тогда количество решений сравнения $c_2u_2 + \ldots + c_du_d = u_1(\delta)$ равно δ^{d-2}. Следовательно, $p \in V(M)$, не менее чем при $\delta^{d-2}(\delta - h_0(p))$ наборах c,α. Обозначим через H_z множество точек $\{p \in Z^d \,|\, p \ge 0,\ p \in \Lambda_z,\ h_0(p) \le \delta/2\}$. Справедливо неравенство $\sigma(P_w,\delta) \ge \frac{1}{2\delta}|H_{b'_{J_w}}|$.

В каждом смежном классе Λ_z найдется вектор x, удовлетворяющий неравенствам $0 \le x \le |\det A_{J_w*}|\mathbf{1}$. Положим $H'_z = \{x \in H_z \,|\, x \ge \Delta_d(A)\mathbf{1}\}$ и $U = \{p \,|\, p \ge \Delta_d(A)\mathbf{1},\ h_0(p) \le \delta/2\}$. Пусть вектор $y \in Z^d$ удовлетворяет неравенствам $0 \le y \le \Delta_d(A)\mathbf{1}$. Для произвольного $x \in H'_z$ вектор $x - y$ имеет неотрицательные компоненты, принадлежит Λ_{z-y} и $h_0(x-y) \le h_0(x)$. Следовательно, установлено включение $H'_z \subseteq y + H_{z-y}$. Для векторов $x, z \in Z^d$ найдется вектор $y \in Z^d$, удовлетворяющий условиям $0 \le y \le \Delta_d(A)\mathbf{1}$ и $x - z - y \in \Lambda$, и, значит, выполнено включение $H'_x \subseteq y + H_z$. Далее, U представляется в виде объединения H'_x по всем смежным классам Λ и, значит, $|U| \le |\det A_{J_w*}||H_z|$. Тем самым установлено неравенство $\sigma(P_w,\delta) \ge \frac{1}{2\delta|\det A_{J_w}|}|U|$.

Пусть z удовлетворяет неравенствам $0 \le z \le \Delta_d(A)\mathbf{1}$. Тогда для $p \ge \Delta_d(A)\mathbf{1}$ справедливы соотношения $h_0(p - \Delta_d(A)\mathbf{1}) \le h_0(p-z) \le h_z(p)$. Суммируя эти неравенства по всем смежным классам относительно Λ, получим неравенство $|\det A_{J_w*}|h_0(p - \Delta_d(A)\mathbf{1}) \le \prod_{i=1}^d (1 + dp_i)$, из которого вытекает $h_0(p) \le \frac{1}{|\det A_{J_w*}|}\prod_{i=1}^d (1 + dp_i + d\Delta_d(A))$. Положим

$$U' = \{p \,|\, p \ge \Delta_d(A)\mathbf{1},\ \prod_{i=1}^d (1 + dp_i + d\Delta_d(A)) \le \delta|\det A_{J_w} * |/2\}.$$

Очевидно, $U' \subseteq U$, и, значит, $\sigma(P_w, \delta) \geq \frac{1}{2\delta|\det A_{J_w*}|}|U'|$.

Положим $D = \{x \,|\, x \geq \Delta_d(A)\mathbf{1},\ \prod_{i=1}^{d}(1+dx_i+d\Delta_d(A)+d) \leq \delta|\det A_{J_w*}|/2\}$. Для любого $x \in D \cap Z^d$ точки куба $\{y \,|\, x \leq y \leq x+\mathbf{1}\}$ принадлежат U', следовательно, $|U'| \geq \int\cdots\int_D \partial x$. Обозначим через $\omega_d(t)$ многочлен $\sum_{i=1}^{d} \frac{(-1)^{i+1}t^{d-i}}{(d-i)!}$. Справедливо равенство

$$\int\cdots\int_D \partial x = \frac{\delta|\det A_{J_w*}|}{2d^d}\omega_d(\ln\delta|\det A_{J_w*}|(1+d+d\Delta_d(A))^{-d}),$$

из которого выводим $\sigma(P_w, \delta) \geq 0,25d^{-d}\omega_d(\ln(\delta(1+d+d\Delta_d(A))^{-d}))$. Тем самым установлено неравенство

$$\sigma(P, \delta) \geq 0,25d^{-d}|F_0(P)|\omega_d(\ln(\delta(1+d+d\Delta_d(A))^{-d})).$$

Положим $a_{ij} = m\,i^j - \sum_{k=1}^{m} k^j$, $b_i = m$, где $i = 1, 2, \ldots, m$, $j = 1, \ldots, d$. Политоп $C = \{x \,|\, Ax \leq b\}$ является двойственным к циклическому политопу, и, значит, является простым. Число вершин политопа C равно $\xi(d, m)$. Далее, элемент i-го столбца матрицы A не превосходит по абсолютной величине m^{i+1}, и, следовательно, по неравенству Адамара $\Delta_d(A) \leq d^{d/2}m^{d(d+3)/2}$. Тем самым установлено неравенство

$$\sigma(C, \delta) \geq 0,25d^{-d}\xi(d, m)\omega_d(\ln\delta - d^2(d+3)\ln(dm)).$$

При фиксированной размерности d и достаточно большом значении δ, правая часть неравенства ограничена полиномом от $\ln\delta$ и m, старший член которого равен $m^{\lceil d/2\rceil}\ln^{d-1}\delta$.

Литература

1. Бренстед А. Введение в теорию выпуклых многогранников. — М.: Мир, 1988.
2. Rubin D. S. On the unlimited number of faces in integer hulls of linear programs with a single constraint // Operations Research. — 1970. —- V. 18, № 5. —P. 940–945.
3. Шевченко В. Н. О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. —№ 2. — С. 133–134.
4. Веселов С. И., Чирков А. Ю. Оценки числа вершин целых полиэдров // Дискретный анализ и исследование операций. —2007. — Серия 2. — Том 14. — № 2. — С. 14–31.
5. Чирков А. Ю., Шевченко В. Н. О числе вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой // Нижегор. ун-т им. Н. И. Лобачевского. — Нижний Новгород, 1993. — 12 с. — Деп. в ВИНИТИ 29.07.93, № 2165–В93
6. Чирков А. Ю., Веселов С. И. О вершинах неявно заданных целых полиэдров. Часть 2 // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2008 — № 2. — С. 166–172.

СОДЕРЖАНИЕ