Нижегородский государственный университет им. Н.И. Лобачевского

На правах рукописи

ЗОЛОТЫХ Николай Юрьевич

# Расшифровка пороговых и близких к ним функций

01.01.09 – Дискретная математика и математическая кибернетика

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора физико-математических наук

Научный консультант
д. ф.-м. н., проф.
Шевченко В. Н.

Нижний Новгород – 2013

# Содержание

# Список обозначений

$\mathbb{N}$ — множество натуральных чисел;

$\mathbb{Z}$ — кольцо целых чисел;

$\mathbb{Q}$ — поле рациональных чисел;

$\mathbb{R}$ — поле вещественных чисел;

$E_k = \{0, 1, \ldots, k-1\}$;

$X^n$ — множество $n$-мерных арифметических векторов (рассматриваемых как строчки или как столбцы) с компонентами из $X$;

$X^{n\times m}$ — множество матриц размером $n \times m$ с элементами из $X$;

$\lfloor \alpha \rfloor$ — целая часть числа $\alpha$ (наибольшее целое, не превосходящее $\alpha$);

$\lceil \alpha \rceil$ — минимальное целое число, не меньшее $\alpha$;

$\log \alpha$ — логарифм $\alpha$ по основанию 2;

$\langle w \rangle$ — длина двоичного разложения рационального числа $w = \frac{u}{v}$, где $u \in \mathbb{Z}$, $v \in \mathbb{N}$: $\langle w \rangle = 1 + \lceil \log(u+1) \rceil + \lceil \log(v+1) \rceil$;

$\langle b \rangle$ — длина двоичного разложения вектора $b = (\beta_1, \ldots, \beta_n) \in \mathbb{Q}^n$: $\langle b \rangle = n + \langle \beta_1 \rangle + \cdots + \langle \beta_n \rangle$;

$\operatorname{Affdim} X$ — аффинная размерность множества $X \subseteq \mathbb{R}^n$;

$\operatorname{Conv} X$ — выпуклая оболочка векторов множества $X \subseteq \mathbb{R}^n$;

$\operatorname{Cone} X$ — коническая оболочка векторов множества $X \subseteq \mathbb{R}^n$ (множество всех линейных комбинаций с неотрицательными коэффициентами);

$\operatorname{Vol} X$ — $n$-мерный объем области $X \subset \mathbb{R}^n$;

$\operatorname{Area} X$ — площадь плоской фигуры $X \subset \mathbb{R}^2$;

$\operatorname{Vert} X$ — множество вершин области $\operatorname{Conv} X$;

$\det A$ — определитель квадратной матрицы $A$; $\det(a_1, a_2, \ldots, a_n)$ — определитель матрицы, составленной из столбцов $a_1, a_2, \ldots, a_n$;

$P(A, a_0) = \{x \in \mathfrak{F}^n : \ Ax \leq a_0\}$ — полиэдр в пространстве $\mathfrak{F}^n$, где $\mathfrak{F}$ — подполе поля $\mathbb{R}$, $A \in \mathfrak{F}^{l \times n}$, $a_0 \in \mathfrak{F}^l$; см. стр. 32;

$M(A, a_0) = P(A, a_0) \cap \mathbb{Z}^n$; см. стр. 32;

$N(A, a_0) = \operatorname{Vert} \operatorname{Conv} M(A, a_0)$; см. стр. 33;

$\mathfrak{P}(n, l, \gamma)$ — множество политопов $P \subseteq \mathbb{R}^n$, каждый из которых можно задать системой $l$ линейных неравенств с целочисленными коэффициентами, ограниченными по модулю величиной $\gamma$; см. стр. 33;

$\mathfrak{M}(n, l, \gamma) = \{P \cap \mathbb{Z}^n : \ P \in \mathfrak{P}(n, l, \gamma)\}$; см. стр. 33;

$\mathfrak{F}(M)$ — множество всех функций $f : M \to \{0, 1\}$, $M \in \mathfrak{M}(n, l, \gamma)$; см. стр. 33;
в частности, $\mathfrak{F}(E_2^n)$ — множество всех булевых функций $n$ переменных;

$M_\nu(f) = \{x \in M : \ f(x) = \nu\}$, $f \in \mathfrak{F}(M)$ $(\nu = 0, 1)$; см. стр. 33;

$P_\nu(f) = \operatorname{Conv} M_\nu(f)$ $(\nu = 0, 1)$; см. стр. 33;

$N_\nu(f) = \operatorname{Vert} P_\nu(f)$ $(\nu = 0, 1)$; см. стр. 34;

$K(f)$ — конус разделяющих функционалов пороговой функции $f \in \mathfrak{T}(M)$; см. стр. 35;

$Q(f) = \mathrm{Cone}\Big(M_0(f) - M_1(f)\Big)$; см. стр. 131;

$R_0(f) = P_0(f) + Q(f)$; см. стр. 131;

$R_1(f) = P_1(f) - Q(f)$; см. стр. 131;

$\mathfrak{F}_\nu(M)$ — множество функций $f$ из $\mathfrak{F}(M)$, для каждой из которых множество $M_\nu(f)$ можно описать некоторой системой линейных неравенств ($\nu = 0, 1$); см. стр. 33;

$\chi(n, \gamma) = (n+1)^{\frac{n+3}{2}}(\gamma\sqrt{n})^{n^2}$; см. стр. 37;

$\xi(n, m) = \binom{m-\lfloor\frac{n-1}{2}\rfloor-1}{\lfloor\frac{n}{2}\rfloor} + \binom{m-\lfloor\frac{n}{2}\rfloor-1}{\lfloor\frac{n-1}{2}\rfloor}$; см. стр. 38;

$\mathfrak{T}(M)$ — множество пороговых функций, заданных на $M$; см. стр. 35; в частности, $\mathfrak{T}(E_2^n)$ — множество булевых пороговых функций $n$ переменных;

$m_\nu(f)$ — пороговое $\nu$-число функции $f \in \mathfrak{F}_\nu(M)$ ($\nu = 0, 1$); см. стр. 34;

$\mathfrak{F}_\nu(M, h)$ — множество тех функций $f \in \mathfrak{F}_\nu(M)$, для которых $m_\nu(f) = h$ ($\nu = 0, 1$); см. стр. 45;

$\mathfrak{F}(M, h)$ — множество таких $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, что $\min\{m_0(f), m_1(f)\} \leq h$; см. стр. 76;

$\tau(\mathscr{A}, f)$ — количество обращений к оракулу при расшифровке алгоритмом $\mathscr{A}$ функции $f$; см. стр. 74;

$\tau_M(\mathscr{A}) = \max\limits_{f\in\mathfrak{F}'} \tau(\mathscr{A}, f)$ — оракульная сложность алгоритма $\mathscr{A}$, где $\mathfrak{F}' \subseteq \mathfrak{F}(M)$; если $M$ ясно из контекста, то вместо $\tau_M(\mathscr{A})$ иногда используется $\tau(\mathscr{A})$; см. стр. 75;

$\rho(\mathscr{A}, f)$ — количество операций при расшифровке алгоритмом $\mathscr{A}$ функции $f$; см. стр. 74;

$\rho_M(\mathscr{A}) = \max\limits_{f\in\mathfrak{F}'}\rho(\mathscr{A},\ f)$ — вычислительная трудоемкость алгоритма $\mathscr{A}$, где $\mathfrak{F}' \subseteq \mathfrak{F}(M)$; если $M$ ясно из контекста, то вместо $\rho_M(\mathscr{A})$ иногда используется $\rho(\mathscr{A})$; см. стр. 74;

$\tau(\mathfrak{F}') = \min\limits_{\mathscr{A}}\tau_M(\mathscr{A})$ — оракульная сложность расшифровки функции в классе $\mathfrak{F}'$; см. стр. 113;

$\sigma(\mathfrak{F}', f)$ — мощность наименьшего разрешающего множества функции $f$ относительно класса $\mathfrak{F}'$; см. стр. 113;

$\sigma(\mathfrak{F}') = \max\limits_{f\in\mathfrak{F}'}\sigma(\mathfrak{F}', f)$ — длина обучения в классе $\mathfrak{F}'$; см. стр. 113;

$\overline{\sigma}(\mathfrak{F}') = \dfrac{1}{|\mathfrak{F}'|}\sum\limits_{f\in\mathfrak{F}'}\sigma(\mathfrak{F}', f)$ — средняя мощность минимального разрешающего множества в $\mathfrak{F}'$; см. стр. 114;

$\tau(M) = \tau\big(\mathfrak{T}(M)\big)$;

$\sigma(f) = \sigma\big(\mathfrak{T}(M),\ f\big)$;

$\sigma(M) = \sigma\big(\mathfrak{T}(M)\big)$;

$\overline{\sigma}(M) = \overline{\sigma}\big(\mathfrak{T}(M)\big)$; см. стр. 115;

$T(f)$ — минимальное разрешающее множество для $f \in \mathfrak{T}(M)$; см. стр. 121;

$T_\nu(f) = T(f) \cap M_\nu(f)$ $(\nu = 0, 1)$; см. стр. 121;

$\mathfrak{G}_1$ — задача построения множеств крайних точек $N_\nu(f)$ и всех неравенств–граней политопа $P_\nu(f)$ для функции $f \in \mathfrak{F}_\nu(M)$; см. стр. 44;

$\mathfrak{G}_2$ — задача построения минимального разрешающего множества $T(f)$ для функции $f \in \mathfrak{T}(M)$; см. стр. 153;

$\mathscr{A}_0$ — алгоритм расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$; см. стр. 84;

$\mathscr{A}_1$ — алгоритм расшифровки в классе $\mathfrak{T}(M)$; см. стр. 95;

$\mathscr{A}_1^+$ — вспомогательный алгоритм при построении $\mathscr{A}_1$; см. стр. 91;

$\mathscr{A}_1'$ — модификация алгоритма $\mathscr{A}_1$; см. стр. 97;

$\mathscr{A}_1^{\mathrm{o}}$ — модификация алгоритма $\mathscr{A}_1$; см. стр. 154;

$\mathscr{A}_2$ — алгоритм расшифровки в классе $\mathfrak{T}(E_p \times E_q)$; см. стр. 104;

$\mathscr{A}'$ — алгоритм расшифровки в классе $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$ [104]; см. стр. 79;

$\mathscr{A}''$ — алгоритм расшифровки в классе $\mathfrak{T}(E_k^n)$ [139]; см. стр. 96;

$\mathscr{A}_{\mathrm{ext}}$ — алгоритма расшифровки пороговой функции, заданной расширенным оракулом; см. стр. 109;

$\mathscr{A}_{\mathrm{опт}}$ — оракульный алгоритм максимизации линейной функции на множестве $M_\nu(f)$, где $f \in \mathfrak{F}_{1-\nu}(M)$; см. стр. 81;

DDM — «метод двойного описания» — алгоритм построения множества всех экстремальных лучей полиэдрального (многогранного) конуса [153]; см. стр. 60;

DDM.M1 — модификация алгоритма DDM; см. стр. 62;

Graph.Adj — «графовая модификация» комбинаторного теста проверки смежности экстремальных лучей; см. стр. 67;

∎ — конец доказательства.

Другие обозначения вводятся в тексте.

Если вектор умножается слева на матрицу, он считается столбцом, если справа — строкой. Равенства и неравенства между векторами понимаются в координатном смысле.

# Введение

В работе исследуется задача расшифровки функций, определенных на множестве целочисленных решений заданной системы линейных неравенств и обладающих определенными свойствами линейной отделимости. В частности, с этой точки зрения изучается класс пороговых функций $k$-значной логики, принимающих значения $0, 1$.

Очевидно, что в общем случае для однозначного определения функции, определенной на конечном множестве $M$ и принимающей значения $0, 1$, необходимо знать ее значения во всех точках области определения. Если же функция принадлежит классу $\mathfrak{F}'$, более узкому, чем множество всех таких функций, то для однозначного определения ее значений во всех точках $M$ иногда достаточно знать значения лишь на некотором его подмножестве. Задача расшифровки в классе $\mathfrak{F}'$ ставится следующим образом. С помощью вопросов о значении неизвестной функции $f$ требуется определить $f(x)$ для всех $x$ из множества $T \subseteq M$, которое бы позволило определить $f(x)$ для остальных точек области определения $M$. Предполагается, что выбор очередного вопроса определяется ответами на предыдущие. Таким образом, мы имеем дело с «черным ящиком», реализующим функцию из $\mathfrak{F}'$. Требуется определить, какую именно функцию он реализует.

Естественной мерой сложности алгоритмов расшифровки служит число вопросов, которые приходится задавать в худшем случае. Алгоритм минимальной сложности, решающий поставленную задачу для класса $\mathfrak{F}'$, назовем оптимальным. Сложность оптимального алгоритма назовем сложностью расшифровки в классе $\mathfrak{F}'$.

Впервые исследуемая задача рассматривалась В. К. Коробковым и Т. Л. Резником [47, 49, 51] для класса монотонных булевых функций. По-

строив специальный алгоритм и доказав его оптимальность, Ж. Ансель [134] окончательно установил сложность расшифровки таких функций. Н. А. Соколов [79] для поставленной задачи дал алгоритм, являющийся оптимальным как по числу вопросов, так и по требуемой памяти. Расшифровка монотонных многозначных и конечнозначных функций рассматривалась В. К. Коробковым, В. Б. Алексеевым, Н. А. Соколовым, А. В. Сержантовым, А. А. Сапоженко, М. В. Горяиновым [2, 14, 48, 73, 74, 78] и др. Близкая задача поиска максимального верхнего нуля монотонной функции рассматривалась в работах [43–45, 70, 76, 77]; см. также [50, 75, 80]. Другие сведения о монотонных функциях и задаче расшифровки монотонных функций приведены в обзоре А. Д. Коршунова [54]. Задачам расшифровки в различных классах функций посвящены многочисленные работы; упомянем [13, 65, 66, 98, 99].

Задача расшифровки пороговой функции впервые была поставлена В. Н. Шевченко [104]. Пороговые функции возникают во многих разделах математической кибернетики и дискретной математики и приложениях, например, в дискретной оптимизации [81, 105], распознавании образов [19, 20, 152], теории графов [18], при синтезе схем из функциональных элементов [57, 58, 64], нейронных сетей [83, 116], в цифровой обработке сигналов [3, 4, 163], машинном обучении [125, 152]. Обстоятельный обзор результатов по пороговым булевым функциям и пороговым представлениям булевых функций содержится в [39].

Пороговой функцией $k$-значной логики называется такое отображение $f$ гиперкуба $E_k^n = \{0, 1, \ldots, k-1\}^n$ в множество $\{0, 1\}$, что существует гиперплоскость, разделяющая множества нулей и единиц функции (точек, в которых $f(x)$ равна 0 или 1 соответственно). В [104] было показано, что для однозначного задания такой функции достаточно знать ее значения в вершинах выпуклых оболочек множеств нулей и

единиц. Установленная В. Н. Шевченко [103] оценка числа этих вершин позволила в [104] построить алгоритм расшифровки пороговой функции, сложность которого при любом фиксированном числе переменных $n$ ограничена некоторым полиномом от $\log k$. Этот алгоритм опирается на процедуру, предложенную В. Н. Шевченко [102] нахождения вершин выпуклой оболочки множества целочисленных решений системы линейных неравенств. В свою очередь эта процедура использует алгоритм Ленстры (H. W. Lenstra) [147] решения таких систем. Данный подход оказался достаточно эффективным и развивался в работах [107, 138] и др. Улучшение верхних оценок сложности алгоритмов расшифровки пороговых функций происходило в этих работах за счет уточнения [10, 95, 97, 102, 105, 127] верхних оценок числа крайних точек. Хегедус (T. Hegedüs) [138] показал, что сложность алгоритма В. Н. Шевченко при фиксированном $n$ есть $O(\log^{\lfloor n/2 \rfloor (n-1)+n} k)$. Дальнейший прогресс на этом пути, по-видимому, не возможен, так как установленная в [127] оценка не улучшаема по порядку [8, 94, 119].

Близкие вопросы рассматриваются в [121, 122, 131, 145, 149, 150] и др.

Основной из известных ранее результатов о нижней оценке сложности расшифровки пороговой функции $k$-значной логики — о невозможности построения алгоритма расшифровки полиномиальной от $n$ сложности [104]. Это заставляет, с одной стороны, искать алгоритмы полиномиальной при фиксированном $n$ сложности (так называемые квазиполиномиальные алгоритмы), а, с другой стороны, пытаться установить более точные нижние оценки, явным образом включающие параметр $k$. Диссертантом получены результаты в обоих направлениях. С одной стороны, предлагается алгоритм расшифровки, сложность которого при фиксированном $n \geq 2$ есть $O(\log^{n-1} k)$. С другой стороны, получена ниж-

няя оценка сложности этой задачи $\Omega(\log^{n-2} k)$.

Нижняя оценка получена на основе анализа структуры и мощности так называемого разрешающего множества [49, 51] пороговой функции — такого множества точек области определения, значений в которых достаточно для однозначного восстановления $f$ в остальных точках, т. е. для однозначной идентификации $f$. Максимальное значение мощности минимального разрешающего множества (где максимум берется по всем функциям из класса $\mathfrak{F}'$) длиной обучения (teaching dimension [132]) в классе $\mathfrak{F}'$. На основе результатов [104, 127] в [138] показано, что длина обучения в классе пороговых функции $k$-значной логики при фиксированном $n$ есть $O(\log^{n-1} k)$. Диссертантом предложена новая характеризация минимального разрешающего множества и на этой основе при фиксированном $n$ установлена оценка длины обучения $\Theta(\log^{n-1} k)$. Для $n = 2$ длина обучения равна 4.

В [117] исследуется среднее значение мощности минимального разрешающего множества. Установлено, что мощность минимального разрешающего множества булевой пороговой функции в среднем не превосходит $n^2$. Этот результат может быть обобщен [12] на случай $k$-значной логики. В этом случае справедлива верхняя оценка $n^2 \log k$. Для $n = 2$ среднее значение мощности минимального разрешающего множества асимптотически равно $\frac{7}{2}$.

Дальнейшие исследования разрешающих множеств пороговых функций, возможно, позволят получить новые результаты, касающиеся мощностных свойств класса пороговых функций $k$-значной логики.

Заметим, что задача оценки числа дискретных функций различных классов, как правило, является весьма сложной. Задача оценки мощности пороговых булевых функций исследуется с середины 1960-х гг. Верхняя оценка получается из классического результата Л. Шлёфли [14] о чис-

ле открытых областей, получаемых при разбиении $n$-мерного пространства гиперплоскостями. С. Яджима и Т. Ибараки [166] получили первую нетривиальную нижнюю оценку. Асимптотика логарифма числа пороговых функций была установлена только в 1989 г. Ю. А. Зуевым [37, 38]. При этом использовался один комбинаторно-вероятностный результат о $\pm 1$-матрицах, полученный А. М. Одлыжко [157]. Другой подход к получению асимптотики логарифма числа пороговых функций, также использующий лемму Одлыжко, предложил А. А. Ирматов [40]. Асимптотика самого числа пороговых функций до сих пор не известна. Обстоятельный обзор результатов по пороговым булевым функциям и пороговым представлениям булевых функций содержится в [39]. Мощность множества пороговых функций $k$-значной логики исследовалась в [103, 105]. Асимптотика логарифма числа пороговых функций $k$-значной логики установлена А. А. Ирматовым и Ж. Д. Ковиянич [42].

Другим примером может служить проблема Дедекинда — оценка числа монотонных булевых функций, как известно, сильно связанная с задачей расшифровки в этом классе [49, 134]. В. К. Коробковым [49], а также Ж. Анселем [134] найден порядок логарифма числа этих функций. Д. Клейтмен [143] установил асимптотику логарифма количества монотонных булевых, В. Б. Алексеев [1] — монотонных $k$-значных функций. Асимптотика числа монотонных булевых функций найдена Д. А. Коршуновым [52, 53]. Компактно этот результат изложил А. А. Сапоженко [71]; см. также [54, 72].

Ранее задача расшифровки пороговых функций рассматривалась лишь для случая булевых, многозначных или конечнозначных логик. Постановка задачи, в которой функции определены на множестве целочисленных решений системы линейных неравенств (в целочисленных точках некоторого политопа $P$), является новой. В этом случае функция

$f : M = P \cap \mathbb{Z}^n \to \{0, 1\}$ называется пороговой, если в $\mathbb{R}^n$ существует гиперплоскость, разделяющая множества ее нулей и единиц. Другим интересным для теории и приложений обобщением является расшифровка в классе функция, заданных на $M$ множество нулей и единиц которой можно задать системами линейных неравенств. Диссертантом разработаны алгоритмы расшифровки функций из указанных классов.

По мнению диссертанта, проводимые обобщения позволяют значительно расширить область применения предлагаемых алгоритмов. Рассмотрим следующий пример, относящийся к распознаванию образов. Пусть объекты из некоторой совокупности характеризуются набором $n$ числовых параметров (признаков) и разделены на 2 класса (образа). Тогда каждый объект может быть представлен точкой, а вся совокупность — некоторой областью в $n$-мерном пространстве. Каждому классу будет соответствовать своя подобласть. Рассмотрим случай, когда параметры объектов суть целые числа, а область, соответствующая всей совокупности, ограничена и представляет собой множество целочисленных решений некоторой заданной системы линейных неравенств (множество $M$ целочисленных точек политопа $P$). Пусть подобласти, представляющие разные образы, могут быть разделены некоторой гиперплоскостью: как отмечено, например, в [128], этот случай имеет «большое практическое значение». Сделаем предположение, что по произвольному объекту из рассматриваемой совокупности можно определить, к какому из двух классов он принадлежит, и будем считать, что в любой момент для этого определения доступен *любой* объект из всей совокупности. В этих условиях задача об определении коэффициентов разделяющей гиперплоскости за минимальное число исследований объектов, очевидно, эквивалентна задаче расшифровки пороговой функции, определенной на множестве $M$.

Коснемся теперь других областей, в которых появляются задачи, тождественные или близкие к рассматриваемым.

В вычислительной теории машинного обучения Д. Англуин [115] предложила следующую модель обучения с помощью *вопросов принадлежности* (membership queries). Пусть $M$ — конечное множество, $\mathscr{C} \subseteq M$, $\mathfrak{C} \subseteq 2^M$. Назовем $M$ *пространством примеров* (instance space), $\mathscr{C}$ *— понятием* (concept), $\mathfrak{C}$ *— классом понятий* (concept class). *Ученик* с помощью вопросов вида «$x \in \mathscr{C}$?», где $x \in M$, должен дать описание заранее не известного понятия $\mathscr{C}$ из некоторого известного класса $\mathfrak{C}$. Каждому $\mathscr{C} \in \mathfrak{C}$ поставим в соответствие характеристическую функцию $f : M \to \{0, 1\}$, такую, что $\mathscr{C}$ совпадает со множеством ее единиц (множеством истинности). При таком отображении множеству $\mathfrak{C}$ соответствует некоторый класс функций (предикатов), определенных на $M$, а сама задача обучения сводится к задаче расшифровки в этом классе.

Другой смежной областью является теория тестов [55, 62, 87]. Рассмотрим частный случай одной из ее задач. Для (диагностической) таблицы с попарно различными столбцами, заполненной числами $0, 1$, исследуется игра двух лиц: первый игрок загадывает столбец таблицы, а второй должен угадать номер этого столбца. Для этого он, последовательно выбирая строки таблицы, спрашивает, что в них содержит загаданный столбец. Алгоритм определения номера столбца есть условный тест для рассматриваемой таблицы, если новый вопрос второго игрока формируется на основе ответов на его предыдущие вопросы. Для класса $\mathfrak{F}'$ функций, отображающих $M$ в $\{0, 1\}$, рассмотрим таблицу, состоящую из $|M|$ строк и $|\mathfrak{F}'|$ столбцов. Каждой строке припишем точку из $M$, а каждому столбцу — функцию из $\mathfrak{F}'$. На пересечении строки, помеченной точкой $x$, и столбца, помеченного функцией $f$, поставим величину $f(x)$. Очевидно, что в такой постановке расшифровка в классе $\mathfrak{F}'$ является

задачей теории тестов.

Одной из важнейших задач целочисленного линейного программирования является *задача о рюкзаке* [81, 105]. Рассмотрим один из ее вариантов: необходимо найти $\max cx$, при ограничениях $x \in \mathscr{C} \equiv \{x \in E_k^n : \ ax \leq a_0\}$. Предположим, что $k$, $n$, $c$ известны, а $\mathscr{C}$ задано с помощью оракула, позволяющего по произвольной точке $x \in E_k^n$ отвечать на вопрос «$x \in \mathscr{C}$?». Очевидно, что эту задачу можно свести к расшифровке пороговой функции. Заметим, что оракульная постановка задач является достаточно популярной в теории оптимизации, включая дискретную оптимизацию [56, 82, 137, 148]. На связь задачи расшифровки монотонной функции с задачами булева линейного программирования, по-видимому, первым указал В. К. Коробков [50].

В диссертации устанавливается связь задачи расшифровки пороговой функции с другой важной проблемой — нахождением наилучшего диофантового приближения.

По теме диссертации автором опубликовано 17 работ [21, 22, 24–30, 32–36, 109, 160, 161], из них 11 статей в изданиях, рекомендованных ВАК [22, 24, 27, 29, 30, 32, 34–36, 109, 160]. Все основные результаты диссертации являются новыми и принадлежат автору. В работах, выполненных совместно с В. Н. Шевченко и А. Ю. Чирковым, диссертанту принадлежат формулировки и доказательства результатов, включенных в диссертацию. Диссертация продолжает исследования, начатые автором в его кандидатской диссертации [23].

**Краткое содержание и основные результаты**

Во введении диссертации обосновывается актуальность темы, приводится обзор литературы и излагаются основные результаты.

**Глава 1** посвящена изучению основных свойств пороговых и близких к ним функций, определенных в целочисленных точках политопа. В разделе 1.1 вводятся основные классы рассматриваемых функций и даются необходимые и достаточные условия принадлежности функций тому или иному из этих классов. Обозначим через $\mathfrak{P}(n, l, \gamma)$ множество выпуклых политопов $P \subseteq \mathbb{R}^n$, каждый из которых можно задать системой $l$ линейных неравенств с целочисленными коэффициентами, ограниченными по абсолютной величине числом $\gamma$; пусть $\mathfrak{M}(n, l, \gamma) = \{P \cap \mathbb{Z}^n : \ P \in \mathfrak{P}(n, l, \gamma)\}$. Для некоторых $n \geq 2$, $l > n$, $\gamma \geq 2$ рассмотрим множество $M \in \mathfrak{M}(n, l, \gamma)$; предположим, что $M \neq \varnothing$. Множество всех функций, отображающих $M$ в $\{0, 1\}$, обозначим через $\mathfrak{F}(M)$. Пусть $E_k = \{0, \ldots, k-1\}$. Класс $\mathfrak{F}(E_2^n)$ объединяет функции булевой логики, а $\mathfrak{F}(E_k^n)$ при $k \geq 2$ является подклассом тех функций $k$-значной логики, множество значений которых есть $\{0, 1\}$. Для $f \in \mathfrak{F}(M)$ обозначим через $M_0(f)$ и $M_1(f)$ множество нулей и единиц функции $f$ соответственно, т. е. $M_\nu(f) = \{x \in M : \ f(x) = \nu\}$ $(\nu = 0, 1)$. Обозначим через $N_\nu(f) = \operatorname{Vert} M_\nu(f)$ множество вершин (крайних точек) политопа $\operatorname{Conv} M_\nu(f)$ $(\nu = 0, 1)$.

Для каждого $\nu \in \{0, 1\}$ обозначим через $\mathfrak{F}_\nu(M)$ множество таких функций $f \in \mathfrak{F}(M)$, для которых $M_\nu(f)$ можно описать в виде некоторой системы линейных неравенств $Ax \leq a_0$, т. е. $M_\nu(f) = \{x \in M : \ Ax \leq a_0\}$. Систему $Ax \leq a_0$ назовем *характеристической*. Обозначим через $m_\nu(f)$ наименьшее число неравенств в системе $Ax \leq a_0$, при котором возможно такое описание. Если для некоторого $\nu \in \{0, 1\}$ справедливо $f \in \mathfrak{F}_\nu(M)$ и $m_\nu(f) = 1$, то функция $f$ называется *пороговой*. Пусть для такой $f$ неравенство $\sum\limits_{j=1}^{n} a_j x_j \leq a_0$, которое назовем *пороговым*, описывает множество $M_0(f)$. Можно считать, что $a_j \in \mathbb{Z}$ $(j = 0, 1, \ldots, n)$. Обозначим через $\mathfrak{T}(M)$ множество всех пороговых функций, заданных на $M$.

В разделе 1.2 для функций из классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$ получены верхние оценки величины коэффициентов характеристической системы, а в разделе 1.3 — верхние оценки величин $|N_\nu(f)|$ ($\nu = 0, 1$). Также в разделе 1.3 исследуется задача построения множеств $N_\nu(f)$ по заданной характеристической системе функции $f$.

Мощностные свойства классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$ изучаются в разделе 1.4. Рассмотрим класс $\mathfrak{F}_\nu(M, m)$ ($\nu = 0, 1$) таких функций $f$ из $\mathfrak{F}_\nu(M)$, для которых $m_\nu(f) = m$. Доказано, что при $\gamma \geq 1$, $m \geq 1$ справедлива асимптотическая оценка $\log|\mathfrak{F}_\nu(M, m)| \lesssim mn^3 \log(\gamma\sqrt{n})$ ($n \to \infty$). Отсюда для класса пороговых функций при $\gamma \geq 1$ получается неравенство $\log|\mathfrak{T}(M)| \lesssim n^3 \log(\gamma\sqrt{n})$ ($n \to \infty$).

Соотношения между классами $\mathfrak{T}(M)$ и $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ исследуются в разделе 1.5. В частности, построены примеры, показывающие, что если $k \geq 2$ и $n \geq 3$, то $\mathfrak{T}(E_k^n)$ является собственным подмножеством класса $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$. Приведено доказательство, что если $k \geq 3$, то $\mathfrak{T}(E_k^2) = \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$ (данное утверждение приведено в [105, стр. 169] без доказательства).

Раздел 1.6 посвящен задаче построения вершин и экстремальных лучей полиэдра $P = \{x \in \mathbb{R}^n : Ax \leq a_0\}$, где $A \in \mathbb{Z}^{m\times n}$, $a_0 \in \mathbb{Z}^m$. Эта задача возникает как вспомогательная при построении алгоритмов расшифровки пороговых и близких к ним функций, но также возникает в большом числе других приложений и представляет несомненный самостоятельный интерес. Стандартным способом она сводится к построению экстремальных лучей полиэдрального (многогранного) конуса $\{(x, x_0) \in \mathbb{R}^{n+1} : Ax \leq x_0 a_0,\ x_0 \geq 0\}$. Для решения задачи известны различные методы, один из них — хорошо известный «*метод двойного описания*» [153] (другие распространенные названия — алгоритм Моцкина–Бургера [88] или алгоритм Фурье–Моцкина [106, 108]).

На каждой итерации алгоритм определяет множество всех пар смежных экстремальных лучей некоторого конуса $C = \{x \in \mathbb{R}^n : \ Ax \geq 0\}$, где $A \in \mathbb{Z}^{m \times n}$. Пусть $U$ — множество экстремальных лучей конуса $C$, $|U| = s$. Обозначим $Z(u) = \{i : \ a_i u = 0\}$, где $a_i$ — $i$-я строка матрицы $A$, $u \in U$. Хорошо известное «комбинаторное правило» [123] проверки смежности утверждает, что для смежности лучей $u$ и $v$ из $U$ необходимо и достаточно, чтобы в $U$ не существовало луча $w$, отличного от $u$ и $v$, такого, что $Z(u) \cap Z(v) \subseteq Z(w)$. Мы предлагаем следующую «графовую» модификацию комбинаторного теста. По конусу $C$ построим простой граф $G$: множество вершин графа $G$ есть множество $U$, а $\{u, v\}$ образует ребро в $G$ тогда и только тогда, когда $|Z(u) \cap Z(v)| \geq n - 2$. Множество всех ребер графа $G$ обозначим $E(G)$. Мы доказываем, что для того, чтобы лучи $u$ и $v$ из $U$ были смежны необходимо и достаточно, чтобы в $U(C)$ не существовало луча $w$, отличного от $u$ и $v$, такого, что $\{u, w\} \in E(G)$, $\{v, w\} \in E(G)$ и $Z(u) \cap Z(v) \subseteq Z(w)$. Трудоемкость построения всех пар экстремальных лучей по комбинаторному правилу составляет $O(ms^3)$, а по его «графовой» модификации $O(ms^2 + ms\delta^2)$, где $\delta$ равно максимуму из степеней вершин в графе $G$. Так как $\delta < s$, то трудоемкость «графового» теста всегда асимптотически не превосходит верхней оценки трудоемкости «комбинаторного». Во многих задачах $\delta \ll s$ и преимущество нового алгоритма более существенно. Результаты вычислительного эксперимента подтверждают это превосходство. Диссертантом предлагаются также другие модификации метода двойного описания.

Результаты первой главы диссертации опубликованы в работах автора [22, 29, 33].

В **главе 2** предлагаются алгоритмы расшифровки пороговых и близких к ним функций. Пусть каждая функция $f$ из некоторого класса $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ задана *оракулом*, позволяющим по произвольной точке $x \in M$

определить $f(x)$. Под *расшифровкой* функции из известного класса $\mathfrak{F}'$ понимается задача, в которой по заданным $C \in \mathbb{Z}^{l\times n}$, $c_0 \in \mathbb{Z}^l$ и заданному оракулу функции $f \in \mathfrak{F}'$, где $M = \{x \in \mathbb{Z}^n : \ Cx \le c_0\}$, необходимо найти такие точки $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$ из $M$, значений в которых достаточно для однозначного определения $f$ в остальных точках из $M$.

Пусть $\mathscr{A}$ — алгоритм расшифровки функции в классе $\mathfrak{F}'$. Предположим, что при расшифровке функции $f \in \mathfrak{F}'$ алгоритм $\mathscr{A}$ обращается к оракулу в $\tau(\mathscr{A}, f)$ точках и выполняет $\rho(\mathscr{A}, f)$ операций. *Оракульной сложностью* алгоритма $\mathscr{A}$ назовем величину

$$\tau_M(\mathscr{A}) = \max_{f\in\mathfrak{F}'} \tau(\mathscr{A}, f).$$

*Вычислительной трудоемкостью* алгоритма $\mathscr{A}$ назовем число операций, выполненных алгоритмом в худшем случае:

$$\rho_M(\mathscr{A}) = \max_{f\in\mathfrak{F}'} \rho(\mathscr{A}, f).$$

Пусть, как обычно, $M = \{x \in \mathbb{Z}^n : \ Cx \le c_0\} \in \mathfrak{M}(n, l, \gamma)$, $C \in \mathbb{Z}^{l\times n}$, $c_0 \in \mathbb{Z}^l$, $|c_{ij}| \le \gamma$, $(i = 1, 2, \ldots, l;\ j = 0, 1, \ldots, n)$. Алгоритм $\mathscr{A}$ назовем *полиномиальным*, если функция $\rho_M(\mathscr{A})$ ограничена некоторым полиномом от трех переменных $n$, $l$, $\log\gamma$. Будем говорить, что алгоритм $\mathscr{A}$ полиномиален при фиксированной размерности $n$ (*квазиполиномиален*), если найдется многочлен $p_n(\cdot,\cdot)$, степень и коэффициенты которого зависят только от $n$, такой, что $\rho_M(\mathscr{A}) \le p_n(l, \log\gamma)$. Очевидно, $\tau_M(\mathscr{A}) \le \rho_M(\mathscr{A})$ и поэтому верхняя оценка вычислительной трудоемкости алгоритма является таковой и для его оракульной сложности.

Если из контекста ясно, о каком множестве $M$ идет речь, то вместо $\tau_M(\mathscr{A})$ и $\rho_M(\mathscr{A})$ будем писать соответственно $\tau(\mathscr{A})$ и $\rho(\mathscr{A})$.

Для классов $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$, $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ от алгоритмов расшифровки будем требовать, чтобы они возвращали также коэффициенты

характеристических систем функции $f$. В случае пороговой функции — коэффициенты порогового неравенства.

В диссертации рассматриваются алгоритмы (условные тесты), в которых выбор точки для нового обращения к оракулу, определяется ответами на предыдущие вопросы. Что же касается алгоритмов, не учитывающих ответы на предыдущие вопросы (безусловные тесты), то для рассматриваемых классов они оказываются весьма неэффективными. Множество $U \subseteq M$ называется *безусловным тестом* для класса функций $\mathfrak{F}'$, если для любых двух $f, g$ из $\mathfrak{F}'$, $f \neq g$, найдется точка $x \in U$, такая, что $f(x) \neq g(x)$. В разделе 2.2 показано, что классы $\mathfrak{T}(M)$, $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$, $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ обладают единственным безусловным тестом $U = M$.

В разделе 2.3 рассматривается задача расшифровки в $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. Вначале (в подразделе 2.3.1) строится вспомогательный оракульный алгоритм $\mathscr{A}_{\text{опт}}$, решающий задачу максимизации линейной функции на множестве $M_\nu(f)$, где $f \in \mathfrak{F}_{1-\nu}(M)$. Алгоритм $\mathscr{A}_{\text{опт}}$ для любого $\nu \in \{0, 1\}$, любой заданной оракулом функции $f \in \mathfrak{F}_{1-\nu}(M)$ и любого вектора $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ находит точку $p = (p_1, \ldots, p_n) \in M_\nu(f)$, такую, что

$$\sum_{j=1}^{n} a_j p_j = \max \left\{ \sum_{j=1}^{n} a_j x_j : \ (x_1, \ldots, x_n) \in M_\nu(f) \right\},$$

или устанавливает, что $M_\nu(f) = \varnothing$. При фиксированном $n$ алгоритм имеет полиномиальную от $l$ и $\log \alpha$ вычислительную трудоемкость и совершает не более $n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\alpha + 1)$ (при $n \geq 2$) и не более $8 + 2 \log \gamma$ (при $n = 1$) обращений к оракулу, где $\alpha = \max\{\gamma, |a_j|, j = 1, \ldots, n\}$.

В подразделе 2.3.2 предлагается алгоритм $\mathscr{A}_0$ расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. Обозначим через $\mathfrak{F}(M, h)$ множество таких функций $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, для которых $\min\{m_0(f), m_1(f)\} \leq h$. В классе $\mathfrak{F}(M, h)$, где $M \in \mathfrak{M}(n, l, \gamma)$, при любом фиксированном $n$ алгоритм имеет полиномиальную от $h$, $l$ и $\log \gamma$ вычислительную трудоемкость $\rho(\mathscr{A}_0)$ и оракуль-

ную сложность

$$\tau(\mathscr{A}_0) = O\Big((l+h)^{\lfloor \frac{n}{2} \rfloor^2} l^{\lfloor \frac{n}{2} \rfloor} \log^{(n-1)\lfloor \frac{n}{2} \rfloor + n}(\gamma+1)\Big)$$

(асимптотика при фиксированном $n$).

Очевидно, алгоритм $\mathscr{A}_0$ применим и для расшифровки функций из класса $\mathfrak{T}(M)$. Для последнего случая однако существует более эффективный алгоритм $\mathscr{A}_1$, описанный в разделе 2.4. Вначале (в подразделе 2.4.1) строится вспомогательный алгоритм $\mathscr{A}_1^+$. Обозначим через $\mathfrak{T}_+(M)$ множество тех функций из $\mathfrak{T}(M)$, для которых существует пороговое неравенство с коэффициентом $a_0 > 0$. Алгоритм $\mathscr{A}_1^+$ проводит расшифровку при допущении $f \in \mathfrak{T}_+(M)$. На его основе в разделе 2.4.2 построен алгоритм $\mathscr{A}_1$ расшифровки в классе $\mathfrak{T}(M)$, для которого при фиксированном $n$ величина $\rho(\mathscr{A}_1)$ ограничена полиномом от $l$ и $\log \gamma$ и

$$\tau(\mathscr{A}_1) \le 16 n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\gamma+1) = O\Big(l^{\lfloor \frac{n}{2} \rfloor} \log^n(\gamma+1)\Big).$$

(асимптотика при фиксированном $n$). В классе $\mathfrak{T}(E_k^n)$ при любом фиксированном $n$ алгоритм имеет оракульную сложность

$$\tau(\mathscr{A}_1) = O(\log^n k).$$

В разделе 2.5 для расшифровки функций из класса $\mathfrak{T}(E_k^2)$ удалось построить более эффективный алгоритм $\mathscr{A}_2$. Алгоритм $\mathscr{A}_2$ имеет полиномиальную вычислительную трудоемкость и оракульную сложность

$$\tau(\mathscr{A}_2) \le 6 \log(k-1) + 4.$$

В разделе 2.6 исследуется задача расшифровки пороговой функции, заданной более информативным — «*расширенным*» — оракулом, который в отличие от «обычного» оракула принимает на вход произвольные точки из $\mathbb{Q}^n$, а не только из $M$. Расширенный оракул связан с конкретным пороговым неравенством функции $f$. По заданной точке $x \in \mathbb{Q}^n$ он возвращает

0, если пороговое неравенство выполнено, и 1 в противном случае. Под *расшифровкой пороговой функции* $f$, *заданной с помощью расширенного оракула*, будем понимать процедуру восстановления коэффициентов ее любого возможного порогового неравенства с помощью обращений к этому оракулу. Предложен алгоритм $\mathscr{A}_{\text{ext}}$ расшифровки функции из класса $\mathfrak{T}(E_k^n)$, заданной с помощью расширенного оракула, для которого вычислительная трудоемкость $\rho(\mathscr{A}_{\text{ext}})$ при фиксированном $n$ ограничена полиномом от $\log k$, а для оракульной сложности справедливо

$$\mathscr{A}_{\text{ext}} = \frac{n^4}{2}\log(n+1) + 2n^3 \log k \qquad (n \to \infty, \quad k \to \infty).$$

Результаты второй главы опубликованы в [21, 22, 25, 30, 34, 160].

В **главе 3** устанавливаются нижние оценки сложности расшифровки пороговых функций. Под *сложностью расшифровки* в некотором классе $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ понимается величина

$$\tau(\mathfrak{F}') = \min_{\mathscr{A}} \tau(\mathscr{A}) = \min_{\mathscr{A}} \max_{f \in \mathfrak{F}'} \tau(\mathscr{A}, f),$$

где минимум берется по всем алгоритмам $\mathscr{A}$ расшифровки в классе $\mathfrak{F}'$. Множество $T \subseteq M$ называется *разрешающим* для $f$ в классе $\mathfrak{F}'$, если для любой функции $g \in \mathfrak{F}'$, $f \neq g$, найдется по крайней мере одна точка $z \in T$, такая, что $g(z) \neq f(z)$. Разрешающее множество, никакое собственное подмножество которого не является разрешающим для $f$, называется *минимальным* или *тупиковым*. Разрешающее множество минимальной мощности называется *наименьшим*. Его мощность обозначим через $\sigma(\mathfrak{F}', f)$. *Длиной обучения* назовем величину

$$\sigma(\mathfrak{F}') = \max_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f) = \max_{f \in \mathfrak{F}'} \min_{\mathscr{A}} \tau(\mathscr{A}, f).$$

Справедливы неравенства $\tau(\mathfrak{F}') \geq \sigma(\mathfrak{F}')$, $\tau(\mathfrak{F}') \geq \log|\mathfrak{F}'|$, являющиеся ключевыми для получения в диссертации нижних оценок сложности

расшифровки. *Средней мощностью минимального разрешающего множества* в классе $\mathfrak{F}'$ называется

$$\overline{\sigma}(\mathfrak{F}') = \frac{1}{|\mathfrak{F}'|} \sum_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f).$$

Для класса пороговых функций $\mathfrak{T}(M)$ будем использовать следующие сокращенные обозначения:

$$\tau(M) = \tau\big(\mathfrak{T}(M)\big), \qquad \sigma(M) = \sigma\big(\mathfrak{T}(M)\big), \qquad \overline{\sigma}(M) = \overline{\sigma}\big(\mathfrak{T}(M)\big).$$

В разделе 3.2 получены некоторые вспомогательные результаты о строении конуса $K(f)$ *разделяющих функционалов* функции $f \in \mathfrak{T}(M)$. $K(f)$ описывается следующей системой линейных неравенств относительно переменных $a_0, a_1, \ldots, a_{n+1}$:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{для всех } (x_1, \ldots, x_n) \in M_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{для всех } (x_1, \ldots, x_n) \in M_1(f); \\ a_{n+1} \ge 0. \end{cases}$$

Показано, что конус $K(f)$ полномерный (телесный) и в важном случае $\operatorname{Affdim} M = n$ — острый. Из теории линейных неравенств выводится лемма о двойственном описании конуса $K(f)$. В частности, если $\operatorname{Affdim} M = n$, то $K(f)$ имеет единственное с точностью до положительных множителей минимальное порождающее множество (остов)

$$\left\{ \widetilde{b^{(i)}} = (b_0^{(i)}, b_1^{(i)}, \ldots, b_n^{(i)}, b_{n+1}^{(i)}),\ i = 1, \ldots, s \right\}.$$

В разделе 3.3 исследуется структура разрешающего множества пороговой функции. Множество $T = T_0 \cup T_1$, $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$ является разрешающим для $f \in \mathfrak{T}(M)$ тогда и только тогда, когда система нера-

венств

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{для всех } (x_1,\dots,x_n)\in T; \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{для всех } (x_1,\dots,x_n)\in T; \\ a_{n+1} \ge 0. \end{cases}$$

описывает конус $K(f)$. Отсюда, в частности, получаем единственность минимального разрешающего множества функции $f \in \mathfrak{T}(M)$ (это обобщение известного результата о булевых пороговых функциях). Обозначим его через $T(f) = T_0(f) \cup T_1(f)$, $T_\nu(f) \subseteq M_\nu(f)$ $(\nu = 0, 1)$. Имеем также $N_\nu(f) \subseteq T_\nu(f)$ $(\nu = 0, 1)$ (это обобщение результата [105]).

Пусть $\operatorname{Affdim} M = n$ и $f \in \mathfrak{T}(M)$. Не нарушая общности, будем считать, что в остове конуса $K(f)$ компонента $b^{(i)}_{n+1} > 0$ $(i = 1,\dots,\mu)$ и $b^{(i)}_{n+1} = 0$ $(i = \mu+1,\dots,s)$. Пусть $a = (a_1,\dots a_n) \in \mathbb{Z}^n$,

$$M_0(f,a) = \left\{ (y_1,\dots,y_n) \in M : \sum_{j=1}^{n} a_j y_j = \max_{x\in M_0(f)} \sum_{j=1}^{n} a_j x_j \right\},$$

$$M_1(f,a) = \left\{ (y_1,\dots,y_n) \in M : \sum_{j=1}^{n} a_j y_j = \min_{x\in M_1(f)} \sum_{j=1}^{n} a_j x_j \right\}.$$

Обозначим через $N_\nu(f,a)$ множество крайних точек (вершин) выпуклой оболочки множества $M_\nu(f,a)$. Доказано, что если $\operatorname{Affdim} M = n$, тогда для любой функции $f \in \mathfrak{T}(M)$

$$T(f) = \bigcup_{i=1}^{\mu} \left( N_0(f, \widetilde{b^{(i)}}) \cup N_1(f, \widetilde{b^{(i)}}) \right) = \bigcup_{a} \Big( N_0(f, a) \cup N_1(f, a) \Big),$$

в последнем случае объединение берется по всем $a = (a_1, a_2 \dots, a_n) \in \mathbb{Z}^n$ таким, что неравенство

$$\sum_{j=1}^{n} a_j x_j \le \max_{x\in M_0(f)} \sum_{j=1}^{n} a_j x_j$$

является пороговым для функции $f$.

В разделе 3.4 на основе анализа структуры разрешающего множества, проведенного ранее, выводятся нижние оценки длины обучения в

классе $\mathfrak{T}(M)$. Доказано, что для любых $n \geq 2$ и $l > n$ найдется такое $\gamma_0$, что для всех $\gamma \geq \gamma_0$ существует политоп $P \in \mathfrak{P}(n, l, \gamma)$ такой, что при фиксированном $n$

$$\tau(M) \geq \sigma(M) = \Omega(l^{\lfloor n/2 \rfloor} \log^{n-1} \gamma),$$

где $M = P \cap \mathbb{Z}^n$. Для класса пороговых функций $k$-значной логики установлена оценка при фиксированном $n$

$$\tau(E_k^n) \geq \sigma(E_k^n) \geq \frac{\left(\frac{1}{2}\log k - n - 3 - (n-1)\log(n-2)\right)^{n-2}}{4(n-1)3^{n-1}(n-2)^{n-2}\left((n-2)!\right)^2} = \Omega(\log^{n-2} k).$$

В разделе 3.5 предлагается другая характеризация минимального разрешающего множества $T(f)$ пороговой функции $f \in \mathfrak{T}(M)$. Пусть $Q(f) = \mathrm{Cone}\Big(M_0(f) - M_1(f)\Big)$; если $f$ — тождественная константа, то $Q(f)$ — нулевой конус;

$$R_0(f) = \mathrm{Conv}\Big(M_0(f)\Big) + Q(f), \qquad R_1(f) = \mathrm{Conv}\Big(M_1(f)\Big) - Q(f).$$

Доказано, что если $f \in \mathfrak{T}(M)$, то

$$T_\nu(f) = \mathrm{Vert}\, R_\nu(f) \qquad (\nu = 0, 1).$$

Отсюда получаем, что если $x, y \in T_\nu(f)$ $(\nu = 0, 1)$ и $x \neq y$, то

$$2x - y \notin R_0(f) \cup R_1(f) \qquad (0.1).$$

В общем случае удобного описания множеств $R_\nu(f)$ $(\nu = 0, 1)$, которое позволило бы достаточно точно оценить $|\mathrm{Vert}\, R_\nu(f)|$, не найдено. Тем не менее, в разделе 3.6 такое описание получено для подкласса $\mathfrak{T}'(E_k^n)$ таких пороговых функций $f$, для каждой из которых найдется пороговое неравенство, в котором $a_0 \in \mathbb{Z}$, $a_j \in \mathbb{Z}$, $0 < a_0 < a_j(k-1)$ $(j = 1, 2, \ldots, n)$.

Говорят, что множество $G \subset \mathbb{Z}_+^n$ обладает *свойством разделенности*, если из условий $x, y \in G$ и $x \neq y$ следует $2x - y \notin \mathbb{Z}_+^n$ [100]. Если

$f \in \mathfrak{T}'(E_k^n)$, то из (0.1) получаем, что каждое из множеств $T_0(f)$ и $T_1(f)$ обладает свойством разделенности. Далее для получения верхних оценок $|T_0(f)|$ и $|T_1(f)|$ используется подход [100, 105]. Доказано, что для любой функции $f \in \mathfrak{T}'(E_k^n)$ при $n \geq 2$

$$|T_\nu(f)| \leq n(1+\log n)\Big(1+\log(k+1)\Big)^{n-2} \qquad (\nu = 0, 1).$$

В разделе 3.7 получены верхние оценки количества неприводимых точек в полиэдре (далее, в разделе 3.8, эти оценки используются для получения верхней оценки $\sigma(E_k^n) = O(\log^{n-2} k)$ при фиксированном $n \geq 2$). Пусть $P$ — полиэдр в $\mathbb{R}^n$. Точка $x \in P \in \mathbb{Z}^n$ называется *неприводимой* в $P$ (а, точнее, в $P \cap \mathbb{Z}^n$), если $x$ нельзя представить в виде $x = \frac{1}{2}(y+z)$ ни для каких двух различных $y$ и $z$ из $P \cap \mathbb{Z}^n$. Пусть $P$, $P_1, P_2, \ldots, P_s$ — политопы (т. е. ограниченные полиэдры) в $\mathbb{R}^n$. Если $P = \bigcup\limits_{i=1}^{s} P_i$, то $\{P_1, P_2, \ldots, P_s\}$ называется *покрытием* политопа $P$. Если пересечение любых двух политопов в покрытии либо пусто, либо является их общей гранью, то покрытие называется *правильным разбиением*. Если все политопы в правильном разбиении — симплексы, то разбиение называется *триангуляцией*. Основная идея получения верхней оценки числа неприводимых точек в политопе заключается в следующем. В подразделе 3.7.1 получена оценка количества неприводимых точек в параллелепипеде. В подразделе 3.7.2 показано, как для произвольного политопа $P$ построить его покрытие параллелепипедами $P_1, P_2, \ldots, P_s$. Для этого сначала строится триангуляция политопа, а затем каждый симплекс триангуляции покрывается параллелепипедами. Легко видеть, что любая неприводимая в $P \cap \mathbb{Z}^n$ точка $x$ неприводима и в $P_i \cap \mathbb{Z}^n$ для любого $i$, если $x \in P_i$. Это свойство позволяет в подразделе 3.7.3 оценить количество неприводимых точек в $P$. А именно, доказано, что если $P$ можно задать системой $m$ линейных неравенств и $P \cap \mathbb{Z}^n \subseteq E_k^n$, то количество неприводимых в

$P \cap \mathbb{Z}^n$ точек есть $O(m^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} k)$. Заметим, что полученная оценка представляет самостоятельный интерес. В разделе 3.8 она используется для получения неулучшаемой верхней оценки длины обучения в классе пороговых функций.

В разделе 3.8, используя результаты разделов 3.6 и 3.7, мы показываем, что

$$\sigma(E_k^n) = O(\log^{n-2} k) \qquad (k \to \infty).$$

Объединяя нижнюю и верхнюю оценки длины обучения, получаем, что при фиксированном $n \geq 2$

$$\sigma(E_k^n) = \Theta(\log^{n-2} k) \qquad (k \to \infty).$$

В разделе 3.9 изучается задача построения минимального разрешающего множества пороговой функции $f \in \mathfrak{T}(M)$, $M = P \cap \mathbb{Z}^n$, по известным коэффициентам порогового неравенства и по известной системе, описывающей политоп $P$. Для решения этой задача предлагается полиномиальная от $\log \gamma$ и $l$ процедура ($n$ фиксировано). Показано, как изменить алгоритм $\mathscr{A}_1$, чтобы сложность нового алгоритма $\mathscr{A}_1^{\circ}$ отличалась бы от сложности оптимального (по числу обращений к оракулу в худшем случае) алгоритма расшифровки не более, чем в $O\left(n^3 \log(n\gamma)\right)$ раз. Для класса $\mathfrak{T}(E_k^n)$ сложность алгоритма $\mathscr{A}_1^{\circ}$ отличается от сложности оптимального алгоритма не более, чем в $O\left(n^2 \log(nk)\right)$ раз и при фиксированном $n$

$$\tau(E_k^n) \leq \tau(\mathscr{A}_1^{\circ}) = O(\log^{n-1} k).$$

В разделе 3.10 рассматривается случай пороговых функций двух переменных. Из результатов предыдущих разделов вытекает

$$4 \log k \lesssim \tau(E_k^2) \lesssim 6 \log k.$$

Для длины обучения в классе $\mathfrak{T}(E_k^2)$ в подразделе 3.10.1 установлено точное значение

$$\sigma(E_k^2) = 4.$$

В подразделе 3.10.2 получена асимптотика среднего значения мощности минимального разрещающего множества в классе $\mathfrak{T}(E_k^2)$:

$$\overline{\sigma}(E_k^2) = \frac{7}{2} + O\left(\frac{1}{k}\right).$$

В подразделе 3.10.3 получены следствия из этих результатов, касающиеся специальных разбиений плоскости прямыми.

Пороговые булевы функции рассматриваются в разделе 3.11. Справедливо следующее равенство: $\sigma(E_2^n) = \tau(E_2^n) = |E_2^n| = 2^n$. В данном разделе также показано, что сложность расшифровки в классе пороговых монотонных булевых функций совпадает со сложностью расшифровки в классе монотонных булевых функций.

В разделе 3.12 полученные результаты о верхних и нижних оценках сложности расшифровки применяются к анализу оракульной сложности задачи о рюкзаке.

Результаты третьей главы диссертации опубликованы в работах [24, 26–28, 32, 33, 36, 109, 161].

В **главе 4** показана связь задачи расшифровки пороговой функции двух переменных с проблемой нахождения диофантовых приближений вещественных чисел. Рассмотрим следующую задачу. Для $\alpha \in \mathbb{R}$, $\alpha \geq 0$, $Q \in \mathbb{N}$ требуется среди всех рациональных дробей со знаменателем, не превосходящим $Q$, найти наилучшее приближение $\frac{p}{q}$ к $\alpha$:

$$\left|\alpha - \frac{p}{q}\right| = \min\left\{\left|\alpha - \frac{y}{x}\right| : x \in \mathbb{N}, x \leq Q, y \in \mathbb{Z}\right\}.$$

Предположим, что вещественное число $\alpha$ задано оракулом, позволяющим по произвольному $r \in \mathbb{Q}$ определить, выполняется или нет

неравенство $\alpha \leq r$. В разделе 4.2 показано, как использовать алгоритм $\mathscr{A}_2$ для решения задачи наилучшего приближения к заданному таким образом числу. Время работы построенной процедуры ограничено полиномом от $\log k$, где $k = \max\{Q, \lceil \alpha Q \rceil\}$. В разделе 4.3 на основе полученных результатов строится полиномиальный алгоритм нахождения наилучших приближений алгебраических вещественных чисел, заданных минимальным многочленом.

Результаты четвертой главы диссертации опубликованы в работе [35].

**В заключении** обсуждаются основные результаты диссертации

# Глава 1

# Свойства пороговых и близких к ним функций

В настоящей главе изучаются свойства функций, определенных на множестве целочисленных точек заданного $n$-мерного выпуклого политопа и обладающих различными свойствами линейной отделимости. Результаты, полученные в [103] для $E_k^n$, распространяются в первых двух разделах на случай произвольного политопа. Определения изучаемых классов и некоторые простые свойства приведены в разделе 1.1. Величина коэффициентов характеристической системы, которая задает поверхность, разделяющую множества различных значений функции, исследуется в разделе 1.2. В разделе 1.3 выводятся оценки числа вершин выпуклой оболочки множеств «нулей» и «единиц» исследуемых функций. В разделах 1.4, 1.5 изучаются мощностные характеристики и соотношения исследуемых классов.

Результаты разделов 1.1–1.5 опубликованы в работах [22, 33], раздела 1.6 — в [29].

## 1.1. Определения исследуемых классов функций

Пусть $\mathfrak{F}$ — некоторое подполе поля действительных чисел $\mathbb{R}$, т. е. $\mathbb{Q} \subseteq \mathfrak{F} \subseteq \mathbb{R}$. *Выпуклым полиэдром* (*многогранным множеством*) в пространстве $\mathfrak{F}^n$ (далее просто *полиэдром*) называется множество

$$P = P(C, c_0) = \{x \in \mathfrak{F}^n : \ Cx \leq c_0\},$$

где $C \in \mathfrak{F}^{l \times n}$, $c_0 \in \mathfrak{F}^l$. Ограниченный полиэдр называется *политопом*. Обозначим $M(C, c_0) = P(C, c_0) \cap \mathbb{Z}^n$ — множество целочисленных точек

полиэдра $P$; $N(C, c_0) = \operatorname{Vert} M(C, c_0)$ — множество вершин выпуклой оболочки целочисленных точек в $P$.

Обозначим через $\mathfrak{P}(n, l, \gamma)$ множество политопов $P \subseteq \mathbb{R}^n$, каждый из которых можно задать системой $l$ линейных неравенств с целочисленными коэффициентами, ограниченными по модулю величиной $\gamma$, т. е. $P = \{x \in \mathbb{R}^n : \ Cx \leq c_0\}$, где $C = (c_{ij}) \in \mathbb{Z}^{l \times n}$, $c_0 = (c_{i0}) \in \mathbb{Z}^l$, $|c_{ij}| \leq \gamma$ $(i = 1, 2, \ldots, l; \ j = 0, 1, \ldots, n)$. Обозначим

$$\mathfrak{M}(n, l, \gamma) = \{P \cap \mathbb{Z}^n : \ P \in \mathfrak{P}(n, l, \gamma)\}.$$

Для некоторых $n \geq 1$, $l > n$, $\gamma \geq 1$ рассмотрим множество $M \in \mathfrak{M}(n, l, \gamma)$; предположим, что $M \neq \varnothing$. Множество всех функций, отображающих $M$ в $\{0, 1\}$, обозначим через $\mathfrak{F}(M)$. Класс $\mathfrak{F}(E_2^n)$ объединяет все булевы функции, зависящие от $n$ переменных, а $\mathfrak{F}(E_k^n)$ при $k \geq 3$ является подклассом тех функций $k$-значной логики $n$ переменных, множество значений которых есть $\{0, 1\}$. Для $f \in \mathfrak{F}(M)$ через $M_0(f)$ и $M_1(f)$ обозначим множество «нулей» и «единиц» функции $f$ соответственно, т. е.

$$M_\nu(f) = \{x \in M : \ f(x) = \nu\} \qquad (\nu = 0, 1).$$

Пусть $P_\nu(f) = \operatorname{Conv} M_\nu(f)$ $(\nu = 0, 1)$. Очевидно, что $P_\nu(f)$ при $\nu = 0, 1$ является политопом.

Для каждого $\nu = 0, 1$ через $\mathfrak{F}_\nu(M)$ будем обозначать множество таких $f \in \mathfrak{F}(M)$, для которых $M_\nu(f)$ можно описать в виде системы линейных неравенств $Ax \leq a_0$:

$$M_\nu(f) = \{x \in M : \ Ax \leq a_0\}. \tag{1.1}$$

В данном случае систему $Ax \leq a_0$ назовем *характеристической*.

**Утверждение 1.1.** *Для того, чтобы функция $f$ из класса $\mathfrak{F}(M)$ принадлежала $\mathfrak{F}_\nu(M)$ для некоторого $\nu = 0, 1$, необходимо и достаточно, чтобы $\mathbb{Z}^n \cap P_\nu(f) = M_\nu(f)$.*

*Доказательство.* Необходимость условий очевидна. Для доказательства достаточности заметим, что выпуклая оболочка конечного числа точек описывается системой линейных неравенств. Так как $\mathbb{Z}^n \cap P_\nu(f) = M_\nu(f)$, то условие (1.1) выполнено. ∎

**Замечание 1.2.** Элементы матрицы $A$ и столбца $a_0$ в описании (1.1) можно считать целочисленными (см. далее следствие 1.9).

**Замечание 1.3.** В случае булевых функций для любой $f \in \mathfrak{F}(E_2^n)$, очевидно, $\mathbb{Z}^n \cap P_\nu(f) = M_\nu(f)$ и, следовательно, $\mathfrak{F}_0(E_2^n) = \mathfrak{F}_1(E_2^n) = \mathfrak{F}(E_2^n)$. Для $k$-значной логики при $k \geq 3$ аналогичные равенства не выполняются.

Из утверждения 1.1 следует

**Утверждение 1.4.** *Для того, чтобы функция $f$ из класса $\mathfrak{F}(M)$ принадлежала $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, необходимо и достаточно, чтобы*

$$P_0(f) \cap P_1(f) \cap M = \varnothing.$$

Обозначим через $m_\nu(f)$ *пороговое $\nu$-число* функции $f$, т. е. наименьшее число неравенств в системе $Ax \leq a_0$, при котором возможно описание (1.1) функции $f \in \mathfrak{F}_\nu(M)$, а через $N_\nu(f)$ — множество вершин (крайних точек) политопа $P_\nu(f)$. Если для некоторого $\nu \in \{0, 1\}$ справедливо $f \in F_\nu(M)$ и $m_\nu(f) = 1$, то функция $f$ называется *пороговой*. Пусть для такой $f$ неравенство

$$\sum_{j=1}^{n} a_j x_j \leq a_0, \tag{1.2}$$

которое назовем *пороговым*, описывает множество $M_0(f)$, т. е.

$$M_0(f) = \left\{ x = (x_1, \ldots, x_n) \in M : \sum_{j=1}^{n} a_j x_j \leq a_0 \right\}. \tag{1.3}$$

Как следует из замечания 1.2, можно считать, что $a_j \in \mathbb{Z}$ $(j = 0, 1, \ldots, n)$ и тогда очевидно, что

$$M_1(f) = \left\{ x = (x_1, \ldots, x_n) \in M : \sum_{j=1}^{n} a_j x_j \geq a_0 + 1 \right\}. \tag{1.4}$$

Итак, если $f \in \mathfrak{F}_\nu(M)$, $m_\nu(f) = 1$, то $f \in \mathfrak{F}_{1-\nu}(M)$, $m_{1-\nu}(f) = 1$ $(\nu = 0, 1)$. Обозначим $\mathfrak{T}(M)$ множество всех пороговых функций, заданных на $M$.

**Утверждение 1.5.** *Условие*

$$P_0(f) \cap P_1(f) = \varnothing \tag{1.5}$$

*является необходимым и достаточным для того, чтобы функция $f$ из класса $\mathfrak{F}(M)$ была пороговой.*

*Доказательство.* Пусть $f \in \mathfrak{T}(M)$, тогда для $M_\nu(f)$ $(\nu = 0, 1)$ существуют описания в виде (1.3) и (1.4). Отсюда следует соотношение (1.5). Достаточность вытекает из теоремы о разделяющей гиперплоскости (см., например, [69]). ∎

## 1.2. Величина коэффициентов характеристической системы

С каждой функцией $f \in \mathfrak{T}(M)$ в $(n + 2)$-мерном пространстве связан конус $K(f)$ *разделяющих функционалов*, описываемый следующей системой линейных неравенств относительно переменных $(a_0, \ldots, a_{n+1})$:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{для всех } (x_1, \ldots, x_n) \in M_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{для всех } (x_1, \ldots, x_n) \in M_1(f); \\ a_{n+1} \ge 0. \end{cases} \tag{1.6}$$

Любое решение $(a_0, \ldots, a_{n+1})$ этой системы при $a_{n+1} > 0$ определяет некоторое пороговое неравенство (1.2) для функции $f$. Верно и обратное: коэффициенты $(a_0, \ldots, a_{n+1})$ любого порогового неравенства функции $f \in \mathfrak{F}(M)$ удовлетворяют системе (1.6) при некотором положительном

значении $a_{n+1}$. Приведенная конструкция хорошо известна в пороговой логике (см., например, [39]).

Наряду с (1.6) рассмотрим систему

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{для всех } (x_1,\dots,x_n) \in N_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{для всех } (x_1,\dots,x_n) \in N_1(f); \\ a_{n+1} \ge 0. \end{cases} \tag{1.7}$$

**Лемма 1.6.** *Для любой* $f \in \mathfrak{T}(M)$ *системы* (1.6) *и* (1.7) *эквивалентны.*

*Доказательство.* Достаточно проверить, что система (1.6) является следствием системы (1.7). Действительно, если $N_0(f) = \{d^{(i)} : i = 1,\dots,s\}$, то для любого $x = (x_1,\dots,x_n) \in M_0(f)$ найдутся $\delta_i \ge 0$, такие, что $\sum\limits_{i=1}^{s} \delta_i = 1$, $x = \sum\limits_{i=1}^{s} \delta_i d^{(i)}$. Отсюда получаем, что неравенство $\sum\limits_{j=1}^{n} a_j x_j \le a_0$ из системы (1.6) есть линейная комбинация неравенств первой группы системы (1.7) с положительными коэффициентами $\delta_i$ $(i = 1,\dots,s)$. Для произвольного $x \in M_1(f)$ можно провести аналогичные рассуждения. ∎

**Лемма 1.7.** [105, стр. 54] *Пусть* $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$, $a_0 = (a_{i0}) \in \mathbb{Z}^m$, $|a_{ij}| \le \alpha$ $(i = 1,2,\dots,m;\ j = 0,1,\dots,n)$. *Для координат любой точки* $x$ *из* $N(A,a_0)$ *выполняется неравенство* $|x_j| < (n+1)(\alpha\sqrt{n})^n$ $(j = 1,\dots,n)$.

**Следствие 1.8.** *Если* $M(A,a_0)$ *конечно, то для координат любой точки* $x$ *из* $M(A,a_0)$ *выполняется неравенство* $|x_j| < (n+1)(\alpha\sqrt{n})^n$ $(j = 1,\dots,n)$.

Согласно следствию 1.8 для любой точки $(x_1,\dots,x_n) \in M \in \mathfrak{M}(n,l,\gamma)$ справедливо

$$|x_j| \le (n+1)(\gamma\sqrt{n})^n \qquad (j = 1,2,\dots,n). \tag{1.8}$$

Из теории линейных неравенств (см., например, [88]) следует, что в $K(f)$ существует такая система векторов $\widetilde{b^{(1)}},\dots,\widetilde{b^{(s)}}$ (порождающая

система), что любой $b$ из $K(f)$ является их линейной комбинацией с неотрицательными коэффициентами. Кроме того, $\widetilde{b^{(i)}}$ $(i = 1, \ldots, s)$ может быть выбран так, что его $j$-я компонента $b_j^{(i)}$ с точностью до знака совпадает с минором порядка $(n+1)$, полученным из матрицы, составленной из коэффициентов системы (1.6) или (1.7). Используя неравенство Адамара (см., например, [60]) и оценку (1.8), получаем

$$|b_j^{(i)}| \le (n+1)^{\frac{n+1}{2}} \left((n+1)(\gamma\sqrt{n})^n\right)^n \qquad (j = 0, n+1;\ i = 1, 2, \ldots, s);$$

$$|b_j^{(i)}| \le (n+1)^{\frac{n+1}{2}} \left((n+1)(\gamma\sqrt{n})^n\right)^{n-1} \qquad (j = 1, 2, \ldots, n;\ i = 1, 2, \ldots, s),$$

поэтому

$$|b_j^{(i)}| \le (n+1)^{\frac{n+3}{2}} (\gamma\sqrt{n})^{n^2} \qquad (j = 0, 1, \ldots, n+1;\ i = 1, 2, \ldots, s). \qquad (1.9)$$

Обозначим выражение в правой части неравенства (1.9) через $\chi(n, \gamma)$. Из (1.9) вытекает

**Следствие 1.9.** *Пусть $M \in \mathfrak{M}(n, l, \gamma)$. Для любой функции $f \in \mathfrak{T}(M)$ существует пороговое неравенство* (1.2) *с целочисленными коэффициентами, ограниченными по модулю величиной $\chi(n, \gamma)$.*

**Следствие 1.10.** *Пусть $M \in \mathfrak{M}(n, l, \gamma)$. Для любого $\nu = 0, 1$ и любой функции $f \in \mathfrak{F}_\nu(M)$ существует характеристическая система $Ax \le a_0$ с целочисленными коэффициентами, ограниченными по модулю величиной $\chi(n, \gamma)$.*

*Доказательство.* Рассмотрим пороговую функцию $f_i$, для которой $M_0(f_i)$ описывается $i$-м неравенством системы $Ax \le a_0$ и воспользуемся следствием 1.9. ∎

Для пороговых функций $k$-значной логики (т. е. при $M = E_k^n$) оценка (1.9) примет вид:

$$|b_j^{(i)}| \le (n+1)^{\frac{n+3}{2}} \left((k-1)\sqrt{n}\right)^{n^2}.$$

В [104] для этого частного случая найдена более точная оценка:

**Лемма 1.11.** [104] *Для любой функции* $f \in \mathfrak{T}(E_k^n)$ *существует пороговое неравенство* (1.2)*, в котором коэффициенты* $a_0, a_1, \ldots, a_n$ *— целые, причем*

$$|a_0| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^n}(k-1)^n, \quad |a_j| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^{n+1}}(k-1)^{n-1} \quad (j = 1, 2, \ldots, n).$$

При $k = 2$ приведенные в лемме 1.11 оценки превращаются в оценки величины коэффициентов порогового неравенства функций из $\mathfrak{T}(E_2^n)$:

$$|a_0| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^n}, \quad |a_j| \le \frac{(n+1)^{\frac{n}{2}+1}}{2^{n+1}} \quad (j = 1, 2, \ldots, n). \tag{1.10}$$

Оценки (1.10) дополняет нижняя оценка [141] величины коэффициентов порогового неравенства. В [141] указан метод построения по произвольному $n = 2^q$ ($q \ge 2$, $q \in \mathbb{N}$) такой функции $f \in \mathfrak{T}(E_2^n)$, коэффициенты порогового неравенства которой нельзя сделать меньше величины

$$\frac{1}{n} e^{-4n^\beta} 2^{\frac{n \ln n}{2} - n - 1},$$

где $\beta = \log(3/2)$.

## 1.3. Число вершин в $P_0(f)$ и $P_1(f)$

Вначале рассмотрим несколько вспомогательных утверждений о количестве вершин в выпуклой оболочке целочисленных точек полиэдра. Пусть $A = (a_{ij}) \in \mathbb{Z}^{m \times n}$, $a_0 = (a_{i0}) \in \mathbb{Z}^m$, $|a_{ij}| \le \alpha$ ($i = 1, 2, \ldots, m$; $j = 0, 1, \ldots, n$).

Введем обозначение:

$$\xi_n(m) = \binom{m - \lfloor \frac{n-1}{2} \rfloor - 1}{\lfloor \frac{n}{2} \rfloor} + \binom{m - \lfloor \frac{n}{2} \rfloor - 1}{\lfloor \frac{n-1}{2} \rfloor}.$$

В частности, $\xi_1(m) = 2$, $\xi_2(m) = m$, $\xi_3(m) = 2m - 4$. При $n \ge 4$, $m \ge n + 1$ выполняется неравенство $\xi_n(m) < m^{\lfloor n/2 \rfloor}$.

**Лемма 1.12.** [10] *Справедливо неравенство*

$$|N(A, a_0)| \leq (n+1)^{n+1} n!\, \xi_n(m) \left(1 + \frac{1}{2}\log(n+1) + \log\Delta\right)^{n-1},$$

*где* $\Delta$ *равен максимуму из абсолютных значений миноров порядка* $n+1$ *матрицы*

$$\begin{pmatrix} -A & a_0 \\ 0 & 1 \end{pmatrix}.$$

Оценивая $\Delta$ сверху с помощью неравенства Адамара (см., например, [60]): $\Delta \leq (\alpha\sqrt{n+1})^{n+1}$, получаем

**Следствие 1.13.** *Справедливо неравенство*

$$|N(A, a_0)| \leq (n+1)^{n+1} n!\, \xi_n(m) \left(1 + \left(\frac{n}{2} + 1\right)\log(n+1) + (n+1)\log\alpha\right)^{n-1}.$$

**Следствие 1.14.** *При* $n \geq 1$, $\alpha \geq 1$ *справедливо неравенство*

$$|N(A, a_0)| \leq n^{4n} \xi_n(m) \log^{n-1}(\alpha+1). \tag{1.1}$$

*Доказательство.* Проверим, что правая часть неравенства в следствии 1.13 не превосходит правой части в оценке (1.1).

Если $n = 1$, то $|N(A, a_0)| \leq 2$ и неравенство (1.1) выполнено.

При $n = 2$, $\alpha \geq 1$ получаем

$$|N(A, a_0)| \leq 3^3 \cdot 2! \log(2 \cdot 3^2 \cdot \alpha^3) = 54(\log 18 + 3\log\alpha) <$$

$$< 226 + 162\log\alpha < 256\log(\alpha+1).$$

При $n = 3$, $\alpha \geq 1$ получаем

$$|N(A, a_0)| \leq 4^4 \cdot 3! \log(2 \cdot 4^{\frac{5}{2}} \cdot \alpha^4)^2 = 1536(6 + 4\log\alpha)^2 < 531441\log^2(\alpha+1).$$

При $n \geq 4$, $\alpha \geq 1$, воспользовавшись неравенствами $(n+1)^n < en^n$ и $\log(n+1) + \log\alpha \leq \log(n+1) \cdot \log(\alpha+1)$, получаем

$$|N(a, a_0)| \leq (n+1)^{n+1} n! \xi_n(m) \left(\log\left(2(n+1)^{\frac{n}{2}+1}\alpha^{n+1}\right)\right)^{n-1} <$$

$$< (n+1)^{n+1} n^n \xi_n(m) \Big( \log\big((n+1)\alpha\big)^{n+1} \Big)^{n-1} =$$

$$= (n+1)^{n+1} n^n (n+1)^{n-1} \xi_n(m) \log^{n-1}\big((n+1)\alpha\big) \le$$

$$\le (n+1)^{2n} n^n \xi_n(m) \log^{n-1}(n+1) \log^{n-1}(\alpha+1) <$$

$$< e^2 n^{2n} n^n \xi_n(m) \log^{n-1}(n+1) \log^{n-1}(\alpha+1) <$$

$$< n^{4n} \xi_n(m) \log^{n-1}(\alpha+1),$$

что завершает доказательство. ∎

Для случая полиэдра (многогранника) задачи о рюкзаке можно получить более точную оценку. Обозначим $N(k, a_0, a_1, \ldots, a_n)$ множество вершин выпуклой оболочки решений системы

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0, \\ 0 \le x_j \le k-1, \quad x_j \in \mathbb{Z} \quad (j = 1, 2, \ldots, n). \end{cases}$$

**Лемма 1.15.** [10] *При любых n, k и любых* $a_0, a_1, \ldots, a_n$

$$|N(k, a_0, a_1, \ldots, a_n)| \le 2^n n \log(2n) \big(1 + \log(k+1)\big)^{n-1}.$$

Как и прежде, предположим, что $M = P \cap \mathbb{Z}^n \in \mathfrak{M}(n, l, \gamma)$ для некоторого политопа $P \in \mathfrak{P}(n, l, \gamma)$; $f \in \mathfrak{F}_\nu(M)$. Пусть $Cx \le c_0$ — система, описывающая $P$. Для $\nu = 0, 1$ рассмотрим систему линейных неравенств, полученную из системы $Cx \le c_0$ добавлением к ней неравенств $Ax \le a_0$ из (1.1). Очевидно, $\gamma < \chi(n, \gamma)$.

Так как максимальный по модулю коэффициент $\alpha$ в новой системе ограничен величиной $\chi(n, \gamma)$, то из следствия 1.14 и следствия 1.10 получаем:

$$|N_\nu(f)| \le n^{4n} \xi_n\big(l + m_\nu(f)\big) \log^{n-1}\big(\chi(n, \gamma) + 1\big). \tag{1.11}$$

Справедливо

**Утверждение 1.16.** *При* $n \geq 1$, $l \geq n+1$, $\gamma \geq 1$, $M \in \mathfrak{M}(n,l,\gamma)$ *для любых* $\nu = 0,1$ *и* $f \in \mathfrak{F}_\nu(M)$

$$|N_\nu(f)| \leq n^{10n-6}\left(l + m_\nu(f)\right)^{\left\lfloor \frac{n}{2} \right\rfloor} \log^{n-1}(\gamma+1). \qquad (1.12)$$

*Доказательство.* Проверим, что правая часть в неравенстве (1.11) не превосходит правой части в (1.12).

Если $n = 1$, то $|N_\nu(f)| \leq 2$ и неравенство (1.12) выполнено.

При $n = 2$ получаем:

$$|N_\nu(f)| \leq 2^8\left(l + m_\nu(f)\right)\log\left(3^{\frac{5}{2}}(\gamma\sqrt{2})^4 + 1\right) <$$

$$< 2^8\left(l + m_\nu(f)\right)(7 + 4\log\gamma) < 2^{14}\left(l + m_\nu(f)\right)\log(\gamma+1).$$

При $n = 3$, учитывая, что $\xi_3\left(l + m_\nu(f)\right) = 2\left(l + m_\nu(f)\right) - 4$, получаем:

$$|N_\nu(f)| \leq 3^{12}\left(2\left(l + m_\nu(f)\right) - 4\right)\log^2\left(4^3(\gamma\sqrt{3})^9 + 1\right) <$$

$$< 3^{13}\left(l + m_\nu(f)\right)\log^2(2^{14}\gamma) < 3^{24}\left(l + m_\nu(f)\right)\log^2(\gamma+1).$$

При $n \geq 4$, воспользовавшись неравенством $\log(1+n) < \log n + \dfrac{1}{n\ln 2}$, получаем:

$$|N_\nu(f)| \leq n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\log^{n-1}\left((n+1)^{\frac{n+3}{2}}(\gamma\sqrt{n})^{n^2} + 1\right) <$$

$$< n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\left(\frac{n+3}{2}\log(n+1) + n^2\log\gamma + \frac{n^2}{2}\log n + \frac{1}{n\ln 2}\right)^{n-1} <$$

$$< n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\left(\frac{n+3}{2}\log n + \frac{n+3}{2n\ln 2} + n^2\log\gamma + \frac{n^2}{2}\log n + \frac{1}{n\ln 2}\right)^{n-1} <$$

$$< n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\left(\frac{n^2+n+3}{2}\log n + n^2\log\gamma + \frac{1}{2\ln 2} + \frac{5}{2n\ln 2}\right)^{n-1} <$$

$$< n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\left(\frac{n^2+n+3}{2}\log n + n^2\log\gamma + 2\right)^{n-1} <$$

$$< n^{4n}\,\xi_n\left(l + m_\nu(f)\right)\cdot n^{2(n-1)}\cdot\log^{n-1} n\cdot n^{2(n-1)}\cdot\log^{n-1}(\gamma+1)\cdot 2^{n-1} <$$

$$< n^{10n-6}\,\xi_n\big(l + m_\nu(f)\big)\log^{n-1}(\gamma+1),$$

откуда, учитывая $\xi_n\big(l + m_\nu(f)\big) < \big(l + m_\nu(f)\big)^{\lfloor \frac{n}{2} \rfloor}$ (при $n \geq 3$), получаем неравенство (1.12). ∎

Таким образом, для всякой $f \in \mathfrak{F}_\nu(M)$ ($\nu = 0, 1$) при любом фиксированном $n$ число крайних точек $|N_\nu(f)|$ ограничено сверху полиномом от трех переменных: $l$, $m_\nu(f)$ и $\log\gamma$.

**Следствие 1.17.** *При $n \geq 1$, $k \geq 2$ для любых $\nu = 0, 1$ и $f \in \mathfrak{F}_\nu(E_k^n)$*

$$|N_\nu(f)| \leq n^{10n-6}\left(2n + m_\nu(f)\right)^{\lfloor \frac{n}{2} \rfloor}\log^{n-1} k.$$

*Доказательство.* Достаточно в (1.12) положить $l = 2n$, $\gamma = k - 1$. ∎

**Утверждение 1.18.** *При $n \geq 1$, $l \geq n+1$, $\gamma \geq 1$, $M \in \mathfrak{M}(n, l, \gamma)$ для любых $\nu = 0, 1$ и $f \in \mathfrak{T}(M)$*

$$|N_\nu(f)| \leq n^{10n-5}\,l^{\lfloor \frac{n}{2} \rfloor}\log^{n-1}(\gamma+1). \tag{1.13}$$

*Доказательство.* Для всех $n \geq 1$ имеем $(l+1)^{\lfloor \frac{n}{2} \rfloor} \leq nl^{\lfloor \frac{n}{2} \rfloor}$. При $n = 1, 2$ это неравенство проверяется непосредственно, а при $n \geq 3$ следует из неравенств

$$\left(1 + \frac{1}{l}\right)^{\lfloor \frac{n}{2} \rfloor} < \left(1 + \frac{1}{\lfloor \frac{n}{2} \rfloor}\right)^{\lfloor \frac{n}{2} \rfloor} < e.$$

Теперь из (1.12), полагая $m_\nu(f) = 1$, получаем:

$$|N_\nu(f)| \leq n^{10n-6}\,(l+1)^{\lfloor \frac{n}{2} \rfloor}\log^{n-1}(\gamma+1) \leq n^{10n-5}\,l^{\lfloor \frac{n}{2} \rfloor}\log^{n-1}(\gamma+1).$$

что завершает доказательство. ∎

Таким образом, для всякой $f \in \mathfrak{T}(M)$ ($\nu = 0, 1$) при любом фиксированном $n$ число крайних точек $|N_\nu(f)|$ ограничено сверху полиномом от двух переменных: $l$ и $\log\gamma$, а именно, при фиксированном $n$

$$|N_\nu(f)| = O\left(l^{\lfloor \frac{n}{2} \rfloor}\log^{n-1}\gamma\right).$$

Применим утверждение 1.18 к пороговым функциям $k$-значной логики ($f \in \mathfrak{T}(E_k^n)$):

**Следствие 1.19.** *При $n \geq 1$, $k \geq 2$ для любых $\nu = 0, 1$ и $f \in \mathfrak{T}(E_k^n)$*

$$|N_\nu(f)| \leq n^{11n-5} \log^{n-1} k. \tag{1.14}$$

*Доказательство.* В (1.13) положим $l = 2n$, $\gamma = k - 1$:

$$|N_\nu(f)| \leq n^{10n} (2n)^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} k \leq n^{11n-5} \log^{n-1} k,$$

что требовалось доказать. ∎

На самом деле, для этого частного случая на основе леммы 1.15 можно получить более точную оценку. А именно, справедливо

**Следствие 1.20.** *Для любой функции $f \in \mathfrak{T}(E_k^n)$*

$$|N_\nu(f)| \leq 2^n n \log(2n) \big(1 + \log(k+1)\big)^{n-1}. \tag{1.15}$$

Заметим, что при фиксированном $n$ оба неравенства: (1.14) и (1.15) — приводят к одинаковой асимптотической оценке:

$$|N_\nu(f)| = O(\log^{n-1} k) \qquad (k \to \infty).$$

Рассмотрим задачу $\mathscr{G}_0$ описания множества $M(A, a_0)$: по заданным $A$ и $a_0$ построить список крайних точек и экстремальных векторов множества $\operatorname{Conv} M(A, a_0)$, а также систему линейных неравенств, множество решений которой совпадает с $\operatorname{Conv} M(A, a_0)$. В [102] предлагается алгоритм, решающий эту задачу. Этот алгоритм опирается на процедуру Ленстры [147] решения в целых числах системы линейных неравенств или доказательства ее несовместности и при любом фиксированном $n$ является полиномиальным. Таким образом, справедлива

**Лемма 1.21.** [102, 105] *При любом фиксированном* $n$ *для задачи* $\mathscr{G}_0$ *существует полиномиальный от* $m$ *и* $\log \alpha$ *алгоритм ее решения.*

Рассмотрим задачу $\mathfrak{G}$ нахождения множества крайних точек $N_\nu(f)$ и множества всех неравенств–граней политопа $P_\nu(f)$ для функции $f \in \mathfrak{F}_\nu(M)$ по заданному $\nu \in \{0,1\}$, заданной целочисленной системе $Cx \leq c_0$, описывающей $M$, и системе $Ax \leq a_0$, описывающей $M_\nu(f)$. Из утверждения 1.18 и леммы 1.21 вытекает

**Утверждение 1.22.** *Пусть* $f \in \mathfrak{F}_\nu(M)$ $(\nu = 0,1)$ *задана характеристической системой* $Ax \leq a_0$, $A \in \mathbb{Z}^{m_\nu(f)\times n}$, $a_0 \in \mathbb{Z}^n$, *коэффициенты которой удовлетворяют неравенству* (1.9). *Тогда для задачи* $\mathfrak{G}$ *существует при фиксированном* $n$ *полиномиальный от* $m_\nu(f)$, $l$ *и* $\log \gamma$ *алгоритм ее решения.*

## 1.4. Мощностные свойства исследуемых классов функций

Оценка числа пороговых функций в рассматриваемых классах является сложной задачей уже при $k = 2$. В частности, для величины $|\mathfrak{T}(E_2^n)|$ известна лишь полученная Ю. А. Зуевым [37, 38] и уточненная А. А. Ирматовым [40] асимптотика ее логарифма.

Обзор работ, посвященных исследованию мощности класса $\mathfrak{T}(E_2^n)$ и смежным вопросам см. в [39]. Из результата Л. Шлёфли [159] о числе открытых областей, на которые $2^n$ гиперплоскостей могут разбивать $n$-мерное пространство, непосредственно следует, что

$$|\mathfrak{T}(E_2^n)| < 2\sum_{j=0}^{n}\binom{2^n-1}{j} < 2^{n^2}.$$

Эта (или близкая) оценка выводится в [64, 124, 158, 164], см. также [154, 165]. С. Яджима и Т. Ибараки [166] (см. также [120]) получили

нижнюю оценку $|\mathfrak{T}(E_2^n)| > 2^{n^2/2}$. Ю. А. Зуев [37, 38], опираясь на результат А. М. Одлыжко [157] о случайных $\pm 1$ матрицах, показал, что для достаточно больших $n$

$$|\mathfrak{T}(E_2^n)| > 2^{n^2(1-10/\ln n)}, \tag{1.16}$$

тем самым установив асимптотическое равенство $\log|\mathfrak{T}(E_2^n)| \simeq n^2$.

Оценка (1.16) улучшена А. А. Ирматовым [40] (см. также [41, 142]). Им показано [40], что для достаточно больших $n$ имеет место неравенство

$$|\mathfrak{T}(E_2^n)| > 2^{n^2(1-7/\ln n)}|\mathfrak{T}(E_2^{\lfloor 7(n-1)\ln 2/\ln(n-1)\rfloor})|.$$

Для пороговых функций $k$-значной логики В. Н. Шевченко [103, 105] показал, что

$$\log|\mathfrak{T}(E_k^n)| \lesssim n^2 \log k \qquad (n \to \infty).$$

Нижнюю оценку, справедливую для достаточно большого $n$, установили А. А. Ирматов и Ж. Д. Ковиянич [42]:

$$|\mathfrak{T}(E_k^n)| \geq \frac{1}{2}\binom{k^n}{\lfloor n-4-2n/\log_k n\rfloor}|\mathfrak{T}(E_k^{\lfloor 2n/\log_k n+4\rfloor})|.$$

Таким образом,

$$\log|\mathfrak{T}(E_k^n)| \sim n^2 \log k \qquad (n \to \infty). \tag{1.17}$$

Пусть, как обычно, $M \in \mathfrak{M}(n, l, \gamma)$. Рассмотрим класс $\mathfrak{F}_\nu(M, m)$ ($\nu = 0, 1$) тех функций $f$ из $\mathfrak{F}_\nu(M)$, для которых $m_\nu(f) = m$.

**Теорема 1.23.** *При любых $\gamma \geq 1$, $m \geq 1$*

$$\log|\mathfrak{F}_\nu(M, m)| \lesssim mn^3 \log(\gamma\sqrt{n}) \qquad (n \to \infty).$$

*Доказательство.* Из следствия 1.10 получаем, что системами $m$ неравенств с целочисленными коэффициентами, ограниченными по абсолютной величине числом $\chi(n, \gamma)$, описываются все возможные функции

из класса $\mathfrak{F}_\nu(M,m)$ ($\nu = 0, 1$). Таким образом,

$$|\mathfrak{F}_\nu(M,m)| \le (2\cdot\chi(n,\gamma)+1)^{m(n+1)} = (2\cdot(n+1)^{\frac{n+3}{2}}(\gamma\sqrt{n})^{n^2}+1)^{m(n+1)}$$

и, следовательно,

$$\log|\mathfrak{F}_\nu(M,m)| \lesssim m(n+1)\cdot\left(\frac{n+3}{2}\log(n+1)+n^2\log(\gamma\sqrt{n})\right),$$

откуда и следует утверждение теоремы. ∎

Заметив, что $\mathfrak{F}_0(M,1) = \mathfrak{F}_1(M,1) = \mathfrak{T}(M)$, получаем

**Следствие 1.24.** *Для любого* $\gamma \ge 1$

$$\log|\mathfrak{T}(M)| \lesssim n^3\log(\gamma\sqrt{n}) \qquad (n\to\infty).$$

Для случая функций $k$-значной логики в [103, 105] найдена более точная оценка:

$$\log|\mathfrak{F}_\nu(E_k^n,m)| \lesssim mn^2\log(k\sqrt{n}) \quad (\nu = 0,1).$$

Отдельно рассматривалась проблема получения оценки числа $|\mathfrak{T}(E_k^2)|$.

В [144] установлено взаимно-однозначное соответствие между множеством всех «линейных разбиений» (linear partitions) произвольного дискретного множества $M \subseteq \mathbb{Z}^2$ (т. е. всех пороговых функций $f: M \to \{0,1\}$, не равных тождественно 0 или 1) и множеством упорядоченных пар смежных точек в $M$. Две точки $x$ и $y$ в $M$ назовем *смежными*, если отрезок $[x, y]$ не содержит других точек из $M$ (см. также раздел 3.10.2). На этой основе в [144] получено:

$$|\mathfrak{T}(E_k^2)| = 2 + \sum_{\substack{-k<i,j<k\\ \text{НОД}(i,j)=1}}(k-|i|)(k-|j|) = \frac{6k^4}{\pi^2} + O(k^3\log k). \qquad (1.18)$$

В [112] (см. также [156, 162]) установлено:

$$|\mathfrak{T}(E_p\times E_q)| = \frac{6p^2q^2}{\pi^2} + O(p^2q\log q + pq^2\log\log q).$$

Чуть более точная оценка получена в [114]:

$$|\mathfrak{T}(E_p \times E_q)| = \frac{6p^2q^2}{\pi^2} + O(p^2 q \log q).$$

## 1.5. Соотношение между классами $\mathfrak{T}(M)$ и $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$

В этом параграфе рассмотрим вопрос о соотношении классов $\mathfrak{T}(M)$ и $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. Как уже отмечалось,

$$\log |\mathfrak{F}_0(E_2^n) \cap \mathfrak{F}_1(E_2^n)| = \log |\mathfrak{F}(E_2^n)| = 2^n,$$

в то же время $\log |\mathfrak{T}(E_2^n)| \sim n^2$.

Вначале для $k \geq 2$, $n \geq 4$ приведем пример функции из класса $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$, не являющейся пороговой. Для четного $n \geq 4$ такой пример предлагался в [105, 107]. Здесь мы обобщим конструкцию построения таких примеров на случай произвольного $n \geq 4$.

**Пример 1.25.** Пусть $M = E_k^n$, $n = 2m + \lambda$ для некоторого натурального $m \geq 2$ и $\lambda \in \{0, 1\}$. Обозначим через $y_{ij} \in E_k^n$ вектор, все компоненты которого суть 0, кроме $i$-й и $(m+j)$-й компонент, равных 1. Предположим, что $M_0(f)$ содержит множество

$$\left\{ x \in E_k^n : 2\sum_{j=1}^{m} x_j + 3\sum_{j=m+1}^{n} x_j \leq 4 \right\},$$

а также все точки гиперплоскости

$$2\sum_{j=1}^{m} x_j + 3\sum_{j=m+1}^{n} x_j = 5 \tag{1.19}$$

вида $y_{ii}$ $(i = 1, \ldots, m)$.

Покажем, что $f \in \mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$, т. е. $P_0(f) \cap P_1(f) \cap \mathbb{Z}^n = \varnothing$. Очевидно, что с этой целью достаточно проверить точки из $E_k^n$, лежащие на гиперплоскости (1.19). Из рассмотрения уравнения (1.19) получаем,

что эти точки суть $y_{ij}$ $(i = 1, \ldots, m;\ j = 1, \ldots, m + \lambda)$. Среди них точки $y_{ii}$ $(i = 1, \ldots, m)$ принадлежат $M_0(f)$, а остальные — $M_1(f)$. Максимум функции $x_i + x_{m+j}$, взятый по всем таким точкам достигается в $y_{ij}$, следовательно, никакая из этих точек не является выпуклой комбинацией остальных. Таким образом, $P_0(f) \cap P_1(f) \cap \mathbb{Z}^n = \varnothing$, откуда по утверждению 1.4 получаем, что $f \in \mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$.

Теперь покажем, что $f \notin \mathfrak{T}(E_k^n)$. Действительно, $P_0(f)$ и $P_1(f)$ содержат общую точку

$$\frac{1}{m}\sum_{j=1}^{m} y_{jj} = \frac{1}{m}\left(\sum_{j=1}^{m-1} y_{j,j+1} + y_{m1}\right),$$

т. е. точку $x = \left(\frac{1}{m}, \ldots, \frac{1}{m}\right)$ при четном $n$ и точку $x = \left(\frac{1}{m}, \ldots, \frac{1}{m}, 0\right)$ при нечетном $m$. Таким образом, $P_0(f) \cap P_1(f) \neq \varnothing$, откуда по утверждению 1.5 получаем, что $f \notin \mathfrak{T}(E_k^n)$.

**Пример 1.26.** Пусть теперь $n = 3$, $k \geq 4$, $M = E_k^3$ и $M_0(f)$ содержит множество $\{(x_1, x_2, x_3) \in E_k^3 :\ x_1 + x_2 + 2x_3 \leq 2\}$, а также точки $(3, 0, 0)$, $(2, 1, 0)$, $(0, 1, 1)$, которые, как легко проверить, лежат на плоскости, описываемой уравнением $x_1 + x_2 + 2x_3 = 3$. На этой гиперплоскости также лежат следующие точки из $M_1(f)$: $(0, 3, 0)$, $(1, 2, 0)$, $(1, 0, 1)$. Как и в примере выше, $P_0(f) \cap P_1(f) \cap \mathbb{Z}^3 = \varnothing$, откуда по утверждению 1.4 получаем, что $f \in \mathfrak{F}_0(E_k^3) \cap \mathfrak{F}_1(E_k^3)$. Однако $f \notin \mathfrak{T}(E_k^3)$, т. к. $P_0(f)$ и $P_1(f)$ содержат общие точки, например, точку $(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}) = \frac{1}{4}(3, 0, 0) + \frac{3}{4}(0, 1, 1) = \frac{1}{4}(0, 3, 0) + \frac{3}{4}(1, 0, 1)$.

**Пример 1.27.** Для случая $n = 3$, $k = 3$ рассмотрим функцию $f \in \mathfrak{F}(E_3^3)$, такую, что $M_0(f)$ содержит точки $(0, 0, 0)$, $(0, 0, 1)$, $(0, 0, 2)$, $(0, 1, 0)$, $(0, 1, 1)$, $(1, 0, 2)$. Остальные точки из $E_3^3$ принадлежат $M_1(f)$. Легко проверить, что все точки из $M_0(f)$ удовлетворяют неравенству $x_1 + x_2 \leq 1$, тогда, как все точки из $M_1(f)$ — неравенству $x_1 + x_2 \geq 1$. Чтобы доказать, что $P_0(f) \cap P_1(f)$ не содержит точек из $E_3^3$, достаточно проверить лишь

точки, лежащие на плоскости $x_1 + x_2 = 1$, а именно: $(0,1,0)$, $(0,1,1)$, $(1,0,2)$ из $M_0(f)$ и $(1,0,0)$, $(1,0,1)$, $(0,1,2)$ из $M_1(f)$. Очевидно, что $P_0(f) \cap P_1(f) \cap \mathbb{Z}^3 = \varnothing$ и, следовательно, $f \in \mathfrak{F}_0(E_3^3) \cap \mathfrak{F}_1(E_3^3)$. С другой стороны, т. к. $P_0(f)$ и $P_1(f)$ содержат общие точки, например, точку $(\frac{1}{2}, \frac{1}{2}, 1) = \frac{1}{2}(0,1,0) + \frac{1}{2}(1,0,2) = \frac{1}{2}(1,0,0) + \frac{1}{2}(0,1,2)$, то $f \notin \mathfrak{T}(E_3^3)$. Заметим, что данный пример легко распространить на случай произвольного $k \geq 2$.

Построенные примеры показывают, что при $n \geq 3$, $k \geq 2$ класс $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$ является собственным подмножеством класса $\mathfrak{T}(E_k^n)$ (см. также [105, стр. 169]). Оказывается, что при $n = 1, 2$, $k \geq 3$ эти классы совпадают. Следующая теорема приведена в [105, стр. 169] без доказательства.

**Теорема 1.28.** *Если $k \geq 3$, то $\mathfrak{T}(E_k^2) = \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$.*

*Доказательство.* Очевидно, что $\mathfrak{T}(E_k^2) \subseteq \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$. Докажем обратное включение.

Рассмотрим произвольную функцию $f \in \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$. Для нее образуем вектор $u = (u_1, \ldots, u_4) \in E_2^4$, где $u_1 = f(0,0)$, $u_2 = f(0, k-1)$, $u_3 = f(k-1, k-1)$, $u_4 = f(k-1, 0)$, и обозначим через $\theta(f)$ величину $\sum\limits_{j=1}^{3} |u_{j+1} - u_j| + |u_4 - u_1|$. Очевидно, что $\theta(f)$ — четно и не превосходит 4. Рассмотрим каждый из следующих случаев:

1. $\theta(f) = 0$;

2. $\theta(f) = 2$;

3. $\theta(f) = 4$.

В случае $\theta(f) = 0$ во всех вершинах квадрата $E_k^2$ функция $f$ принимает одно и то же значение $\nu \in \{0, 1\}$. Так как $f \in \mathfrak{F}_\nu(E_k^2)$, то $f(x) = \nu$ для всех $x \in E_k^2$. Очевидно, что в этом случае $f \in \mathfrak{T}(E_k^2)$.

Прежде чем рассмотреть случай $\theta(f) = 2$, докажем следующее вспомогательное утверждение.

**Лемма 1.29.** *Пусть* $\Phi$ *— выпуклый многоугольник с вершинами* $R_1, \ldots, R_s$ *(в положительном направлении обхода),* $s \geq 2$, $T$ *— конечная система точек,*

$$T = T_0 \cup T_1 \subset \Phi, \tag{1.20}$$

$T_0 \cap T_1 = \varnothing$. *Тогда для любого* $s'$ $(1 \leq s' \leq s-1)$ *пересечение множеств* $\Phi_0 = \mathrm{Conv}\left(\{R_i, i = 1, \ldots, s'\} \cup T_0\right)$ *и* $\Phi_1 = \mathrm{Conv}\left(\{R_i, i = s'+1, \ldots, s\} \cup T_1\right)$ *либо пусто, либо содержит одну из точек множества* $T$.

*Доказательство.* Стороны многоугольника $\Phi_\nu$ $(\nu = 0, 1)$, не являющиеся также сторонами исходного многоугольника $\Phi$ (т. е. сторонами $R_1R_2$, $R_2R_3, \ldots, R_{s'-1}R_{s'}$ для $\nu = 0$ и $R_{s'+1}R_{s'+2}, \ldots, R_{s-1}R_s$ для $\nu = 1$), назовем $\varsigma$-сторонами. Прямые $R_{s'}R_{s'+1}$ и $R_sR_1$ являются опорными для многоугольника $\Phi_\nu$ $(\nu = 0, 1)$. Действительно, $\Phi_\nu$ $(\nu = 0, 1)$ имеет с каждой из них общую точку: точку $R_{s'}$ при $\nu = 0$ или $R_{s'+1}$ при $\nu = 1$ с прямой $R_{s'}R_{s'+1}$ и точку $R_1$ при $\nu = 0$ или $R_s$ при $\nu = 1$ с прямой $R_sR_1$ — и ввиду (1.20) лежит по одну сторону от каждой из этих прямых (см. рис. 1.1).

Известно (см., например, [6, стр. 190]), что при положительном обходе границы выпуклого многоугольника вектор внешней нормали, построенный к текущей стороне, вращается также в положительном направлении, причем направление сохранится, если в обходе учитывать внешние нормали к опорным прямым, построенным произвольным образом в вершинах многоугольника. В последнем случае за нормалями, построенными к очередной стороне, рассматривается нормаль к опорной прямой в инцидентной (в направлении положительного обхода) вершине, затем — нормаль к следующей стороне и т. д.

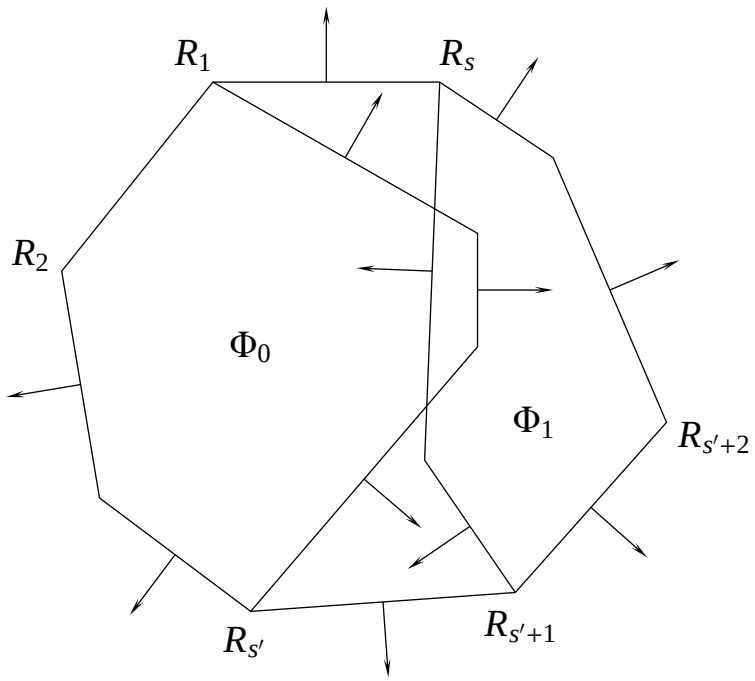


Рис. 1.1

Построим нормали к $\varsigma$-сторонам многоугольников $\Phi_0$ и $\Phi_1$ и к опорным прямым $R_{s'}R_{s'+1}$ и $R_sR_1$. Теперь упорядочим $\varsigma$-стороны в порядке вращения в положительном направлении их нормалей, начав с нормали к прямой $R_sR_1$. Учитывая все вышесказанное, получаем, что вначале будут идти $\varsigma$-стороны многоугольника $\Phi_1$, а затем $\varsigma$-стороны многоугольника $\Phi_0$, взятые в их естественном порядке.

Если пересечение $\Phi_0 \cap \Phi_1$ не пусто, то оно является многоугольником. Очевидно, что граница этого многоугольника составлена из частей $\varsigma$-сторон многоугольников $\Phi_\nu$ ($\nu = 0, 1$). Из только что установленного свойства нормалей $\varsigma$-сторон многоугольников $\Phi_\nu$ ($\nu = 0, 1$) получаем, что граница многоугольника $\Phi_0 \cap \Phi_1$ составлена из двух ломаных: одна из них есть часть границы многоугольника $\Phi_0$, а другая — часть границы многоугольника $\Phi_1$. Возможны следующие случаи:

1. $\Phi_0 \cap \Phi_1$ — точка;

2. $\Phi_0 \cap \Phi_1$ — отрезок;

3. $\Phi_0 \cap \Phi_1$ — невырожденный многоугольник.

Понятно, что в любом из этих трех случаев $\Phi_0 \cap \Phi_1$ содержит одну из вершин $\Phi_0$ или $\Phi_1$. Лемма 1.29 доказана. ∎

Вернемся теперь к доказательству теоремы 1.28, а именно, к рассмотрению случая $\theta(f) = 2$. Пусть $\Phi = \operatorname{Conv} E_k^2$, $R_1, \ldots, R_4$ — вершины многоугольника $\Phi$, взятые в порядке положительного обхода таким образом, что $f(R_i) = 0$ $(i = 1, \ldots, s')$, $f(R_j) = 1$ $(j = s' + 1, \ldots, 4)$, $1 \le s' \le 3$, $T_\nu = M_\nu(f) \backslash \{R_1, \ldots, R_4\}$ $(\nu = 0, 1)$. Воспользовавшись леммой 1.29, получаем, что либо $M_0(f) \cap M_1(f) = \varnothing$, а, следовательно, по утверждению 1.5 $f \in \mathfrak{T}(E_k^2)$, либо $M_0(f) \cap M_1(f) \cap \mathbb{Z}^2 \ne \varnothing$, т. е. по утверждению 1.4 $f \notin \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$.

Рассмотрим теперь случай $\theta(f) = 4$. Возможны 2 подслучая:

1. $f(0,0) = f(k-1, k-1) = 0$, $f(0, k-1) = f(k-1, 0) = 1$;

2. $f(0,0) = f(k-1, k-1) = 1$, $f(0, k-1) = f(k-1, 0) = 0$.

Покажем, что, первый подслучай невозможен. Доказательство невозможности второго проводится аналогично.

Если $k$ нечетно, то, очевидно,

$$\left(\frac{k-1}{2}, \frac{k-1}{2}\right) = \frac{1}{2}(0,0) + \frac{1}{2}(k-1, k-1) = \frac{1}{2}(k-1, 0) + \frac{1}{2}(0, k-1)$$

и, следовательно, по утверждению 1.4 $f \notin \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$. Для рассмотрения случая четного $k \ge 4$ введем следующие обозначения: $R_0 = (0,0)$; $R_1 = (k-1, 0)$; $R_2 = (k-1, k-1)$; $R_3 = (0, k-1)$; $R_4 = (k-2, 0)$; $R_5 = (1, 0)$; $R_6 = (1, k-1)$; $R_7 = (k-1, k-2)$; $R_8 = (k-1, 1)$; $R_9 = \left(\frac{k}{2}, \frac{k}{2}\right)$; $R_{10} = (k-2, k-1)$; $R_{11} = (0, k-2)$; $R_{12} = (0, 1)$; $R_{13} = \left(\frac{k-2}{2}, \frac{k}{2}\right)$.

Вначале заметим, что $R_i \in E_k^2$ $(i = 0, 1, \ldots, 13)$. Все импликации в следующих двух абзацах вытекают из утверждения 1.4.

Пусть $f(R_4) = 0$. Так как $R_5 \in [R_0, R_4]$, то $f(R_5) = 0$. Отрезки $[R_5, R_6]$, $[R_1, R_3]$ и отрезки $[R_5, R_7]$, $[R_1, R_3]$ пересекаются в целых точках, следовательно, $f(R_6) = f(R_7) = 1$. Так как $R_8 \in [R_1, R_7]$, то $f(R_8) = 1$. Поскольку $\{R_9\} = [R_0, R_2] \cap [R_6, R_8]$ и $f(R_0) = f(R_2) = 0$, $f(R_6) = f(R_8) = 1$, то $f \notin \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$.

Пусть $f(R_4) = 1$. Так как отрезки $[R_4, R_{10}]$, $[R_0, R_2]$ и отрезки $[R_4, R_{11}]$, $[R_0, R_2]$ пересекаются в целых точках, то $f(R_{10}) = f(R_{11}) = 0$. Так как $R_{12} \in [R_0, R_{11}]$, то $f(R_{12}) = 0$. Поскольку $\{R_{13}\} = [R_{12}, R_{10}] \cap [R_1, R_3]$ и $f(R_{12}) = f(R_{10}) = 0$, $f(R_1) = f(R_3) = 1$, то $f \notin \mathfrak{F}_0(E_k^2) \cap \mathfrak{F}_1(E_k^2)$. Теорема 1.28 полностью доказана. ∎

В заключение раздела построим функцию

$$f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M) \setminus \mathfrak{T}(M),$$

где $M = E_{k_1} \times E_{k_2} \times \cdots \times E_{k_n}$, $k_j \geq 2$ $(j = 1, \ldots, n)$, НОД$(k_1 - 1, k_2 - 1, \ldots, k_n - 1) = 1$.

**Пример 1.30.** Пусть $M_0(f)$ состоит из двух точек:

$$x^{(1)} = (0, 0, \ldots, 0), \qquad x^{(2)} = (k_1 - 1, k_2 - 1, \ldots, k_n - 1).$$

Так как отрезок $[x^{(1)}, x^{(2)}]$ не содержит других точек из $M$, то

$$P_0(f) \cap P_1(f) \cap \mathbb{Z}^n = \varnothing$$

и, следовательно, из утверждения 1.4 $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. С другой стороны, очевидно, что $P_0(f) \cap P_1(f) \neq \varnothing$, поэтому $f \notin \mathfrak{T}(M)$.

## 1.6. Построение двойственного описания полиэдра

Данный раздел посвящен задаче построения вершин и экстремальных лучей полиэдра $P$, заданного системой линейных неравенств. Эта

задача возникает как вспомогательная при построении алгоритмов расшифровки пороговых и близких к ним функций, но также возникает в большом числе других приложений и представляет несомненный самостоятельный интерес. Предлагается новая модификация хорошо известного «метода двойного описания». Теоретические оценки сложности и результаты вычислительного эксперимента подтверждают превосходство по трудоемкости нового алгоритма по сравнению с классическим.

### 1.6.1. Введение

Пусть $\mathfrak{F}$ — произвольное подполе поля $\mathbb{R}$, т. е. $\mathbb{Q} \subseteq \mathfrak{F} \subseteq \mathbb{R}$. Хорошо известно [81, 88], что каждый полиэдр в $\mathfrak{F}^n$ можно представить любым из следующих двух способов:

1) как множество решений некоторой системы линейных неравенств;

2) как сумму (по-Минковскому) конической оболочки некоторой системы векторов $u_1, u_2, \ldots, u_s$ и выпуклой оболочки некоторой системы точек $v_1, v_2, \ldots, v_k$ в $\mathfrak{F}^n$.

Если полиэдр телесен, то неприводимая система линейных неравенств для этого полиэдра определяется единственным образом с точностью до умножения каждого неравенства на положительные константы, при этом каждому неравенству соответствует фасета (грань максимальной размерности). Далее, если полиэдр не содержит ненулевых аффинных подпространств, то неприводимые порождающие системы векторов $u_1, u_2, \ldots, u_s$ и точек $v_1, v_2, \ldots, v_k$ определяются единственным образом с точностью до умножения векторов $u_1, u_2, \ldots, u_s$ на положительные скаляры. При этом $v_1, v_2, \ldots, v_k$ суть вершины полиэдра, а $u_1, u_2, \ldots, u_s$ — его экстремальные рецессивные лучи. Задача построения неприводимого представления (2) по представлению (1) называется, допуская неко-

торую вольность речи, *задачей нахождения вершинного описания*. Обратная задача — *задачей нахождения фасетного описания* или *задачей построения выпуклой оболочки*. Согласно классической теореме Вейля, любая из этих двух задач не более чем за линейное время сводится к обратной (двойственной).

Аналогично, каждый полиэдральный конус в $\mathfrak{F}^n$ можно представить любым из следующих двух способов:

1) как множество решений некоторой однородной системы линейных неравенств;

2) как множество всех неотрицательных комбинаций некоторой системы векторов в $\mathfrak{F}^n$.

Неприводимая система векторов, множество неотрицательных комбинаций которой есть заданный конус, называется *остовом*. Если конус острый (т. е. не содержит ненулевых подпространств), то остов конуса определяется единственным образом с точностью до умножения векторов на положительные скаляры и образует множество экстремальных лучей конуса.

Существует стандартный способ свести задачу построения вершинного/фасетного описания для полиэдров к соответствующей задаче для полиэдральных конусов. Например, для нахождения вершинного описания полиэдра $P(A, a_0) = \{x \in \mathfrak{F}^n : Ax \geq a_0\}$ достаточно решить аналогичную задачу для конуса $\{(x_0, x) \in \mathfrak{F}^{n+1} : Ax - a_0 x_0 \geq 0,\ x_0 \geq 0\}$ и затем положить $x_0 = 1$.

Указанные задачи возникают во многих приложениях: компьютерной графике, физической симуляции, обработке изображений, картографии, вычислительной биологии, теоретической физике и многих других. К построению фасетного описания (выпуклой оболочки) могут быть све-

дены задачи построения триангуляции Делоне и диаграммы Вороного [68].

В настоящее время не известно, существуют ли алгоритмы, решающие поставленные задачи, время работы которых было бы ограничено полиномом от суммарной длины входа и выхода. Более того, ни один из известных алгоритмов таковым не является [118]. С другой стороны, данные задачи возникают во многих приложениях и необходимы быстрые практические алгоритмы их решения.

В работе рассматривается классический «метод двойного описания» [153] (другие распространенные названия — алгоритм Моцкина–Бургера [88] или алгоритм Фурье–Моцкина [106, 108]), решающий поставленные задачи. Разными авторами предлагались различные улучшения этого метода; см., например, [9, 88–90, 108, 110, 123, 129, 130, 146].

Метод двойного описания относится к классу «инкрементных» и основная его идея заключается в следующем. Пусть рассматривается задача построения вершинного описания полиэдра $P(A, a_0) = \{x : \ Ax \leq a_0\}$. Вначале задача решается для некоторой подсистемы системы $Ax \leq a_0$ (например, для одного неравенства или подсистемы ранга $n$). Далее в эту подсистему добавляются одно за одним все неравенства исходной системы, при этом вершинное описание каждый раз пересчитывается. Название метода «двойного описания» объясняется следующим образом. На каждой итерации поддерживаются *два* описания текущего полиэдра: вершинное и фасетное — и вся другая необходимая информация вычисляется по ним, в частности, вычисляется множество всех ребер текущего полиэдра. Пусть на текущей итерации добавляется неравенство $ax \leq \beta$. Множество вершин нового полиэдра состоит из вершин текущего полиэдра, координаты которых удовлетворяют этому неравенству, а также точек пересечения его ребер с гиперплоскостью $ax = \beta$.

В отличие от других инкрементных алгоритмов, метод двойного описания не пересчитывает полную решетку граней текущего полиэдра, как, например, метод «под–над» [68] или метод Шевченко–Чиркова [110], а также не использует триангуляций, как, например, [91, 108, 126] и др. Заметим, что размер полной решетки граней и размер триангуляции может суперполиномиально зависеть от суммарного размера входа и выхода [118], поэтому метод двойного описания часто опережает по скорости работы другие алгоритмы, в частности, на крайне вырожденных задачах. (Задача нахождения вершинного описания *вырождена*, если существует вершина, инцидентная более, чем $n$ фасетам.)

Одним из «узких мест» метода является вызываемая на каждой итерации процедура нахождения множества ребер текущего полиэдра. Для этого обычно для каждой пары его вершин проверяется какое-либо необходимое и достаточное условие их смежности. Хорошо известны два из них: «алгебраический» и «комбинаторный» тесты. Как правило, на практике комбинаторный тест работает значительно быстрее алгебраического. Мы предлагаем новую ускоренную модификацию комбинаторного теста, названную нами «графовой». Другое улучшение связано с уменьшением количества рассматриваемых пар вершин при проверке их на смежность. В [130] замечено, что не все ребра текущего полиэдра приводят на поздних итерациях к порождению новых вершин и показано, как на этой основе можно существенно снизить объем используемой памяти и время работы. Мы развиваем эту идею и применяем ее для модификации метода двойного описания с динамическим порядком добавления неравенств. Теоретические результаты и вычислительный эксперимент показывают значительное превосходство в быстродействии предлагаемых модификаций по сравнению с исходным алгоритмом и другими модификациями, например, [130].

Для определенности будем рассматривать задачу построения остова полиэдрального (многогранного) конуса, заданного однородной системой линейных неравенств $Ax \geq 0$. Ограничимся случаем острого конуса. Задача для произвольного конуса легко сводится к данной путем перехода из исходного пространства $\mathbb{F}^n$ в ортогональное дополнение к подпространству $\{x \in \mathbb{F}^n : \ Ax = 0\}$.

Необходимые определения и обозначения мы вводим в разделе 1.6.2. Схема метода двойного описания представлена в разделе 1.6.3. В разделе 1.6.4 мы рассматриваем ряд известных способов добавления неравенств исходной системы. Разделы 1.6.5 и 1.6.6 посвящены двум важным процедурам в методе двойного описания. В разделе 1.6.5 рассматриваются известные способы проверки смежности экстремальных лучей полиэдрального (многогранного) конуса и предлагается новая, «графовая», модификация этого теста. В разделе 1.6.6 описаны некоторые способы уменьшения количества генерируемых пар смежных экстремальных лучей и предлагаются новые методы для решения этой задачи. В разделе 1.6.7 мы кратко описываем программу SKELETON, в которой реализованы предлагаемые модификации, и приводим результаты вычислительных экспериментов.

### 1.6.2. Определения и предварительные сведения

Изложение в данном разделе следует в основном монографиям [17, 81, 88, 167]. *Полиэдральным* (*многогранным*) *конусом* в пространстве $\mathbb{F}^n$ (далее просто *конусом*) называется множество

$$C = \{x \in \mathbb{F}^n : \ Ax \geq 0\},$$

где $A \in \mathbb{F}^{m \times n}$ — матрица размера $m \times n$ с элементами из $\mathbb{F}$. Говорят, что система линейных неравенств $Ax \geq 0$ *определяет* конус $C$. Конус

называется *острым*, если он не содержит ненулевых подпространств. Хорошо известно, что для того, чтобы конус $C$ был острым, необходимо и достаточно, чтобы $\operatorname{rank} A = n$, где $\operatorname{rank} A$ обозначает ранг матрицы $A$. Любой полиэдральный конус $C$ может быть задан в виде конической оболочки некоторой конечной системы векторов $u_1, u_2, \ldots, u_s$ пространства $\mathfrak{F}^n$, т. е.

$$C = \{x = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_s u_s : \ \alpha_i \geq 0 \ (i = 1, 2, \ldots, s)\}.$$

Говорят, что система векторов $u_1, u_2, \ldots, u_s$ *порождает* конус $C$.

Ненулевой вектор $u \in C$ назовем *лучом* конуса $C$. Два луча $u$ и $v$ будем называть равными и записывать $u \simeq v$, если для некоторого $\alpha \geq 0$ верно $u = \alpha v$. Луч $u \in C$ называется *экстремальным*, если из условий $u = \alpha v + \beta w$, $\alpha \geq 0$, $\beta \geq 0$, $v, w \subseteq C$ следует $u \simeq v \simeq w$. Множество экстремальных лучей острого конуса является его минимальной порождающей системой и называется *остовом* конуса. Пусть $P$ — выпуклое подмножество в $\mathfrak{F}^n$ и для некоторых $a \in \mathfrak{F}^n$, $\alpha \in \mathfrak{F}$ верно, что $P \subseteq \{x : \ ax \leq \alpha\}$, тогда $P \cap \{x : \ ax = \alpha\}$ называется *гранью* множества $P$. Два экстремальных луча $u$ и $v$ острого конуса $C$ называются *смежными*, если минимальная грань, содержащая оба луча, не содержит никаких других экстремальных лучей конуса. Остов конуса $C$ будем обозначать через $U(C)$, а множество всех пар $\{u, v\}$ смежных экстремальных лучей — через $E(C)$.

Если $A \in \mathfrak{F}^{m \times n}$, $i \in \{1, 2, \ldots, m\}$, $K \subseteq \{1, 2, \ldots, m\}$, то через $a_i$ обозначена $i$-я строка матрицы $A$, а через $A_K$ — подматрица матрицы $A$, составленная из строк $a_i$, где $i \in K$. В выражениях вида $ax$, где $a \in \mathfrak{F}^n$, $x \in \mathfrak{F}^n$, вектор $a$ следует интерпретировать как вектор-строку, а $x$ — как вектор-столбец.

### 1.6.3. Метод двойного описания

Основная идея метода двойного описания [153] заключается в следующем. На вход поступает матрица $A \in \mathfrak{F}^{m\times n}$, $\operatorname{rank} A = n$. На предварительном этапе находим подсистему $Bx \geq 0$ системы $Ax \geq 0$ из $n$ неравенств ранга $n$. Легко видеть, что остов конуса, заданного этой подсистемой, образуют столбцы матрицы $B^{-1}$. Далее к подсистеме $Bx \geq 0$ по очереди добавляем неравенства исходной системы, каждый раз пересчитывая остов. Правила пересчета дает следующая теорема.

**Теорема 1.31.** [153] *Пусть* $A \in \mathfrak{F}^{m\times n}$, $\operatorname{rank} A = n$, $a \in \mathfrak{F}^n$. *Если* $U$ — *остов конуса* $K = \{x \in \mathfrak{F}^n : \ Ax \geq 0\}$,

$$U_0 = \{u \in U : au = 0\}, \quad U_+ = \{u \in U : au > 0\}, \quad U_- = \{u \in U : au < 0\},$$

*тогда остов конуса*

$$K' = \{x \in \mathfrak{F}^n \ Ax \geq 0, \ ax \geq 0\}$$

*есть объединение* $U_+ \cup U_0 \cup U_\pm$, *где*

$$U_\pm = \{w = (au)v - (av)u : \ u \in U_+, \ v \in U_-, \ (u, v) \in E(K)\}.$$

Приведем общую схему метода двойного описания [153]. На вход алгоритма DDM подается матрица $A \in \mathfrak{F}^{m\times n}$, $\operatorname{rank} A = n$. На выходе получаем остов $U$ конуса $\{x : \ Ax \geq 0\}$.

Алгоритм DDM

Шаг 0. Найти $I \subseteq \{1, 2, \ldots, m\}$, такое, что $|I| = n$, $\det A_I \neq 0$. Построить остов $U$ конуса $\{x : \ A_I x \geq 0\}$.

Шаг 1. Пока $I \neq \{1, 2, \ldots, m\}$, выполнять шаги 1.1–1.4.

Шаг 1.1. Выбрать $i \in \{1, 2, \ldots, m\} \setminus I$.

Шаг 1.2. Положить $U_+ = \{u \in U : \ a_i u > 0\}$, $U_- = \{u \in U : \ a_i u < 0\}$, $U_0 = \{u \in U : \ a_i u = 0\}$, $U_\pm = \varnothing$.

Шаг 1.3. Для каждой пары векторов $(u, v)$, где $u \in U_+$, $v \in U_-$, если $u$ и $v$ смежны в конусе $\{x : \ A_I x \geq 0\}$, то поместить вектор $w = (a_i u)v - (a_i v)u$ в множество $U_\pm$.

Шаг 1.4. Положить $U = U_+ \cup U_0 \cup U_\pm$ и поместить $i$ в $I$.

Одна из основных черт метода двойного описания заключается в том, что на каждой итерации алгоритм имеет *два* полных описания текущего конуса: определяющую его систему неравенств $A_I x \geq 0$ и его остов $U$ — отсюда название метода.

Модификации метода двойного описания отличаются друг от друга, в частности, по следующим параметрам:

1) порядком рассмотрения неравенств исходной системы на шаге 1.1;

2) способом определения смежности векторов остова на шаге 1.3;

3) временем, когда определяется смежность векторов.

Многочисленные эксперименты, например, [9, 118, 130], показывают, что общее время работы алгоритма существенным образом зависит от порядка, в котором рассматриваются неравенства. С другой стороны, на каждой итерации большое время занимает процедура построения множества $E$ пар смежных экстремальных лучей.

Способы проверки смежности векторов остова на шаге 1.3 описаны в разделе 1.6.5.

Разными авторами, например, [9, 130], предлагались модификации алгоритма, в которых множество $E$ пар смежных экстремальных лучей перестраивается сразу, как только обновляется список экстремальных векторов. Приведем описание одной из таких модификаций.

Алгоритм DDM.M1

Шаг 0. Найти $I \subseteq \{1, 2, \ldots, m\}$, такое, что $|I| = n$, $\det A_I \neq 0$.
Построить остов $U$ конуса $\{x : \ A_I x \geq 0\}$.
Положить $E = \{\{u, v\} : \ u, v \in U, \ u \neq v\}$.

Шаг 1. Пока $I \neq \{1, 2, \ldots, m\}$ выполнять шаги 1.1–1.7.

Шаг 1.1. Выбрать $i \in \{1, 2, \ldots, m\} \setminus I$.

Шаг 1.2. Положить $U_+ = \{u \in U : \ a_i u > 0\}$, $U_- = \{u \in U : \ a_i u < 0\}$, $U_0 = \{u \in U : \ a_i u = 0\}$, $U_\pm = \varnothing$.

Шаг 1.3. Положить $E_+ = \{\{u, v\} \in E : \ u, v \in U_+ \cup U_0\}$, $E' = \varnothing$.

Шаг 1.4. Для каждой пары $\{u, v\} \in E$, где $u \in U_+$ и $v \in U_-$, положить $w = (a_i u)v - (a_i v)u$, поместить $w$ в $U_\pm$, поместить $\{u, w\}$ в $E'$.

Шаг 1.5. Положить $U = U_+ \cup U_0 \cup U_\pm$.

Шаг 1.6. Построить множество $E''$ пар лучей из $U_0$, смежных в конусе $\{x \in \mathfrak{F}^n : \ A_I x \geq 0, \ A_i x \geq 0\}$.

Шаг 1.7. Положить $E = E_+ \cup E' \cup E''$ и поместить $i$ в $I$.

### 1.6.4. Порядок добавления неравенств

В ряде работ, например, [9, 130], предлагалось несколько способов добавления неравенств исходной системы в методе двойного описания. Каждый из них детерминирует правило выбора номера $i$ на шаге 1.1 алгоритмов DDM и DDM.M1.

В методах minindex, lexmin, mincutoff, minpairs в качестве $i$ выбираем соответственно

$$i_{\text{minindex}} = \min I, \qquad i_{\text{lexmin}} = \arg\operatorname{lexmin} \{a_i : \ i \in I\},$$

$$i_{\text{mincutoff}} = \arg\min\{|U_-| : \ i \in I\}, \quad i_{\text{minpairs}} = \arg\min\{|U_-| \cdot |U_+| : \ i \in I\}.$$

Методы maxindex, lexmax, maxcutoff, maxpairs отличаются от рассмотренных тем, что в этих в формулах нужно заменить везде min и lexmin на max и lexmax соответственно. В методе random индекс $I$ выбирается из множества $I$ случайно равновероятно. Таким образом, метод mincutoff (соответственно, maxcutoff) на каждой итерации алгоритма минимизируют (соответственно, максимизирует) количество отсекаемых экстремальных лучей. Метод minpairs (соответственно, maxpairs) минимизируют (соответственно, максимизирует) количество рассматриваемых потенциально смежных пар.

Способы добавления неравенств можно условно разбить на две группы:

1) методы с фиксированным порядком неравенств;

2) методы с динамически определяемым порядком неравенств.

При первом способе порядок выбора неравенств может быть определен заранее до начала выполнения итераций. К таким методам относятся minindex, maxindex, lexmin, lexmax, random. В этом случае неравенства исходной системы $Ax \geq 0$ можно отсортировать заранее и на шаге 1.1 считать, что $i = \min I$.

Во втором случае номер $i$ не может быть известен заранее. К методам с динамическим порядком относятся mincutoff, maxcutoff, minpairs, maxpairs.

В разделе 1.6.7 приведены некоторые результаты по экспериментальному сравнению рассмотренных методов добавления неравенств.

### 1.6.5. Методы проверки смежности экстремальных лучей

Здесь мы рассматриваем некоторые известные способы проверки на смежность экстремальных лучей конуса и предлагаем один новый метод. Необходимые и достаточные условия смежности лучей, приведенные далее, можно использовать как в исходном алгоритме DDM, так и в его модификации DDM.M1. Заметим, что на шаге 1.6 алгоритма DDM.M1 множество экстремальных лучей конуса $\{x \in \mathbb{F}^n : A_I x \geq 0,\ a_i x \geq 0\}$, принадлежащих $U_0$, совпадает со множеством всех экстремальных лучей конуса $\{x \in \mathbb{F}^n : A_I x \geq 0,\ a_i x = 0\}$. Это обстоятельство имеет смысл учитывать при проверке описанных ниже тестов на смежность.

Пусть, как обычно, $C = \{x : Ax \geq 0\}$, $A \in \mathbb{F}^{m \times n}$, $\operatorname{rank} A = n$ и $u \in \mathbb{F}^n$. Обозначим $Z(u) = \{i : A_i u = 0\}$. Таким образом, $Z(u)$ есть множество номеров ограничений системы $Ax \geq 0$, активных для вектора $u$.

Хорошо известны два необходимых и достаточных условия для смежности экстремальных лучей конуса: «комбинаторный» и «алгебраический».

**Утверждение 1.32** (Алгебраический тест)**.** *Пусть* $u, v \in U(C)$. *Для того, чтобы* $\{u, v\} \in E(C)$ *необходимо и достаточно, чтобы* $\operatorname{rank} A_{Z(u) \cap Z(v)} = n - 2$.

**Утверждение 1.33** (Комбинаторный тест)**.** *Пусть* $u, v \in U(C)$. *Для того, чтобы* $\{u, v\} \in E(C)$ *необходимо и достаточно, чтобы* $Z(u) \cap Z(v) \subset Z(w)$ *ни для какого* $w \in U(C) \setminus \{u, v\}$.

Алгебраический тест является следствием теоремы Минковского (см., например, [88]). Комбинаторный тест впервые предложен в работе [153], его доказательство приведено в [123].

Ранг в алгебраическом тесте можно вычислить с помощью общеизвестных алгоритмов линейной алгебры, что требует не более $O(mn^2)$

арифметических операций. Таким образом, трудоемкость процедуры построения всех пар смежных лучей с помощью алгебраического теста составляет $O(mn^2s^2)$, где $s = |U(C)|$.

Из утверждения 1.32 получаем следующее простое необходимое условие смежности лучей.

**Утверждение 1.34.** *Если* $\{u, v\} \in E(C)$*, тогда* $Z(u) \cap Z(v) \geq n - 2$.

Сформулированное необходимое условие рассматривалось многими авторами, например, [9, 89, 123, 130, 146]. Многочисленные эксперименты показывают, что его разумно проверять всякий раз перед выполнением любого теста на смежность лучей.

Рассмотрим более подробно комбинаторный тест. Словестная его формулировка выглядит так: для того, чтобы экстремальные лучи $u$ и $v$ конуса $C$ были смежны, необходимо и достаточно, чтобы неравенства, являющиеся активными для обоих лучей, не являлись одновременно активными ни для какого другого экстремального луча, иными словами, чтобы минимальная грань, содержащая оба вектора $u$ и $v$, не содержала других экстремальных лучей. Последняя формулировка делает очевидным обоснование комбинаторного теста.

Выполнять комбинаторный тест удобно, имея в распоряжении матрицу $T = (t_{ij}) \in \{0, 1\}^{s \times m}$, в которой $t_{ij} = 1$ тогда и только тогда, когда $a_j u_i > 0$, где $U = \{u_1, u_2, \ldots, u_s\}$. Для того, чтобы лучи $u_i$ и $u_{i'}$ были смежны, необходимо и достаточно, чтобы для любого $k \in \{1, 2, \ldots, s\} \setminus \{i, i'\}$ нашлось $\ell$, такое, что

$$t_{i\ell} = t_{i'\ell} = 0, \qquad t_{k\ell} = 1.$$

Трудоемкость проверки смежности двух лучей $u$ и $v$ составляет $O(ms)$ операций. Таким образом, трудоемкость процедуры построения всех пар смежных лучей с помощью комбинаторного теста есть $O(ms^3)$.

Мы предлагаем новую, «графовую», модификацию комбинаторного теста, которая позволяет существенно ускорить процедуру проверки смежности экстремальных лучей. Рассмотрим простой (неориентированный, без петель и кратных ребер) граф $G$, который построим по конусу $C$ следующим образом. Множество вершин графа $G$ есть множество $U$ экстремальных лучей конуса $C$, а $\{u, v\}$ образует ребро в $G$ тогда и только тогда, когда $|Z(u) \cap Z(v)| \geq n - 2$. Множество всех ребер графа $G$ обозначим $E(G)$.

**Утверждение 1.35** («Графовый» тест)**.** *Пусть* $u, v \in U(C)$. *Для того, чтобы* $\{u, v\} \in E(C)$ *необходимо и достаточно, чтобы в* $U(C)$ *не существовало луча* $w$, *отличного от* $u$ *и* $v$, *такого, что* $\{u, w\} \in E(G)$, $\{v, w\} \in E(G)$ *и* $Z(u) \cap Z(v) \subseteq Z(w)$.

*Доказательство.* Пусть $u, v \in U(C)$. Согласно утверждению 1.33, для того, чтобы $\{u, v\} \in E(C)$ необходимо и достаточно, чтобы $Z(u) \cap Z(v) \subseteq Z(w)$ ни для какого $w \in U(C)$. Однако согласно утверждению 1.34, это условие не выполнено ни для какого $w \in U(C)$, не смежного в графе $G$ одновременно $u$ и $v$, поэтому данное условие достаточно проверить только для лучей $w$, таких, что $\{u, w\} \in E(G)$, $\{v, w\} \in E(G)$. ∎

Заметим, что для использования доказанного утверждения в алгоритме проверки смежности экстремальных лучей нет необходимости в явном построении графа $G$. Вместо этого на каждой итерации мы можем строить только окрестность $D$ очередной вершины $u$ этого графа.

Мы приходим к алгоритму Graph.Adj («графовая» модификация комбинаторного теста) нахождения всех пар смежных экстремальных лучей. На вход алгоритма поступает остов $U = U(C)$ конуса $C$. Предполагается, что для каждого экстремального луча $u$ известно множество

$Z(u)$. На выходе получаем множество $E$ всех пар смежных экстремальных лучей.

Алгоритм Graph.Adj

Шаг 0. Положить $E = \varnothing$, $S = \varnothing$.

Шаг 1. Для каждого $u \in U$ выполнить шаги 1.1–1.3

Шаг 1.1. Положить $D = \varnothing$, $S = S \cup \{u\}$.

Шаг 1.2. Для каждого $v \in U \setminus \{u\}$: если $|Z(u) \cap Z(v)| \geq n - 2$, то поместить $v$ в $D$.

Шаг 1.3. Для каждого $v \in D \setminus S$: если $|Z(u) \cap Z(v)| \geq n - 2$ и не существует $w \in D \setminus \{v\}$, такого, что $Z(u) \cap Z(v) \subseteq Z(w)$, то поместить $\{u, v\}$ в $E$

В алгоритм Graph.Adj мы поместили также проверку необходимого условия из утверждения 1.34.

Обозначим $\delta$ максимум из степеней вершин в графе $G$. Трудоемкость построения окрестности $D$ (шаг 1.2) есть $O(ms^2)$, трудоемкость обхода этой окрестности (шаг 1.3) есть $O(ms\delta)$, откуда трудоемкость всего алгоритма Graph.Adj есть $O(ms^2 + ms\delta)$. Так как $\delta < n$, то эта трудоемкость всегда асимптотически не превосходит верхней оценки $O(ms^3)$ трудоемкости решения данной задачи с помощью комбинаторного теста. Во многих задачах $\delta \ll n$ и преимущество алгоритма Graph.Adj оказывается намного более существенным. Результаты вычислительного эксперимента, приведенные в разделе 1.6.7, подтверждают это превосходство.

### 1.6.6. Уменьшение количества рассматриваемых пар смежных лучей

Алгоритм DDM при добавлении нового неравенства рассматривает все пары экстремальных лучей $u$ и $v$, таких, что $A_i u \cdot A_i v < 0$, а затем проверяет их на смежность. В отличие от него алгоритм DDM.M1 не перебирает все такие пары, а на каждой итерации обновляет список $E$ только смежных пар экстремальных лучей. Заметим, что для хранения $E$ требуется память, объем которой может квадратично зависеть от количества сгенерированных лучей. На практике это может приводить к нехватке машинной памяти. С другой стороны, далеко не каждая пара $\{u, v\} \in E$ приводит к появлению нового луча. Выявление на ранних этапах пар лучей в остове конуса, которые не могут в дальнейшем привести к появлению нового луча, уменьшает объем требуемой памяти, так как такие пары не будут попадать в множество $E$. Это также должно уменьшить время выполнения шага 1.3 и количество итераций в цикле 1.4 алгоритма DDM.M1. Более того, выявление такой пары до проверки ее на смежность может сэкономить время на выполнение этой проверки.

Сначала рассмотрим метод DDM.M1 с фиксированным порядком неравенств. Предположим, что неравенства уже отсортированы в нужном порядке, поэтому на шаге 1.1 алгоритма DDM.M1 можно считать $i = \min I$. В работе [130] для алгоритма DDM.M1 предложен следующий способ уменьшения количества рассматриваемых пар смежных лучей. Назовем данный метод PlusPlus.

Пусть $u, v \in E$, $a_i u = a_i v = 0$. Вычислим $a_k u$, $a_k v$ $(k = 1, 2, \ldots, m)$. Заметим, что $a_k u \geq 0$, $a_k v \geq 0$ $(k = 1, 2, \ldots, i-1)$. Пусть для некоторого $i' > i$

$$a_k u \geq 0, \quad a_k v \geq 0 \quad (k = i+1, 2, \ldots, i'-1), \quad a_{i'} u < 0, \quad a_{i'} v < 0.$$

Легко видеть, что в этом случае на последующих итерациях пара $\{u, v\}$ не приведет к появлению ни одного нового экстремального луча, поэтому эту пару можно исключить из рассмотрения, т. е. не включать в множество $E$.

Мы предлагаем следующую модификацию метода PlusPlus для алгоритма DDM.M1 с динамическим порядком неравенств. Пусть $u, v \in E$, $a_i u = a_i v = 0$. Вычислим $a_k u$, $a_k v$ ($k = 1, 2, \ldots, m$). Заметим, что $a_k u \geq 0$, $a_k v \geq 0$ ($k = 1, 2, \ldots, i-1$). Пусть

$$a_k u \cdot a_k v \geq 0 \quad (k = i+1, 2, \ldots, m).$$

Легко видеть, что в этом случае ни на одной из последующих итераций пара $\{u, v\}$ не приведет к появлению ни одного нового экстремального луча, поэтому эту пару можно исключить из рассмотрения, т. е. не включать в множество $E$.

В разделе 1.6.7 приведены результаты вычислительных экспериментов, показывающих преимущество описанных модификаций.

### 1.6.7. Вычислительный эксперимент

В программе SKELETON[1], написанной автором, реализованы все предлгаемые модификации метода двойного описания. Программа поддерживает целочисленную арифметику ограниченной точности (данные представлены как целые числа длиной 4 байта), целочисленную арифметику неограниченной точности (используются целые числа неограниченного размера) и вещественную арифметику с плавающей запятой двойной точности. С. В. Лобанов разработал он-лайн доступ[2] к программе.

Эксперименты проводились на вычислительной системе Intel Core 2 CPU 6300 1.86 GHz, 2 Gb RAM, Microsoft Windows XP Professional,

[1] Программа доступна в Интернет по адресу `http://www.uic.unn.ru/~zny/skeleton`.

[2] Сервис доступен в сети Интернет по адресу `http://www.arageli.org/skeletondemo`.

Version 2002, SP2. Использовался компилятор C++ MS Visual Studio 2005 с включенной опцией `/o2`.

В таблицах 1.1, 1.2 приведены результаты вычислительного эксперимента, в котором на вход программы подавались остов (63 вектора в $\mathbb{Q}^{21}$) полного разрезного конуса $ccc_7$ и вершины (64 точки в $\mathbb{Q}^{21}$) полного разрезного полиэдра (многогранника) $ccp_7$; см. [16]. Программа вычисляла их фасетное описание (38780 и 116764 неравенства соответственно). Использовалась целочисленная арифметика ограниченной точности. В первом столбце указан используемый порядок рассмотрения неравенств системы. Во втором и третьем столбцах обозначено, использовались или нет модификации PlusPlus и Graph.Adj. В четвертом столбце указано время (в секундах), в течение которого программа решила задачу. В двух последних столбцах обозначены соответственно суммарное (по всем итерациям алгоритма) число построенных экстремальных лучей и суммарное число сгенерированных пар смежных лучей.

Из таблицы видно, что использование модификаций Graph.Adj и PlusPlus, как правило, существенно увеличивает производительность программы.

В таблице 1.3 приведены результаты сравнения быстродействия программ SKELETON (с включенными опциями Graph.Adj и PlusPlus) и `cdd` К. Фукуды[3]. Программа `cdd` реализует алгоритм DDM.M1 с рядом модификаций из [130]. Эксперимент проводился на задачах, описанных в [130]. Использовалась вещественная арифметика с плавающей запятой двойной точности.

Параллельная версия алгоритма и реализующего его программа описана в [31]. Дальнейшее развитие описанных здесь идей см. в [5].

[3] Программа доступна в Интернет по адресу `http://www.ifor.math.ethz.ch/~fukuda/cdd_home/cdd.html`.

Таблица 1.1. Время работы программы SKELETON на задаче $ccc_7$

| *Порядок рассмотрения неравенств* | *Модиф.* PlusPlus | *Модиф.* Graph.Adj | *Время, с* | *Общее число построенных лучей* | *Общее число построенных пар смежных лучей* |
|---|---|---|---|---|---|
| (1) | (2) | (3) | (4) | (5) | (6) |
| lexmax | + | + | 257 | 337803 | 443041 |
| | + | – | 372 | | 14453733 |
| | – | + | 519 | | |
| | – | – | 1302 | | |
| maxindex | + | + | 3010 | 1087966 | 1313076 |
| | + | – | 6703 | | 41591800 |
| | – | + | 4582 | | |
| | – | – | 17169 | | |
| mincutoff | + | + | 3615 | 1207557 | 10442749 |
| | + | – | 10764 | | 44135376 |
| | – | + | 4586 | | |
| | – | – | 17761 | | |
| lexmin | + | + | 4285 | 1225951 | 1533651 |
| | + | – | 9458 | | 50631122 |
| | – | + | 7961 | | |
| | – | – | 23401 | | |
| maxcutoff | + | + | 7566 | 1789770 | 8459167 |
| | + | – | 26128 | | 59093531 |
| | – | + | 9400 | | |
| | – | – | 41580 | | |
| minindex | + | + | 8378 | 1691488 | 2125675 |
| | + | – | 19117 | | 73114625 |
| | – | + | 13480 | | |
| | – | – | 58506 | | |
| maxpairs | + | + | 14719 | 2547932 | 12445583 |
| | + | – | 54832 | | 76720581 |
| | – | + | 16911 | | |
| | – | – | 82620 | | |
| minpairs | + | + | 15468 | 2180085 | 12468623 |
| | + | – | 53931 | | 76176098 |
| | – | + | 19002 | | |
| | – | – | 94830 | | |

Таблица 1.2. Время работы программы SKELETON на задаче $ccp_7$

| *Порядок рассмотрения неравенств* | *Модиф.* PlusPlus | *Модиф.* Graph.Adj | *Время, с* | *Общее число построенных лучей* | *Общее число построенных пар смежных лучей* |
|---|---|---|---|---|---|
| (1) | (2) | (3) | (4) | (5) | (6) |
| lexmin | + | + | 5502 | 1186741 | 1434203 |
| | + | – | 11932 | | |
| | – | + | 9738 | | 52433304 |
| | – | – | 37635 | | |
| mincutoff | + | + | 9413 | 1921944 | 14673772 |
| | + | – | 26500 | | |
| | – | + | 12300 | | 73419448 |
| | – | – | 50989 | | |
| minindex | + | + | 9589 | 1815547 | 2264908 |
| | + | – | 21153 | | |
| | – | + | 16475 | | 80150892 |
| | – | – | 66086 | | |
| maxindex | + | + | 37293 | 3712906 | 4384170 |
| | + | – | 90336 | | |
| | – | + | 53458 | | 150592933 |
| | – | – | 259914 | | |
| lexmax | + | + | 42412 | 4072635 | 4774940 |
| | + | – | 105143 | | |
| | – | + | 58899 | | 158090265 |
| | – | – | 287400 | | |
| minpairs | + | + | 60920 | 4131333 | 20266953 |
| | + | – | 211875 | | |
| | – | + | 76248 | | 152416312 |
| | – | – | 397073 | | |
| maxcutoff | + | + | 67566 | 5501375 | 28885642 |
| | + | – | 259762 | | |
| | – | + | 78645 | | 180817307 |
| | – | – | 422795 | | |
| maxpairs | + | + | 78205 | 5935122 | 30214584 |
| | + | – | 302448 | | |
| | – | + | 95036 | | 196189215 |
| | – | – | 507222 | | |

Таблица 1.3. Сравнение производительностей программ SKELETON и `cdd`

| *Задача* | *Порядок рассмотрения неравенств* | *Вход* | | *Выход* | *Время работы, с* | |
|---|---|---|---|---|---|---|
| | | *m* | *n* | *s* | SKELETON | `cdd` |
| cube16 | lexmin | 17 | 32 | 65536 | 10 | 27 |
| cube18 | minindex | 19 | 36 | 262144 | 190 | 1103 |
| mit729-9 | lexmin | 8 | 729 | 4862 | 97 | 57 |
| ccc7 | lexmax | 63 | 21 | 38780 | 271 | 4232 |
| ccp7 | lexmin | 64 | 22 | 116765 | 5681 | 15981 |

# Глава 2

# Алгоритмы расшифровки пороговых и близких к ним функций

## 2.1. Постановка задачи

Обозначим

$$\mathfrak{M} = \bigcup_{\substack{l>n\geq 1\\ \gamma\geq 1}} \mathfrak{M}(n,l,\gamma), \qquad \mathfrak{F} = \bigcup_{M\in\mathfrak{M}} \mathfrak{F}(M).$$

Пусть $\mathfrak{M}'$ — некоторое (конечное или бесконечное) подмножество множества $\mathfrak{M}$, а $\mathfrak{F}'$ — некоторое подмножество множества $\mathfrak{F}$. Например, $\mathfrak{M}'$ — множество всех $E_k^n$ для всех $n \geq 1$, $k \geq 2$, а $\mathfrak{F}'$ — множество всех пороговых функций, заданных на $E_k^n$ для всех $n \geq 1$, $k \geq 2$. Обозначим $\mathfrak{F}'(M) = \mathfrak{F}' \cap \mathfrak{F}(M)$, где $M \in \mathfrak{M}'$.

Предположим, что с каждой функцией $f \in \mathfrak{F}'(M)$ связан *оракул*, позволяющий по произвольной точке $x \in M$ определить $f(x)$. Математическую формализацию понятий оракула и оракульного алгоритма см. в [15]. Под *расшифровкой* функции из известного класса $\mathfrak{F}' \subseteq \mathfrak{F}$ понимается задача, в которой по заданным $C \in \mathbb{Z}^{l\times n}$, $c_0 \in \mathbb{Z}^l$ и заданному оракулу функции $f \in \mathfrak{F}'(M)$, где $M = \{x \in \mathbb{Z}^n : Cx \leq c_0\}$, необходимо найти такие точки $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$ из $M$, значений в которых достаточно для однозначного определения $f$ в остальных точках из $M$.

Пусть $\mathscr{A}$ — алгоритм расшифровки функции в классе $\mathfrak{F}'$. Предположим, что при расшифровке функции $f \in \mathfrak{F}'$ алгоритм $\mathscr{A}$ обращается к оракулу в $\tau(\mathscr{A}, f)$ точках и выполняет $\rho(\mathscr{A}, f)$ операций. *Оракульной*

*сложностью* алгоритма $\mathscr{A}$ назовем величину

$$\tau_M(\mathscr{A}) = \max_{f \in \mathfrak{F}'(M)} \tau(\mathscr{A}, f).$$

*Вычислительной трудоемкостью* алгоритма $\mathscr{A}$ назовем число операций, выполненных алгоритмом в худшем случае:

$$\rho_M(\mathscr{A}) = \max_{f \in \mathfrak{F}'(M)} \rho(\mathscr{A}, f).$$

Пусть, как обычно, $M \in \mathfrak{M}(n, l, \gamma)$ задано в виде

$$M = \{x \in \mathbb{Z}^n : \ Cx \leq c_0\},$$

$$C \in \mathbb{Z}^{l \times n}, \quad c_0 \in \mathbb{Z}^l, \quad |c_{ij}| \leq \gamma \quad (i = 1, 2, \ldots, l, \ j = 0, 1, \ldots, n).$$

Алгоритм $\mathscr{A}$ назовем *полиномиальным*, если функция $\rho_M(\mathscr{A})$ ограничена некоторым полиномом от трех переменных $n$, $l$, $\log \gamma$. Будем говорить, что алгоритм $\mathscr{A}$ полиномиален при фиксированной размерности $n$ (*квазиполиномиален*), если найдется такой многочлен $p_n(\cdot, \cdot)$, степень и коэффициенты которого зависят только от $n$, что $\rho_M(\mathscr{A}) \leq p_n(l, \log \gamma)$. Очевидно, $\tau_M(\mathscr{A}) \leq \rho_M(\mathscr{A})$, и поэтому верхняя оценка вычислительной трудоемкости алгоритма является таковой и для его оракульной сложности.

Если из контекста ясно, о каком множестве $M$ идет речь, то вместо $\tau_M(\mathscr{A})$ и $\rho_M(\mathscr{A})$ будем писать соответственно $\tau(\mathscr{A})$ и $\rho(\mathscr{A})$.

В работе в качестве множества $\mathfrak{F}'$ рассматриваются, в частности, следующие классы функций:

1, 2) классы всех функций, множество нулей (соответственно единиц) которых можно задать системой линейных неравенств,

$$\bigcup_{M \in \mathfrak{M}} \mathfrak{F}_\nu(M) \qquad (\nu = 0, 1);$$

3) класс $\bigcup\limits_{M\in\mathfrak{M}}\Big(\mathfrak{F}_0(M)\cap\mathfrak{F}_1(M)\Big)$;

4) класс пороговых функций $\bigcup\limits_{M\in\mathfrak{M}}\mathfrak{T}(M)$;

5) класс пороговых функций $k$-значной логики $\bigcup\limits_{k\geq 2,\,n\geq 1}\mathfrak{T}(E_k^n)$;

6) класс пороговых функций $k$-значной логики, зависящих от двух переменных, $\bigcup\limits_{k\geq 2}\mathfrak{T}(E_k^2)$.

Для краткости расшифровку в перечисленных классах будем называть расшифровкой в классах $\mathfrak{F}_0(M)$, $\mathfrak{F}_1(M)$, $\mathfrak{F}_0(M)\cap\mathfrak{F}_1(M)$, $\mathfrak{T}(M)$, $\mathfrak{T}(E_k^n)$, $\mathfrak{T}(E_k^2)$, соответственно.

Для всех перечисленных классов от алгоритмов расшифровки будем требовать, чтобы они возвращали коэффициенты характеристических систем расшифровываемой функции. В случае пороговой функции — коэффициенты порогового неравенства.

Мы будем рассматривать алгоритмы, в которых выбор точки для нового обращения к оракулу, определяется ответами на предыдущие вопросы (условные тесты) [55, 62, 87]. Что же касается алгоритмов, не учитывающих ответы на предыдущие вопросы (безусловные тесты), то для рассматриваемых классов они оказываются весьма неэффективными (см. раздел 2.2).

Пусть $\mathfrak{F}(M,h)$ — множество таких $f\in\mathfrak{F}_0(M)\cap\mathfrak{F}_1(M)$, для которых $\min\{m_0(f),m_1(f)\}\leq h$. В разделе 2.3 описывается алгоритм $\mathscr{A}_0$ расшифровки в классе $\mathfrak{F}_0(M)\cap\mathfrak{F}_1(M)$. При любом фиксированном $n$ величина $\rho(\mathscr{A}_0)$ ограничена полиномом от $h$, $l$, $\log\gamma$, а

$$\tau(\mathscr{A}_0)=O\Big((l+h)^{\lfloor\frac{n}{2}\rfloor^2}l^{\lfloor\frac{n}{2}\rfloor}\log^{(n-1)\lfloor\frac{n}{2}\rfloor+n}(\gamma+1)\Big).$$

Алгоритм $\mathscr{A}_0$ использует в качестве вспомогательного оракульный алгоритм $\mathscr{A}_{\text{опт}}$ максимизации линейной функции $f\in\mathfrak{F}_{1-\nu}(M)$ на множестве $M_\nu$, описанный в подразделе 2.3.1.

Класс $\mathfrak{T}(M)$ пороговых функций рассматривается в разделе 2.4. Предлагается алгоритм $\mathscr{A}_1$ расшифровки в классе $\mathfrak{T}(M)$, для которого при фиксированном $n$ вычислительная трудоемкость $\rho(\mathscr{A}_1)$ ограничена полиномом от $l$ и $\log\gamma$, а

$$\tau(\mathscr{A}_1) \leq 16n^{10n-1}l^{\left\lfloor\frac{n}{2}\right\rfloor}\log^n(\gamma+1).$$

В частности, в классе $\mathfrak{T}(E_k^n)$ алгоритм имеет оракульную сложность

$$\tau(\mathscr{A}_1) = O(\log^n k).$$

Заметим, что на основе алгоритма $\mathscr{A}_1$ в разделе 3.9 будет построен алгоритм $\mathscr{A}_1^{\mathrm{o}}$, для которого при любом фикисрованном $n \geq 2$

$$\tau(\mathscr{A}_1^{\mathrm{o}}) = O(\log^{n-1} k).$$

В разделе 2.5 предлагается алгоритм $\mathscr{A}_2$ расшифровки в классе $\mathfrak{T}(E_k^2)$. Вычислительная трудоемкость $\rho(\mathscr{A}_2)$ алгоритма $\mathscr{A}_2$ ограничена полиномом от $\log k$, а

$$\tau(\mathscr{A}_2) = 6\log(k-1) + 4.$$

Нижние оценки оракульной сложности расшифровки функций из рассматриваемых классов получены в главе 3.

В разделе 2.6 исследуется задача расшифровки пороговой функции, заданной более информативным — «*расширенным*» — оракулом, который в отличие от «обычного» оракула принимает на вход произвольные точки из $\mathbb{Q}^n$, а не только из $M$. Расширенный оракул связан с конкретным пороговым неравенством функции $f$. По заданной точке $x \in \mathbb{Q}^n$ он возвращает 0, если пороговое неравенство выполнено, и 1 в противном случае. Под *расшифровкой пороговой функции $f$, заданной с помощью расширенного оракула*, будем понимать процедуру восстановления коэффициентов

ее любого возможного порогового неравенства с помощью обращений к этому оракулу. Предложен алгоритм расшифровки функции из класса $\mathfrak{T}(E_k^n)$, заданной с помощью расширенного оракула. При фиксированном $n$ алгоритм имеет полиномиальную от $\log k$ вычислительную трудоемкость и использует асимптотически не более $\frac{n^4}{2}\log(n+1) + 2n^3 \log k$ обращений к оракулу.

Результаты раздела 2.3 опубликованы в работе [22, 27]; раздела 2.4 — в работах [34, 160]; раздела 2.5 — в [21, 25]; раздела 2.6 — в [30].

## 2.2. Безусловные тесты для пороговых функций

Множество $U \subseteq M$ назовем *безусловным тестом* для класса функций $\mathfrak{F}' \subseteq \mathfrak{F}(M)$, если для любых двух $f, g$ из $\mathfrak{F}'$, $f \neq g$, найдется точка $x \in U$, такая, что $f(x) \neq g(x)$.

**Утверждение 2.1.** *Класс $\mathfrak{T}(E_k^n)$ обладает единственным безусловным тестом $U = E_k^n$.*

*Доказательство.* Рассмотрим отображение $h(x) : E_k^n \to \mathbb{N}$, заданное равенством $h(x) = h_{kn}(x) = k^{n-1}x_1 + (k^{n-1} + k^{n-2})x_2 + \cdots + (k^{n-1} + \cdots + 1)x_n$. Докажем, что если $x \neq y$, $x, y \in E_k^n$, то $h(x) \neq h(y)$.

Для $n = 1$ получаем $h_{k1}(x) = x_1$ и доказываемое утверждение очевидно. Предположим, что утверждение выполняется для числа переменных, меньших $n$, и докажем его для $n$. Пусть $h_{kn}(x) = h_{kn}(y)$, тогда $x_n \equiv y_n \pmod{k}$. Так как $0 \leq x_j \leq k-1$, $0 \leq y_j \leq k-1$, то $x_n = y_n$. Пусть $x' = (x_1, \ldots, x_{n-1})$, $y' = (y_1, \ldots, y_{n-1})$. Имеем

$$h_{kn}(x) = h_{k,n-1}(x') + (k^{n-1} + \cdots + 1)x_n = h_{k,n-1}(y') + (k^{n-1} + \cdots + 1)y_n,$$

следовательно, $x' = y'$ и $x = y$.

Упорядочим все наборы из $E_k^n$ по $h(x)$. В результате получим последовательность точек $x^{(1)}, x^{(2)}, \ldots, x^{(k^n)}$ и последовательность чисел

$$\left\{\alpha_i = h_{kn}(x^{(i)}) : \ i = 1, 2, \ldots, k^n\right\},$$

где $\alpha_1 = 0$, $\alpha_2 = k^{n-1}$, $\ldots$, $\alpha_{k^n} = (k-1)(k^{n-1} + \cdots + (k^{n-1} + \cdots + 1)) = nk^n - \frac{k^n-1}{k-1}$. Для каждого $i \in \{1, \ldots, k^n\}$ рассмотрим функцию $f_i \in F(E_k^n)$, такую, что $M_0(f_i) = \left\{x \in E_k^n : \ h_{kn}(x) \leq \alpha_i\right\}$. Очевидно, $f_i \in \mathfrak{T}(E_k^n)$, так как неравенство $h(x) \leq \alpha_i$ является для нее пороговым. Для любого $i \in \{1, \ldots, k^n\}$ имеем $M_0(f_{i+1}) = M_0(f_i) \cup \left\{x^{(i)}\right\}$.

Предположим, что безусловный тест $U$ не содержит точку $x = x^{(i)}$ для некоторого $i \in \{1, 2, \ldots, k^n\}$. Тогда найдется по крайней мере две функции $f_i$ и $f_{i+1}$ из класса $\mathfrak{T}(E_k^n)$, значения которых не различаются в точках из $U$. Полученное противоречие показывает, что $U = E_k^n$. ∎

Так как $\mathfrak{T}(E_k^n) \subseteq \mathfrak{F}_\nu(E_k^n)$ $(\nu = 0, 1)$, то аналогичные утверждения справедливы для классов $\mathfrak{F}_\nu(E_k^n)$ $(\nu = 0, 1)$, $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$. Все рассуждения легко переносятся на случай произвольного $M \in \mathfrak{M}(n, l, \gamma)$.

## 2.3. Расшифровка функций в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$

В [104] (см. также [105]) предложен алгоритм $\mathscr{A}'$ расшифровки функций из класса $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$. При фиксированных $n$ и $h$ алгоритм $\mathscr{A}'$ расшифровывает любую функцию $f$ из $\mathfrak{F}(E_k^n, h)$, совершая при этом полиномиальное от $\log k$ число операций и полиномиальное число обращений к оракулу. Так как $\mathfrak{T}(E_k^n) \subseteq \mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$, то алгоритм $\mathscr{A}'$, очевидно, применим и для расшифровки пороговых функций. В [138] с использованием результатов [127] показано, что в классе $\mathfrak{T}(E_k^n)$ алгоритм $\mathscr{A}'$ при фиксированном $n$ имеет сложность

$$\tau(\mathscr{A}') = O\left(\log^{\lfloor n/2 \rfloor (n-1)+n} k\right).$$

Здесь алгоритм $\mathscr{A}'$ обобщается на случай функций из класса $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. В классе $\mathfrak{F}(M, h)$ при любом фиксированном $n$ построенный алгоритм $\mathscr{A}_0$ имеет полиномиальную от $h$, $l$, $\log \gamma$ вычислительную трудоемкость и оракульную сложность

$$\tau(\mathscr{A}_0) = O\left((l+h)^{\lfloor n/2 \rfloor^2} l^{\lfloor n/2 \rfloor} \log^{(n-1)\lfloor n/2 \rfloor + n} \gamma\right).$$

Для заданной оракулом функции $f$ данный алгоритм находит $N_\nu(f)$ при некотором $\nu = 0, 1$. Дальнейшее вычисление $f(x)$ сводится затем к определению принадлежности $x$ выпуклой оболочке множества $N_\nu(f)$. Как следует из [81] и утверждения 1.16, при любом фиксированном $n$ это можно сделать за полиномиальное от $l$ и $\log \gamma$ время.

### 2.3.1. Оракульный алгоритм максимизация линейной функции

Вначале построим вспомогательный оракульный алгоритм $\mathscr{A}_{\text{опт}}$, решающий задачу максимизации линейной функции на множестве $M_\nu(f)$, где $f \in \mathfrak{F}_{1-\nu}(M)$.

**Теорема 2.2.** *Существует алгоритм $\mathscr{A}_{\text{опт}}$, который для любого $\nu \in \{0, 1\}$, любой заданной оракулом функции $f \in \mathfrak{F}_{1-\nu}(M)$ и любого вектора $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ находит точку $p = (p_1, \ldots, p_n) \in M_\nu(f)$, такую, что*

$$\sum_{j=1}^{n} a_j p_j = \max\left\{\sum_{j=1}^{n} a_j x_j : \ (x_1, \ldots, x_n) \in M_\nu(f)\right\},$$

*или устанавливает, что $M_\nu(f) = \varnothing$. При фиксированном $n$ алгоритм имеет полиномиальную от $l$ и $\log \alpha$ вычислительную трудоемкость и совершает не более $n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\alpha+1)$ (при $n \geq 2$) и не более $8 + 2\log \gamma$ (при $n = 1$) обращений к оракулу, где $\alpha = \max\{\gamma, |a_j|, j = 1, \ldots, n\}$.*

*Доказательство.* Для любой точки $(x_1, \ldots, x_n) \in M$ по следствию 1.8

выполняется неравенство:

$$\left|\sum_{j=1}^{n} a_j x_j\right| < \sum_{j=1}^{n}(n+1)(\gamma\sqrt{n})^n|a_j| \le \beta,$$

где $\beta = n^{1+\frac{n}{2}}(n+1)\alpha^{n+1}$. Следовательно,

$$\max_{x\in M_\nu(f)} \sum_{j=1}^{n} a_j x_j - \min_{x\in M_\nu(f)} \sum_{j=1}^{n} a_j x_j < 2\beta.$$

Из леммы 1.21 следует, что для любого целого $a_0$, такого, что $|a_0| \le \beta$, при фиксированном $n$ с полиномиальной от $l$ и $\log\alpha$ вычислительной трудоемкостью можно построить множество $N(a, a_0)$ вершин политопа

$$\mathrm{Conv}\left(\left\{x = (x_1, \ldots, x_n) : \sum_{j=1}^{n} a_j x_j \ge a_0\right\} \cap M\right).$$

Рассмотрим функцию $g \in \mathfrak{T}(M)$, определяемую пороговым неравенством $\sum\limits_{j=1}^{n} a_j x_j \ge a_0$. Из утверждения 1.18 получаем

$$|N(a, a_0)| = |N_0(g)| \le n^{10n-5} l^{\lfloor\frac{n}{2}\rfloor} \log^{n-1}(\gamma+1). \qquad (2.1)$$

Обращаясь к оракулу не более $|N(a, a_0)|$ раз, можно найти точку $x$ в $M_\nu(f) \cap N(a, a_0)$ или доказать, что таких точек нет. Так как $f \in \mathfrak{F}_{1-\nu}(M)$, то из равенства $M_\nu(f) \cap N(a, a_0) = \varnothing$ следует, что для всех $x = (x_1, \ldots, x_n) \in M$, таких, что $\sum\limits_{j=1}^{n} a_j x_j \ge a_0$, выполняется соотношение $f(x) = 1 - \nu$, т. е. если $x = (x_1, \ldots, x_n) \in M_\nu(f)$, то $\sum\limits_{j=1}^{n} a_j x_j \le a_0 - 1$.

Опишем теперь алгоритм $\mathscr{A}_{\text{опт}}$.

Шаг 0. Положим $u := -\beta$; $v := \beta$; построим $N(a, u)$. С помощью обращений к оракулу в точках из $N(a, u)$ определим, выполнено ли равенство $N(a, u) \cap M_\nu(f) = \varnothing$. Если это равенство выполнено, то стоп: $M_\nu(f) = \varnothing$.

Шаг 1. Положим $w := \left\lfloor \dfrac{u+v}{2} \right\rfloor$.

Шаг 2. Построим $N(a, w)$.

Шаг 3. С помощью обращений к оракулу в точках из $N(a, w)$ определим, выполнено ли равенство $N(a, w) \cap M_v(f) = \varnothing$. Если это равенство выполнено, то положим $v := w$. В противном случае обозначим через $p$ какую-нибудь точку из $N(a, w) \cap M_v(f)$ и положим $u := w$.

Шаг 4. Если $v = u + 1$, то стоп: возвращаем точку $p$, иначе перейдем на шаг 1.

Шаги 0–4 являются дихотомией по отрезку $[-\beta, \beta]$, находящей такую точку $p = (p_1, \ldots, p_n)$, что

$$\sum_{j=1}^{n} a_j p_j = w = \max \left\{ \sum_{j=1}^{n} a_j x_j : x \in M_v(f) \right\}.$$

Очевидно, число итераций этой процедуры не превосходит величины $1 + \lfloor \log 2\beta \rfloor$. Учитывая трудоемкость построения $N(a, a_0)$ на шаге 2, получаем, что при фиксированном $n$ вычислительная трудоемкость алгоритма $\mathscr{A}_{\text{опт}}$ полиномиальна от $l$ и $\log \alpha$.

Оценим теперь количество обращений к оракулу. Они происходят на шагах 0 и 3 в точках множеств $N(a, w)$ при различных $w$. Общее число итераций этих шагов не превосходит величины

$$\lfloor \log 2\beta \rfloor + 2 \le 4 + \left(1 + \frac{n}{2}\right) \log n + \log(n+1) + (n+1) \log \alpha <$$

$$< 4 + \left(2 + \frac{n}{2}\right) \log n + \frac{1}{n} \log e + (n+1) \log(\alpha + 1).$$

Легко видеть, что при $n \ge 2$ оцениваемая величина не превосходит (грубая оценка) $n^4 \log(\alpha + 1)$. Используя неравенство (2.1), получаем, что

общее число обращений к оракулу при $n \geq 2$ не превосходит

$$n^{10n-5} l^{\lfloor \frac{n}{2} \rfloor} \log^{n-1}(\gamma+1) \cdot n^4 \log(\alpha+1) \leq n^{10n-1} l^{\lfloor \frac{n}{2} \rfloor} \log^n(\alpha+1).$$

При $n = 1$ имеем $|N(a, a_0)| \leq 2$, поэтому общее число обращений к оракулу не превосходит $2(\lfloor \log 2\gamma \rfloor + 2) \leq 8 + 2\log\gamma$. ∎

**Лемма 2.3.** *Если $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, то для любого $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ точка $p$, возвращаемая алгоритмом $\mathscr{A}_{\text{опт}}$, принадлежит $N_\nu(f)$.*

*Доказательство.* Покажем, что при $f \in \mathfrak{F}_0 \cap \mathfrak{F}_1$ и $M_\nu(f) \neq \varnothing$ алгоритм $\mathscr{A}_{\text{опт}}$ выдает точку $p = (p_1, \ldots, p_n)$ из множества $N_\nu(f)$. Предположим, что $p \notin N_\nu(f)$. Тогда найдутся такие точки $p^{(i)} = (p_1^{(i)}, \ldots, p_n^{(i)}) \neq p$ из $M_\nu(f)$ и такие числа $\alpha_i > 0$ $(i = 1, \ldots, s)$, что $\sum\limits_{i=1}^{s} \alpha_i = 1$ и

$$p = \sum_{i=1}^{s} \alpha_i p^{(i)}. \tag{2.2}$$

Отсюда

$$\sum_{j=1}^{n} a_j p_j = \sum_{i=1}^{s} \alpha_i \sum_{j=1}^{n} a_j p_j^{(i)} = w, \tag{2.3}$$

где $w$ — найденный максимум. Так как $\alpha_i > 0$, $\sum\limits_{i=1}^{s} \alpha_i = 1$, то из (2.3) следует, что либо найдется $i' \in \{1, \ldots, s\}$, такое, что $\sum\limits_{j=1}^{n} a_j p_j^{(i')} > w$, либо для каждого $i \in \{1, \ldots, s\}$ выполняется равенство $\sum\limits_{j=1}^{n} a_j p_j^{(i)} = w$. В первом из этих случаев $p$ не является точкой максимума, а во втором — ввиду (2.2) $p \notin N(a, w)$. ∎

### 2.3.2. Алгоритм расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$

**Теорема 2.4.** *Существует алгоритм $\mathscr{A}_0$ расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. В классе $\mathfrak{F}(M, h)$, где $M \in \mathfrak{M}(n, l, \gamma)$, при любом фиксированном $n$*

*алгоритм имеет полиномиальную от* $h$, $l$ *и* $\log\gamma$ *вычислительную трудоемкость и оракульную сложность*

$$\tau(\mathscr{A}_0) = O\big((l+h)^{\lfloor\frac{n}{2}\rfloor^2} l^{\lfloor\frac{n}{2}\rfloor} \log^{(n-1)\lfloor\frac{n}{2}\rfloor+n}(\gamma+1)\big)$$

(*асимптотика при фиксированном* $n$).

*Доказательство.* Прежде чем переходить к пошаговому описанию алгоритма $\mathscr{A}_0$, опишем его общую идею. Алгоритм $\mathscr{A}_0$ с помощью вспомогательной процедуры $\mathscr{A}_{\text{опт}}$ последовательно находит крайние точки множеств $P_\nu(f)$ $(\nu = 0, 1)$, запоминая их в $S_\nu \subseteq N_\nu(f)$. Неравенства системы, описывающей $P_\nu(f)$, накапливаются в $H_\nu$. Множество $H'_\nu$ содержит неравенства из описания $\operatorname{Conv} S_\nu$, не вошедшие в $H_\nu$. На выходе алгоритма — множества $N_\nu(f)$ $(\nu = 0, 1)$.

Неравенство из системы неравенств $H$ назовем эквивалентным неравенству $h'$ относительно $H$, если после замены первого вторым множество решений системы $H$ не меняется. Известно (см. [81], а также раздел 1.6), что для нахождения общего решения системы линейных неравенств с целыми (или рациональными) коэффициентами при любом фиксированном числе переменных $n$ существуют полиномиальные алгоритмы. На их основе легко построить алгоритмы, проверяющие эквивалентность пар неравенств.

Опишем алгоритм $\mathscr{A}_0$.

Шаг 0. Пусть $H_\nu$ $(\nu = 0, 1)$ — пустая система линейных неравенств. Определим $f(x)$ для всех вершин множества $\operatorname{Conv} M$ и обозначим через $S_\nu$ $(\nu = 0, 1)$ множество тех из них, для которых $f(x) = \nu$. Если при $\nu = 0$ или при $\nu = 1$ множество $S_\nu$ пусто, то расшифровка завершена, так как в этом случае $M_\nu(f) = \varnothing$.

Шаг 1. Для каждого $\nu \in \{0,1\}$ найдем неприводимую систему линейных неравенств, описывающую $\operatorname{Conv} S_\nu$; из этой системы удалим те неравенства, для каждого из которых в $H_\nu$ существует ему эквивалентное (относительно исходной системы) неравенство. Полученную систему обозначим через $H'_\nu$.

Шаг 2. Для каждого $\nu \in \{0,1\}$ выполним последовательность шагов 2.1–2.4 и затем вернемся на шаг 1.

Шаг 2.1. Если система $H'_\nu$ пуста, то $N_\nu(f) = S_\nu$ — расшифровка завершена.

Шаг 2.2. Из $H'_\nu$ выберем произвольное неравенство $\sum\limits_{j=1}^{n} a_j x_j \le a_0$ и исключим его оттуда.

Шаг 2.3. С помощью алгоритма $\mathscr{A}_{\text{опт}}$ найдем точку $p = (p_1, \ldots, p_n) \in N_\nu(f)$, максимизирующую $\sum\limits_{j=1}^{n} a_j x_j$ на $M_\nu(f)$.

Шаг 2.4. Если $\sum\limits_{j=1}^{n} a_j p_j \le a_0$, то добавим к $H_\nu$ неравенство $\sum\limits_{j=1}^{n} a_j x_j \le a_0$ и перейдем на шаг 2.1, в противном случае присоединим $p$ к $S_\nu$.

Для доказательства корректности алгоритма $\mathscr{A}_0$ заметим, что на шаге 0 при любом $\nu = 0,1$ $S_\nu \subseteq N_\nu(f)$ и, если $S_\nu = \varnothing$, то по утверждению 1.5 $M_\nu(f) = \varnothing$. Легко видеть, что алгоритм завершит свою работу, когда для некоторого $\nu = 0,1$ все точки $x \in M_\nu(f)$ будут удовлетворять системе $H_\nu$, т. е. при $S_\nu = N_\nu(f)$.

Оценим вычислительную трудоемкость алгоритма $\mathscr{A}_0$. По лемме 1.21 построить все вершины множества $\operatorname{Conv} M$ на шаге 0 можно при фиксированном $n$ за полиномиальное от $l$ и $\log \gamma$ время. Лемма 1.12 гарантирует, что число обращений к оракулу на этом шаге не больше

$n^{4n}\xi_n(l)\log^{n-1}(\gamma+1)$. Для нахождения на шаге 1 системы, описывающей $\operatorname{Conv} S_\nu$, достаточно решить $\binom{|S_\nu|}{n}$ систем $n$ линейных уравнений от $n+1$ неизвестных. Как и в следствии 1.10, из неравенства Адамара следует, что при фиксированном $n$ абсолютные величины найденных таким образом коэффициентов ограничены сверху некоторым полиномом от $\gamma$. Учитывая, что количество систем, которые нужно решить, полиномиально от $|S_\nu|$, для процедуры шага 1 при фиксированном $n$ получаем алгоритм, полиномиальный от $|S_\nu|$ и $\log\gamma$ и числа неравенств в $H_\nu$. На каждой итерации шага 2 для каждого $\nu = 0,1$ к $S_\nu$ присоединяется лишь одна точка. Следовательно, ввиду того, что $S_\nu \subseteq N_\nu(f)$, получаем: $|S_\nu| \leq |N_{\nu'}(f)|$, где $\nu'$ определяется из равенства $m_{\nu'}(f) = h$. Учитывая оценку из утверждения 1.16, получаем:

$$|S_\nu| \leq |N_{\nu'}(f)| \leq n^{10n-6}(l+h)^{\lfloor \frac{n}{2} \rfloor}\log^{n-1}(\gamma+1).$$

Для дальнейшего доказательства сделаем несколько очевидных замечаний. Во-первых, к $H_\nu$ на шаге 2.4 добавляются только неравенства, соответствующие опорным к $P_\nu(f)$ и $\operatorname{Conv} S_\nu$ гиперплоскостям. Во-вторых, каждое такое неравенство либо описывает некоторую фасету (грань максимальной размерности) политопа $\operatorname{Conv} S_\nu$, либо является неявным равенством (см., например, [81, §§ 8.1, 8.4]). По теореме МакМюллена [151] (см. [7]) число фасет (граней максимальной размерности) выпуклой оболочки конечной системы из $s$ точек не превосходит $\xi_n(s)$ (определение функции $\xi_n(s)$ см. на стр. 38). Так как система, построенная на шаге 1, неприводима, то число $|H_\nu|$ неравенств в $H_\nu$ можно оценить: $|H_\nu| < \xi_n(|N_\nu(f)|)$. Так как при каждом обращении к алгоритму $\mathscr{A}_{\text{опт}}$ происходит добавление нового элемента либо к $H_\nu$, либо к $S_\nu$, из оценки (2.3.2) получаем, что количество этих обращений, а также общее число

итераций шага 2 не превосходит величины

$$|S_\nu| + |H_\nu| \le C_n\big((l+h)^{\lfloor \frac{n}{2} \rfloor} \log^{n-1}(\gamma+1)\big)^{\lfloor \frac{n}{2} \rfloor},$$

где $C_n$ — некоторая зависящая только от $n$ величина. Принимая во внимание количество обращений к оракулу в алгоритме $\mathscr{A}_{\text{опт}}$ и на шаге 0 алгоритма $\mathscr{A}_0$, получаем:

$$\tau(\mathscr{A}_0) \le C_n (l+h)^{\lfloor \frac{n}{2} \rfloor^2} l^{\lfloor \frac{n}{2} \rfloor} \log^{(n-1)\lfloor \frac{n}{2} \rfloor + n}(\gamma+1),$$

где $C_n$ — некоторая зависящая только от $n$ величина. ∎

Так как $\mathfrak{T}(M) \subseteq \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, то алгоритм $\mathscr{A}_0$ применим и к классу $\mathfrak{T}(M)$, однако верхняя оценка его оракульной сложности выше, чем у алгоритма $\mathscr{A}_1$, описанного ниже в разделе 2.4.

Если известно, что $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$, то алгоритмом $\mathscr{A}_0$ мы можем найти множества $N_\nu(f)$ $(\nu = 0, 1)$, а затем построить систему линейных неравенств, эквивалентную (1.6) и найти ее порождающую систему $b^{(1)}, \ldots, b^{(s)}$. Если существуют $b^{(i)}$ с положительной последней координатой, то $f \in \mathfrak{T}(M)$, в противном случае $f \notin \mathfrak{T}(M)$. Так как при фиксированном $n$ трудоемкость вычисления каждого $b^{(i)}$ полиномиальна от $l$, $m_0(f)$, $m_1(f)$, $\log\gamma$, то имеет место

**Теорема 2.5.** *Если $f \in \mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$ задана оракулом, то при любом фиксированном $n$ существует полиномиальный от $l$, $m_0(f)$, $m_1(f)$, $\log\gamma$ алгоритм распознавания пороговости и построения конуса $K(f)$.*

## 2.4. Расшифровка пороговых функций

Здесь предлагается алгоритм $\mathscr{A}_1$ расшифровки функций в классе $\mathfrak{T}(M)$. При любой фиксированной размерности $n$ алгоритм имеет полиномиальную от $l$ и $\log\gamma$ вычислительную трудоемкость и оракульную

сложность

$$\tau(\mathscr{A}_1) \leq 16n^{10n-1}l^{\lfloor \frac{n}{2} \rfloor} \log^n(\gamma + 1).$$

### 2.4.1. Расшифровка функций из класса $\mathfrak{T}_+(M)$

Обозначим через $\mathfrak{T}_+(M)$ множество тех функций из $\mathfrak{T}(M)$, для которых существует пороговое неравенство (1.2) с коэффициентом $a_0 > 0$. Очевидно, что для любой $f \in \mathfrak{T}_+(M)$ существует пороговое неравенство вида

$$\sum_{i=1}^{n} a_i x_i \leq 1, \tag{2.4}$$

в котором по следствию 1.9 коэффициенты $a_i$ можно сделать рациональными и не превосходящими по модулю величины $\chi(n, \gamma)$. Запишем систему (1.6) в следующем виде:

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \leq 1 \quad \text{для всех} \quad (x_1, \ldots, x_n) \in M_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j > 1 \quad \text{для всех} \quad (x_1, \ldots, x_n) \in M_1(f). \end{cases} \tag{2.5}$$

В пространстве $\mathbb{R}^n$ векторов $(a_1, \ldots, a_n)$ замыкание множества решений этой системы есть некоторый полиэдр $W(f)$, любая внутренняя точка которого дает коэффициенты порогового неравенства (2.4) функции $f$. Заметим, что похожие преобразования осуществляются в [150] для функций из класса $\mathfrak{T}(E_k^n)$.

**Лемма 2.6.** (ср. [150]) *Для любой функции* $f \in \mathfrak{T}_+(M)$

$$\operatorname{Vol} W(f) \geq \frac{1}{\big(\chi(n, \gamma) + 1\big)^n n^n \big((n+1)(\gamma\sqrt{n})^n\big)^n}. \tag{2.6}$$

*Доказательство.* Пусть $a_0, \ldots, a_n$ — коэффициенты порогового неравенства (1.2), существование которых утверждается в следствии 1.9, причем $a_0 > 0$. Введем обозначение $\varkappa(n, \gamma) = (n+1)(\gamma\sqrt{n})^n$ (см. лемму 1.7). Пусть

$w = (w_1, \ldots, w_n)$, где $w_j = \dfrac{2a_j}{2a_0 + 1}$ $(j = 1, \ldots, n)$. Покажем, что точка $w$ вместе с окрестностью

$$W' = \prod_{i=1}^{n} \left[ w_i - \frac{1}{2(a_0 + 1)n\varkappa(n, \gamma)};\ w_i + \frac{1}{2(a_0 + 1)n\varkappa(n, \gamma)} \right]$$

включена в $W(f)$ (через $\prod\limits_{i=1}^{n} \Gamma_i$ обозначено декартово произведение $\Gamma_1 \times \Gamma_2 \times \cdots \times \Gamma_n$). Для этого рассмотрим точку $u = (u_1, \ldots, u_n) \in \mathbb{R}^n$, такую, что $u_i = w_i + \varepsilon_i$ $(i = 1, \ldots, n)$ и

$$\varepsilon_i \in \left[ -\frac{1}{2(a_0 + 1)n\varkappa(n, \gamma)};\ \frac{1}{2(a_0 + 1)n\varkappa(n, \gamma)} \right].$$

а) Пусть $x = (x_1, \ldots, x_n) \in M_0(f)$, т. е. $\sum\limits_{j=1}^{n} a_j x_j \leq a_0$, тогда

$$\sum_{j=1}^{n} u_j x_j = \sum_{j=1}^{n} \frac{2a_j}{2a_0 + 1} x_j + \sum_{j=1}^{n} \varepsilon_j x_j \leq \frac{2a_0}{2a_0 + 1} + \frac{n\varkappa(n, \gamma)}{2(a_0 + 1)n\varkappa(n, \gamma)} =$$

$$= 1 - \frac{1}{2a_0 + 1} + \frac{1}{2a_0 + 2} < 1.$$

б) Пусть $x = (x_1, \ldots, x_n) \in M_1(f)$, т. е. $\sum\limits_{j=1}^{n} a_j x_j \geq a_0 + 1$, тогда

$$\sum_{j=1}^{n} u_j x_j = \sum_{j=1}^{n} \frac{2a_j}{2a_0 + 1} x_j + \sum_{j=1}^{n} \varepsilon_j x_j = \frac{2}{2a_0 + 1} \sum_{j=1}^{n} x_j a_j + \sum_{j=1}^{n} \varepsilon_j x_j \geq$$

$$\geq \frac{2(a_0 + 1)}{2a_0 + 1} - \frac{\varkappa(n, \gamma)n}{2(a_0 + 1)\varkappa(n, \gamma)n} = 1 + \frac{1}{2a_0 + 1} - \frac{1}{2a_0 + 2} > 1.$$

Таким образом,

$$\operatorname{Vol} W(f) \geq \frac{1}{(a_0 + 1)^n n^n \big(\varkappa(n, \gamma)\big)^n} \geq \frac{1}{\big(\chi(n, \gamma) + 1\big)^n n^n \big((n + 1)(\gamma\sqrt{n})^n\big)^n},$$

что требовалось доказать. ∎

**Лемма 2.7.** *Объем области*

$$W(f) \cap \{a = (a_1, \ldots, a_n) \in \mathbb{R}^n : |a_i| \leq 3\chi(n, \gamma)\}$$

*не меньше величины в правой части неравенства* (2.6).

*Доказательство.* Требуемое неравенство следует из включения

$$W' \subseteq W(f) \cap \{a = (a_1, \ldots, a_n) \in \mathbb{R}^n : \ |a_i| \leq 3\chi(n, \gamma)\},$$

справедливость которого очевидна. ∎

Описываемый ниже алгоритм $\mathscr{A}_1^+$ проводит расшифровку при допущении $f \in \mathfrak{T}_+(M)$. Впоследствии мы покажем, как обобщить $\mathscr{A}_1^+$ на случай $f \in \mathfrak{T}(M)$.

Задача расшифровки решена, если найдена точка $a \in W(f)$. Алгоритм $\mathscr{A}_1^+$ последовательно выдвигает гипотезы $a^{(1)}, a^{(2)}, \ldots, a^{(i)}, \ldots$ о векторе $a$. Всякий раз гипотеза $a^{(i)}$ проверяется с помощью серии обращений к оракулу. Если гипотеза верна, т. е. $a^{(i)} \in W(f)$, то алгоритм $\mathscr{A}_1^+$ завершает свою работу, в противном случае используются результаты проверки — значения функции в нескольких новых точках из $M$. Эти точки и значения в них дают коэффициенты неравенств, которым должна удовлетворять любая точка из $W(f)$. Алгоритм начинает поиск точки $a \in W(f)$ с «подозрительной области»

$$W_0 = \left\{(w_1, \ldots, w_n) : \ |w_j| \leq 3\chi(n, \gamma) \ \ (j = 1, \ldots, n)\right\}, \qquad (2.7)$$

постепенно уменьшая ее объем и давая последовательность вложенных политопов: $W_0 \supseteq W_1 \supseteq \cdots \supseteq W_i \supseteq \ldots$ Проверка очередной гипотезы $a^{(i)}$ с помощью обращений к оракулу либо завершает работу алгоритма, либо добавляет к неравенствам, описывающим $W_i$, новые. Этим новым неравенствам, однако, не удовлетворяет точка $a^{(i)}$. По–видимому, для быстрой расшифровки необходимо в качестве гипотез $a^{(i)}$ брать точки, лежащие в «центре» политопа $W_i$ (ср. [150]). Давая различные определения «центра» политопа, будем получать различные алгоритмы расшифровки. Заметим, что аналогичная идея используется в выпуклом программировании и комбинаторной оптимизации (см. обзоры в [81, 111]), в [150]

приведенный метод используется для получения алгоритмов обучения пороговых элементов.

В данной работе в качестве $a^{(i)}$ берется центр тяжести политопа $W_i$, т. е. точка

$$a^{(i)} = \int\limits_{W_i} x dx \Big/ \int\limits_{W_i} dx\,, \tag{2.8}$$

где $\int_{W_i} dx = \operatorname{Vol} W_i$. По лемме 2.6 $\operatorname{Vol} W_i > 0$. Отсюда в частности получаем, что $a^{(i)}$ является внутренней точкой политопа $W_i$.

Перейдем теперь к пошаговому описанию алгоритма $\mathscr{A}_1^+$.

Шаг 0. Положим $S_\nu := \varnothing$ $(\nu = 0, 1)$, $i = 0$.

Шаг 1. (Выдвинуть гипотезу.) Найдем точку $a^{(i)} = (a_1^{(i)}, a_2^{(i)}, \ldots, a_n^{(i)})$ — центр тяжести политопа $W_i$, описываемого системой линейных неравенств

$$\begin{cases} \sum\limits_{j=1}^{n} w_j x_j \le 1 & \text{для всех } (x_1, \ldots, x_n) \in S_0; \\ \sum\limits_{j=1}^{n} w_j x_j \ge 1 & \text{для всех } (x_1, \ldots, x_n) \in S_1; \\ |w_j| \le 3\chi(n, \gamma) & (j = 1, 2, \ldots, n). \end{cases} \tag{2.9}$$

Шаг 2. (Проверить гипотезу.) Определим множество $N_0^{(i)}$ крайних точек выпуклой оболочки множества

$$M \cap \left\{ (x_1, \ldots, x_n) : \sum_{j=1}^{n} x_j a_j^{(i)} \le 1 \right\}$$

и множество $N_1^{(i)}$ крайних точек выпуклой оболочки множества $M \cap \left\{ (x_1, \ldots, x_n) : \sum\limits_{j=1}^{n} x_j a_j^{(i)} > 1 \right\}$. Для каждого $\nu = 0, 1$ и каждого $x \in N_\nu^{(i)}$ выполним следующие действия: с помощью оракула найдем $f(x)$; если $f(x) = 1 - \nu$, то присоединим $x$ к $S_\nu$. Если точек $x$, таких, что $x \in N_\nu^{(i)}$, $f(x) = 1 - \nu$, не нашлось, т. е. на

текущей итерации шага 2 ни к $S_0$, ни к $S_1$ не добавлено ни одного элемента, то стоп: $a^{(i)} \in W(f)$, процесс расшифровки закончен, в противном случае увеличим $i$ на единицу и перейдем на шаг 1.

Пусть все процедуры, используемые только что описанным алгоритмом (нахождение центра тяжести, нахождение множества крайних точек и др.), можно выполнить за конечное число шагов. Из равносильности систем (1.7) и (1.6) получаем, что если $g, f \in \mathfrak{T}(M)$ и для любого $x \in N_\nu(g)$ выполняется $f(x) = \nu$ ($\nu = 0, 1$), то $g = f$. Таким образом, если алгоритм $\mathscr{A}_1^+$ завершил свою работу, то $a^{(i)} \in W(f)$ — функция $f$ расшифрована.

Для оценки числа обращений к оракулу в алгоритме $\mathscr{A}_1^+$ сначала воспользуемся следующей геометрической леммой.

**Лемма 2.8.** [59] *Пусть $W$ — выпуклое замкнутое ограниченное тело в $\mathbb{R}^n$; $W_+$ и $W_-$ — части, на которые делит $W$ проходящая через центр тяжести тела гиперплоскость. Тогда*

$$\max\Big\{\operatorname{Vol} W_+, \operatorname{Vol} W_-\Big\} \le \left(1 - \left(\frac{n}{n+1}\right)^n\right) \operatorname{Vol} W \le \frac{e-1}{e} \operatorname{Vol} W \approx 0.63 \operatorname{Vol} W.$$

Данная лемма показывает, что выбор в качестве очередной гипотезы $a^{(i)}$ центра тяжести политопа $W_i$ действительно гарантирует значительное сокращение объема «подозрительной» области $W_i$ — не менее чем в $(e-1)/e$ раз: так как политоп $W_i$ — выпуклый и $a^{(i)}$ либо не принадлежит $W_{i+1}$, либо лежит на границе $W_{i+1}$, то $W_{i+1}$ полностью содержится в одной из частей, на которые разбивается $W_i$ некоторой гиперплоскостью, проходящей через $a^{(i)}$ . Отсюда и из леммы 2.7 следует, что любая функция $f \in \mathfrak{T}_+(M)$ будет расшифрована не более, чем за $S_{\max}$ гипотез вида «$a^{(i)} \in W(f)$?», где

$$S_{\max} = \log \frac{\operatorname{Vol} W_0}{\operatorname{Vol} W(f)} \Big/ \log \frac{e}{e-1} + 1 \approx 1.51 \times \log \frac{\operatorname{Vol} W_0}{\operatorname{Vol} W(f)}. \qquad (2.10)$$

Вспоминая определение политопа $W_0$, из следствия 1.9 и леммы 2.7 получаем:

$$\frac{\operatorname{Vol} W_0}{\operatorname{Vol} W(f)} \le \big(6\chi(n,\gamma)\big)^n \cdot \big(\chi(n,\gamma)+1\big)^n n^n \big((n+1)(\gamma\sqrt{n})^n\big)^n \le$$

$$\le 6^n e\chi(n,\gamma)^{2n} n^n (n+1)^n (\gamma\sqrt{n})^{n^2} < 6^n e(n+1)^{\frac{n+3}{2}\cdot 2n} (\gamma\sqrt{n})^{2n^3} e n^{2n} (\gamma\sqrt{n})^{n^2} \le$$

$$\le e^2 2^{n^2+3n} 6^n n^{n^3+\frac{3}{2}n^2+5n} \gamma^{2n^3+n^2},$$

откуда

$$\log\frac{\operatorname{Vol} W_0}{\operatorname{Vol} W(f)} \le 2\log e + n^2 + 3n + n\log 6 + \left(n^3+\frac{3}{2}n^2+5n\right)\log n + (2n^3+n^2)\log\gamma.$$

Таким образом, из (2.10)

$$S_{\max} \lesssim \frac{2n^3\log(\gamma\sqrt{n})}{\log e/(e-1)} \qquad (n\to\infty) \tag{2.11}$$

и, как нетрудно проверить, $S_{\max} \le 16n^4\log(\gamma+1)$. Теперь из утверждения 1.18 получаем:

$$\tau(\mathscr{A}_1^+) \le 16n^{10n-1} l^{\left\lfloor\frac{n}{2}\right\rfloor} \log^n(\gamma+1).$$

Для оценки $\rho(\mathscr{A}_1^+)$ докажем следующее вспомогательное утверждение.

**Лемма 2.9.** *Пусть политоп $Q \subset \mathbb{R}^n$ задан системой $m$ линейных неравенств с целочисленными коэффициентами, по абсолютной величине не превосходящими $\alpha$. Тогда при любом фиксированном $n$ центр тяжести $a$ политопа $Q$ есть рациональная точка с длиной двоичного разложения не выше полинома от $m$ и $\log\alpha$ и существует полиномиальный от $m$ и $\log\alpha$ алгоритм ее отыскания.*

*Доказательство.* Построим этот алгоритм. В начале найдем разбиение политопа $Q$ на симплексы $\Upsilon_i$, т. е. получим такое представление

$$Q = \bigcup_{i=1}^{\sigma} \Upsilon_i, \tag{2.12}$$

что $\Upsilon_i$ $(i = 1, \ldots, \sigma)$ — симплекс и аффинная размерность пересечения любых двух различных симплексов из этого представления меньше $n$. Алгоритмы, которые при фиксированном $n$ за полиномиальное от $m$ и $\log \alpha$ время по системе неравенств, описывающей политоп $Q$, строят список вершин симплексов $\Upsilon_1, \ldots, \Upsilon_\sigma$ для некоторого разбиения (2.12) приведены в [92, 105]. Понятно, что при любом фиксированном $n$ длины двоичного разложения построенных вершин и параметр $\sigma$ ограничены некоторым полиномом от $m$ и $\log \alpha$. Известно (см. [63, стр. 71]), что центр тяжести $z = (z_1, \ldots, z_n)$ и объем $\operatorname{Vol} \Upsilon$ симплекса $\Upsilon$ может быть найден соответственно по формулам:

$$z_j = \frac{v_j^{(0)} + v_j^{(1)} + \cdots + v_j^{(n)}}{n+1} \quad (j = 1, \ldots, n),$$

$$\operatorname{Vol} \Upsilon = \frac{1}{n!} \begin{vmatrix} 1 & v_1^{(0)} & \ldots & v_n^{(0)} \\ 1 & v_1^{(1)} & \ldots & v_n^{(1)} \\ \vdots & \vdots & & \vdots \\ 1 & v_1^{(n)} & \ldots & v_n^{(n)} \end{vmatrix},$$

где $v_\mu = (v_1^{(\mu)}, v_2^{(\mu)}, \ldots, v_n^{(\mu)})$ $(\mu = 0, 1, \ldots, n)$ — вершины симплекса $\Upsilon$, а для нахождения объема берется абсолютная величина соответствующего определителя. Координаты центра тяжести $a = (a_1, \ldots, a_n)$ всего политопа $Q$, как следует из (2.8), выражаются тогда через координаты центров тяжести $z^{(i)} = (z_1^{(i)}, \ldots, z_n^{(i)})$ и объемы $\operatorname{Vol} \Upsilon_i$ симплексов $\Upsilon_i$ следующим образом:

$$a_j = \frac{\sum\limits_{i=1}^{\sigma} \operatorname{Vol} \Upsilon_i \cdot z_j^{(i)}}{\sum\limits_{i=1}^{\sigma} \operatorname{Vol} \Upsilon_i} \quad (j = 1, \ldots, n).$$

Оценки на длину компонент центра тяжести $a$ и трудоемкость алгоритма вытекают теперь из приведенных формул. ∎

Количество неравенств в системе (2.9), описывающей политоп $W_i$,

очевидно, не превосходит $\tau(\mathscr{A}_1^+) + 2n$. Абсолютные величины коэффициентов этой системы, как следует из следствия 1.9, при фиксированном $n$ ограничены полиномом от $\gamma$. Из леммы 2.9 получаем, что при фиксированном $n$ центр тяжести $a^{(i)}$ политопа $W_i$ будет найден за полиномиальное от $l$ и $\log\gamma$ время. Для нахождения множеств $N_0^{(i)}$ и $N_1^{(i)}$ на шаге 2 воспользуемся полиномиальным при фиксированном $n$ алгоритмом из леммы 1.21. Вследствие полиномиальной от $l$ и $\log\gamma$ ограниченности двоичного разложения векторов $a^{(i)}$ $(i = 1, 2, \dots)$ множества $N_0^{(i)}$ и $N_1^{(i)}$ будут найдены за полиномиальное при фиксированном $n$ время. Учитывая теперь, что общее число обращений к шагам 1, 2 алгоритма совпадает с количеством гипотез $a^{(i)}$, получаем, что вычислительная трудоемкость алгоритма $\mathscr{A}_1^+$ при фиксированном $n$ ограничена полиномом от $l$ и $\log\gamma$.

### 2.4.2. Расшифровка функций из класса $\mathfrak{T}(M)$

Нам осталось лишь избавиться от предположения, что $f \in \mathfrak{T}_+(M)$. Опишем алгоритм $\mathscr{A}_1$ расшифровки функции из класса $\mathfrak{T}(M)$. С помощью оракула найдем значение $f(x)$ во всех вершинах выпуклой оболочки множества $M$. Если найдется такое $\nu \in \{0, 1\}$, что для каждой вершины $f(x) = \nu$, то $f \equiv \nu$. В противном случае, выбрав какую-нибудь вершину $v$, в которой $f(v) = 0$, перенесем начало координат в точку $v$, т. е. осуществим преобразование $x' = x - v$. Тогда $M$ перейдет в некоторое множество $M'$, а функция $f$ перейдет в $f'$:

$$f' : M' \to \{0, 1\}.$$

Очевидно, что $f' \in \mathfrak{T}_+(M')$, поэтому для расшифровки $f'$ можно применить алгоритм $\mathscr{A}_1^+$. Из следствия 1.9 получаем, что после такого преобразования алгоритм остается полиномиальным при фиксированном $n$. Далее, на первой итерации шага 1 алгоритма $\mathscr{A}_1^+$ центром тяжести по-

литопа $W_0$ является точка $a^{(0)} = (0, \ldots, 0)$. Следовательно, $N_1^{(0)} = \varnothing$, а $N_0^{(0)}$ совпадает с множеством вершин выпуклой оболочки множества $M$. Таким образом, при $i = 0$ на шаге 2 алгоритма $\mathscr{A}_1^3$ нет необходимости обращаться к оракулу, т. к. во всех точках из $N_0^{(0)}$ значения функции $f$ уже известны. Следовательно, $\tau(\mathscr{A}_1) = \tau(\mathscr{A}_1^3)$. Доказана следующая

**Теорема 2.10.** *Существует алгоритм $\mathscr{A}_1$ расшифровки пороговой функции из класса $\mathfrak{T}(M)$ для которого при фиксированном $n$ величина $\rho(\mathscr{A}_1)$ ограничена полиномом от $l$ и $\log \gamma$, а*

$$\tau(\mathscr{A}_1) \leq 16n^{10n-1} l^{\left\lfloor \frac{n}{2} \right\rfloor} \log^n(\gamma + 1).$$

Таким образом, при фиксированном $n$

$$\tau(\mathscr{A}_1) = O\left(l^{\lfloor n/2 \rfloor} \log^n(\gamma + 1)\right).$$

Заметим, что в классе $\mathfrak{T}(E_k^n)$ алгоритм $\mathscr{A}_1$ использует $O(\log^n k)$ обращений к оракулу. На основе алгоритма $\mathscr{A}_1$ в разделе 3.9 будет построен алгоритм $\mathscr{A}_1^{\mathrm{o}}$, для которого при любом фикисрованном $n \geq 2$

$$\tau(\mathscr{A}_1^{\mathrm{o}}) = O(\log^{n-1} k).$$

В [139] предложен алгоритм $\mathscr{A}''$, который для произвольных $n \geq 2$, $k \geq 3$ расшифровывает любую функцию из класса $\mathfrak{T}(E_k^n)$, совершая при этом (при фиксированном $n$)

$$\tau(\mathscr{A}'') = O\left(\frac{\log^n k}{\log \log k}\right)$$

обращений к оракулу. Алгоритм $\mathscr{A}''$ опирается на результаты М. Ю. Мошкова в теории тестов [61, 62] (см. также [113, 139, 140]) и в отличие от алгоритмов $\mathscr{A}_1$ и $\mathscr{A}_1^{\mathrm{o}}$ не имеет полиномиально ограниченной (при фиксированном $n$) вычислительной трудоемкости. Таким образом, $\tau(\mathscr{A}'')$ ограничено сверху полиномом от $\log k$, а $\rho(\mathscr{A}'')$ — нет.

### 2.4.3. Модификация алгоритма

Используя [150], покажем, как нужно изменить алгоритм $\mathscr{A}_1^+$, чтобы вычислительная трудоемкость шага 1 (выдвинуть гипотезу) стала бы полиномиальной от $n$, $l$ и $\log\gamma$. Заметим, что общая вычислительная трудоемкость полученного такой заменой алгоритма $\mathscr{A}_1'$ останется экспоненциальной от $n$. Рассмотрим выпуклое тело $W \subseteq \mathbb{R}^n$ и обозначим через $r$ натуральное число, такое, что объем пересечения тела $W$ с шаром радиуса $r$, построенным вокруг начала координат, не меньше $r^{-n}$. В [81, 133] рассматривается следующая

**Задача отделения.** *Для заданного вектора* $v = (v_1, \ldots, v_n) \in \mathbb{Q}^n$ *определить, содержится ли* $v$ *в* $W$ *и, если не содержится, найти такой вектор* $z = (z_1, \ldots, z_n)$, *что* $\sum\limits_{j=1}^{n} z_j w_j < \sum\limits_{j=1}^{n} z_j v_j$ *для всех* $(w_1, \ldots, w_n) \in W$.

Алгоритм решения данной задачи назовем *оракулом отделения* для выпуклого тела $W$. Будем предполагать, что для любого $v \in \mathbb{Q}^n$ размер двоичной записи вектора $z$, выдаваемого оракулом, не выше некоторого полинома от $\langle v \rangle$, $\log r$ и $n$. Метод эллипсоидов [84, 85] можно адаптировать для поиска точки в выпуклом теле $W \subseteq \mathbb{R}^n$, заданном оракулом отделения. Справедлива

**Лемма 2.11.** [133] *В выпуклом теле* $K \subseteq \mathbb{R}^n$, *заданном оракулом отделения, задача нахождения внутренней точки может быть решена с полиномиальной от* $n$ *и* $\log r$ *вычислительной трудоемкостью за* $O(n^2 \log r)$ *обращений к оракулу отделения.*

Пусть $W'(f)$ — множество решений системы (2.5). Очевидно, $W'(f)$ — выпуклое тело, замыкание которого в $\mathbb{R}^n$ есть $W(f)$. Таким образом, $\operatorname{Vol} W'(f) = \operatorname{Vol} W(f)$ и, следовательно, $\operatorname{Vol} W'(f)$ удовлетворяет неравен-

ству (2.6). Так как

$$\log\chi(n,\gamma) = O\big(n^2\log(n\gamma)\big), \qquad \log\frac{1}{\operatorname{Vol} W'(f)} = O\big(n^3\log(n\gamma)\big) \qquad (n\to\infty),$$

то по лемме 2.7 для параметра $r$ тела $W'(f)$ справедливо соотношение $\log r = O\big(n^2\log(n\gamma)\big)$.

Покажем, как на основе оракула функции $f$ построить оракул отделения для тела $W'(f)$. Пусть $v = (v_1,\dots,v_n) \in \mathbb{Q}^n$ — вход задачи отделения. Алгоритмом из леммы 1.21 построим множества $N_0$ и $N_1$ крайних точек выпуклой оболочки множеств $M \cap \left\{(x_1,\dots,x_n) : \sum\limits_{j=1}^{n} x_j v_j \le 1\right\}$ и $M \cap \left\{(x_1,\dots,x_n) : \sum\limits_{j=1}^{n} x_j v_j > 1\right\}$ соответственно. С помощью оракула функции найдем значения $f$ в точках множеств $N_0$ и $N_1$. Если $f(x) = \nu$ для каждого $x \in N_\nu$ $(\nu = 0, 1)$, то, очевидно, $v \in W'(f)$, в противном случае найдется такое $z = (z_1,\dots,z_n) \in N_\nu$, что $f(z) = 1-\nu$. Если $f(z) = 0$, то $\sum\limits_{j=1}^{n} z_j w_j \le 1$ для любого $w \in W'(f)$, однако $z \in N_1$ и, следовательно, $\sum\limits_{j=1}^{n} z_j v_j > 1$. Если $f(z) = 1$, то $\sum\limits_{j=1}^{n} z_j w_j > 1$, $\sum\limits_{j=1}^{n} z_j v_j \le 1$. В первом случае решением задачи отделения является вектор $z$, а во втором — вектор $-z$. Таким образом, чтобы ответить на вопрос оракулу отделения тела $W'(f)$ (т. е. проверить гипотезу $v$) необходимо не более, чем $C_n l^{\lfloor n/2\rfloor}$ раз обратиться к оракулу функции $f$, где $C_n$ — некоторая зависящая только от $n$ величина. По лемме 1.12 $\langle z\rangle$ ограничено полиномом от $n$ и $\log\gamma$, следовательно, по лемме 2.11 за $O(n^4\log(n\gamma))$ гипотез (обращений к оракулу отделения) можно найти внутреннюю точку тела $W'(f)$, т. е. расшифровать функцию $f$. Очевидно, что вычислительная трудоемкость получения новой гипотезы полиномиальна от $n$ и $\log\gamma$. Для оракульной сложности всего алгоритма $\mathscr{A}_1'$ при фиксированном $n$ получаем: $\tau(\mathscr{A}_1') = O\big(l^{\lfloor\frac{n}{2}\rfloor}\log^n(\gamma+1)\big)$.

Другая модификация $\mathscr{A}_1^{\circ}$ алгоритма $\mathscr{A}_1$ описана в 3.9.

## 2.5. Расшифровка пороговых функций двух переменных

Здесь предлагается алгоритм $\mathscr{A}_2$ расшифровки в классе $\mathfrak{T}(E_k^2$, для которого $\rho(\mathscr{A}_2)$ ограничено полиномом от $\log k$, а

$$\tau(\mathscr{A}_2) \leq 6\log(k-1) + 4.$$

Заметим, что в [122] для решения этой задачи предлагается другой алгоритм с верхней оценкой оракульной сложности $6\log k + 33\log\log k - 26$.

**Лемма 2.12.** (Формула Г. А. Пика, см., например, [67, задача 24.7].) *Если внутри простого многоугольника с вершинами в точках решетки $\mathbb{Z}^2$ лежит $s$, а на границе — $p$ точек решетки, то площадь многоугольника равна $s + \frac{p}{2} - 1$.*

Рассмотрим определитель

$$\det(a, b) = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, \tag{2.13}$$

где $a = (a_1, a_2)$, $b = (b_1, b_2)$. Хорошо известно, что $|\det(a, b)|$ есть площадь параллелограмма, построенного на векторах $a$ и $b$, или удвоенная площадь треугольника, построенного на тех же векторах.

**Лемма 2.13.** *Пусть $\Phi = R_0R_1R_2R_3$ — выпуклый четырехугольник, $R_i \in \mathbb{Z}^2$ $(i = 0, \ldots, 3)$. Если треугольники $R_1R_2R_3$ и $R_0R_2R_3$ не содержат целочисленных точек, кроме своих вершин, тогда $\Phi$ является трапецией, причем стороны $R_0R_1$, $R_2R_3$ параллельны. Если, кроме того, длины сторон $R_0R_1$ и $R_2R_3$ совпадают, то $\Phi$, кроме вершин, не содержит ни одной целочисленной точки.*

*Доказательство.* Положим $a = R_1 - R_2$, $b = R_3 - R_2$, $c = R_0 - R_2$. Так как $\triangle R_1R_2R_3$ и $\triangle R_0R_2R_3$ не содержат внутренних целочисленных точек,

то по формуле Пика (лемма 2.12) имеем: $|\det(a,b)| = 1$ и $|\det(b,c)| = 1$. Таким образом, система векторов $\{a, b\}$ является базисом решетки $\mathbb{Z}^2$. Следовательно, найдутся такие целые $\alpha$ и $\beta$, что $c = \alpha a + \beta b$. Так как система $R_0, R_1, R_2, R_3$ выпукло независима, то $\alpha, \beta \in \mathbb{N}$. Используя свойства определителей, получаем $\det(b,c) = \det(b, \alpha a + \beta b) = \alpha \det(b,a) + \beta \det(b,b) = -\alpha \det(a,b)$. Следовательно, $\alpha = 1$. Таким образом, $c = a + \beta b$, $\beta \in \mathbb{N}$ и $R_0 - R_1 = c - a = \beta b = \beta(R_3 - R_2)$, т. е. четырехугольник Ф является трапецией.

Если длины сторон $R_0R_1$ и $R_2R_3$ совпадают, то Ф — параллелограмм и его площадь есть $|\det(a,b)| = 1$. Из формулы Пика теперь получаем, что Ф кроме вершин не содержит целочисленных точек. ∎

Пусть в параллелограмме Ф с целочисленными вершинами $R_0, R_1, R_2, R_3$ стороны $R_0R_1$ и $R_2R_3$ кроме концов не содержат других целочисленных точек:

$$\begin{gathered} R_i \in \mathbb{Z}^2 \quad (i = 0, \ldots, 3), \\ [R_0, R_1] \cap \mathbb{Z}^2 = \{R_0, R_1\}, \qquad [R_2, R_3] \cap \mathbb{Z}^2 = \{R_2, R_3\}. \end{gathered} \tag{2.14}$$

Назовем неравенство

$$\alpha_1 x_1 + \alpha_2 x_2 \leq \alpha_0 \tag{2.15}$$

*отсечением* вершины $R_i$ $(i = 0, \ldots, 3)$ параллелограмма Ф, если оно не выполняется для координат точки $R_i$. Будем говорить, что отсечение проходит через точку $(x_1, x_2)$, если $\alpha_1 x_1 + \alpha_2 x_2 = \alpha_0$. Отсечение (2.15) вершины $R_i$ называется *правильным*, если выполняются следующие условия:

1) неравенство (2.15) справедливо для всех целочисленных точек из Ф, кроме $R_i$;

2) отсечение (2.15) проходит через вершину $R'$, соседнюю с $R_i$ по ребру $R_0R_1$ или $R_2R_3$;

3) отсечение (2.15) проходит по крайней мере еще через одну точку из $\Phi \cap \mathbb{Z}^2$.

Для любой вершины параллелограмма $\Phi$, обладающего свойством (2.14), правильное отсечение всегда существует. Действительно, так как сторона $R_iR'$ кроме концов не содержит других целочисленных точек, то для $R_i$ существует отсечение, обладающее свойствами 1), 2). Кроме этого, в силу того, что в $\Phi$ найдется еще по крайней мере одна целочисленная точка, то существует правильное отсечение.

**Лемма 2.14.** *Существует полиномиальный от* $\log k$ *алгоритм* $\mathscr{A}_3'$*, который для любого параллелограмма* $\Phi = R_0R_1R_2R_3 \subseteq E_k^2$*, обладающего свойством 2.14 и заданного своими вершинами, строит правильное отсечение вершины* $R_0$.

*Доказательство.* Пусть $A \in \mathbb{Z}^{4\times 2}$, $a_0 \in \mathbb{Z}^4$, $Ax \leq a_0$ — система, описывающая $\Phi$. Предположим, что $B$ — квадратная подматрица матрицы $A$, а $b_0$ — столбец, составленный из соответствующих элементов столбца $a_0$, такие, что $\det B = \Delta \neq 0$, $Bx = b_0$, где $x$ — столбец, составленный из координат точки $R_0$. С помощью алгоритма из [101] с линейной от $\log \Delta$ трудоемкостью построим все крайние точки множества $\mathrm{Conv}\left((\Phi \setminus \{R_0\}) \cap \mathbb{Z}^2\right)$. В [101] показано, что число построенных крайних точек ограничено величиной $1 + \log(\Delta + 1)$. Сделав не более, чем $1 + \log(\Delta + 1)$ сравнений, легко найти правильное отсечение вершины $R_0$. Матрицу $B$, очевидно, можно составить так, чтобы ее коэффициенты не превосходили по модулю $k$, отсюда $\Delta \leq 2k^2$. Таким образом, вычислительная трудоемкость алгоритма $\mathscr{A}_3'$ ограничена сверху полиномом от $\log k$. ∎

**Лемма 2.15.** *Пусть параллелограмм* $\Phi = R_0R_1R_2R_3$ *обладает свойством* (2.14) *и кроме вершин содержит еще хотя бы одну целочисленную точ-*

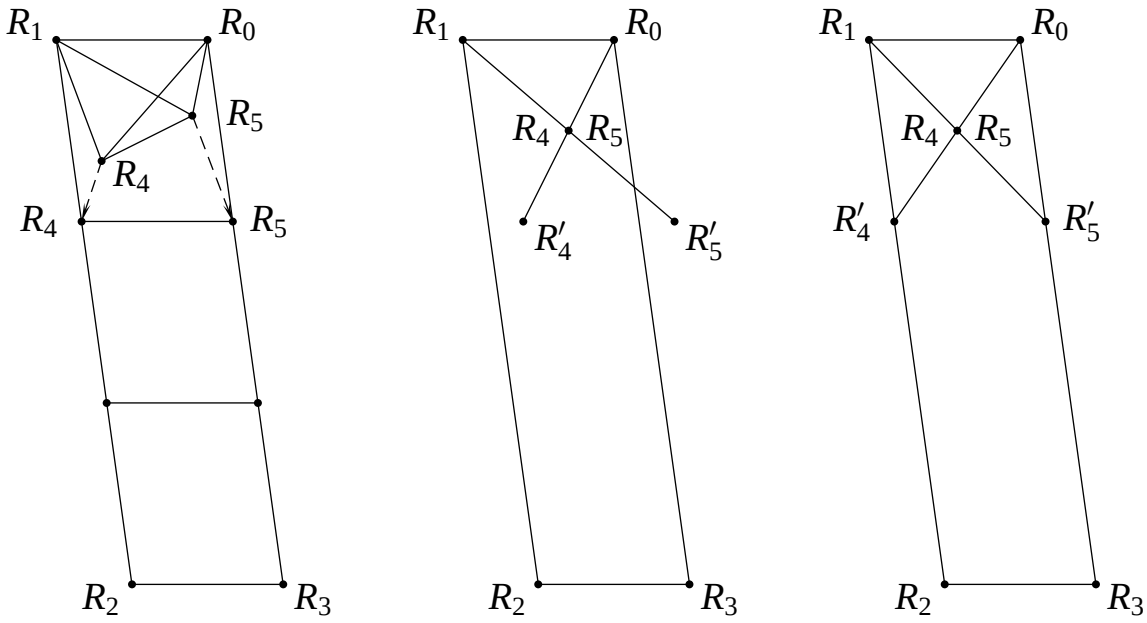


Рис. 2.1

*ку. Тогда либо правильное отсечение вершины* $R_0$*, либо правильное отсечение вершины* $R_1$ *проходит не менее чем через* 3 *точки множества* $\Phi \cap \mathbb{Z}^2$.

*Доказательство.* Обозначим через $R_4$ точку из $\Phi \cap \mathbb{Z}^2$, лежащую на правильном отсечении вершины $R_1$, ближайшую к $R_0$, а через $R_5$ — точку из $\Phi \cap \mathbb{Z}^2$, лежащую на правильном отсечении вершины $R_0$, ближайшую к $R_1$. Вначале предположим, что $R_4 \neq R_5$ (см. рис. 2.1 а). Так как $\triangle R_0R_1R_5$, $\triangle R_0R_1R_4$ не содержат внутренних целочисленных точек, то по лемме 2.13 $R_0R_1R_4R_5$ — параллелограмм, следовательно, точки $R_4$, $R_5$ лежат на отрезках $R_1R_2$, $R_0R_3$ и не являются внутренними точками параллелограмма Ф. Очевидно, в этом случае Ф не содержит ни одной внутренней целочисленной точки.

Пусть теперь $R_4 = R_5$ (см. рис. 2.1 б, в). Очевидно, что каждая из точек $R'_4 = 2R_4 - R_0$ и $R'_5 = 2R_5 - R_1$ имеет целочисленные координаты и по крайней мере одна из них в силу параллельности сторон $R_1R_2$, $R_0R_3$

принадлежит Ф. ∎

Обозначим через $\eta(\Phi)$ количество внутренних целочисленных точек параллелограмма Ф. Справедлива

**Лемма 2.16.** *Пусть параллелограмм* $\Phi = R_0R_1R_2R_3$ *обладает свойством* (2.14)*, тогда* $\eta(\Phi) \leq \mathrm{Area}(\Phi) - 1$.

*Доказательство.* Так как на границе параллелограмма Ф лежит не менее 4 целочисленных точек, то из формулы Пика (лемма 2.12) получаем: $\mathrm{Area}(\Phi) \geq \eta(\Phi) + 1$. ∎

**Теорема 2.17.** *Существует полиномиальный алгоритм* $\mathscr{A}_2$ *расшифровки функции из класса* $\bigcup\limits_{\substack{p\geq 2\\ q\geq 2}} \mathfrak{T}(E_p \times E_q)$*, для которого*

$$\tau(\mathscr{A}_2) \leq 6\log(k-1) + 4,$$

*где* $k = \max\{p, q\}$.

*Доказательство.* Вначале рассмотрим следующую вспомогательную процедуру. Предположим, что в концах отрезка $[u, v]$ $(u, v \in E_p \times E_q)$, содержащем $s$ внутренних целочисленных точек, значения функции $f$ уже известны и $f(u) \neq f(v)$.

Процедура дихотомического поиска, находящая две соседние целочисленные точки отрезка $[u, v]$, в которых функция $f$ принимает различные значения, заключается в следующем: положим $w := u + \lfloor \varsigma/2 \rfloor \cdot \dfrac{v-u}{\varsigma}$, где $\varsigma$ — НОД компонент вектора $v - u$, и обратимся к оракулу в точке $w$; если $f(u) = f(w)$, то $u := w$, иначе $v := w$; если $u, v$ не являются соседними целочисленными точками, то найдем новое $w$ и т. д.

Очевидно, что описанная процедура завершается не более, чем за $\lceil \log(s+1) \rceil$ обращений к оракулу функции $f$. Заметим, что если $i \in \mathbb{N}$,

$2^i \le s < 2^{i+1}$, то $i \le \log s < i+1$ и $i < \log(s+1) \le i+1$. Отсюда при $s \in \mathbb{N}$ получаем: $\lceil \log(s+1) \rceil = \lfloor \log s \rfloor + 1$.

Перейдем теперь к пошаговому описанию алгоритма $\mathscr{A}_2$ расшифровки функций из класса $\mathfrak{T}(E_p \times E_q)$.

Шаг 0. Определим $f(x)$ в вершинах прямоугольника $E_p \times E_q$ и обозначим через $S_\nu$ $(\nu = 0, 1)$ множество тех из них, для которых $f(x) = \nu$. Если при $\nu = 0$ или при $\nu = 1$ множество $S_\nu$ пусто, то расшифровка закончена, так как в этом случае $M_\nu(f) = \varnothing$ и $f \equiv 1 - \nu$.

Шаг 1. Пусть $L_i$ $(i = 0, 1)$ — сторона прямоугольника $E_p \times E_q$, в концах которой функция $f$ принимает различные значения. Дихотомией на каждой из сторон $L_0$, $L_1$ найдем пару соседних целочисленных точек $R_0$, $R_1$ и $R_2$, $R_3$ соответственно, так, чтобы $f(R_0) = f(R_3) = \nu$, $f(R_1) = f(R_2) = 1 - \nu$ $(\nu = 0, 1)$. Присоединим $R_0$, $R_3$ к $S_\nu$, а $R_1$, $R_2$ к $S_{1-\nu}$. Для целочисленных точек из $\operatorname{Conv} S_\nu$ $(\nu = 0, 1)$ имеем $f(x) = \nu$. Если $L_0$ и $L_1$ — противоположные стороны прямоугольника $E_p \times E_q$, то $R_0 - R_1 = R_3 - R_2$, следовательно, $R_0R_1R_2R_3$ — параллелограмм. В противном случае, когда $L_0$, $L_1$ — смежные, обозначим через $R_6$ их общую вершину и рассмотрим ту пару точек $R_{2i}$, $R_{2i+1}$, которая расположена дальше от $R_6$. Пусть $j \in \{1, 2\}$ и $\nu \in \{0, 1\}$ выбраны так, что $R_{2i}$, $R_{2i+1}$ являются соседями по координате $j$ и $R_{2i+\nu}$ расположена дальше от $R_6$, чем $R_{2i+1-\nu}$. Заменим $R_{2i+\nu}$ точкой $R'_{2i+\nu}$, соседней с $R_{2i+1-\nu}$ по координате $3 - j$. Очевидно, что $f(R'_{2i+\nu}) = f(R'_{2i+\nu})$ и $R_0 - R_1 = R_3 - R_2$. Положим $\mu := 1$, $R_{2i+\nu} := R'_{2i+\nu}$. Возможен случай, когда до замены обе пары $R_0$, $R_1$ и $R_2$, $R_3$ были равноудалены от $R_6$, тогда, очевидно, $\Phi = R_0R_1R_2R_3$ не содержит внутренних

целочисленных точек и $M_\nu(f) = \operatorname{Conv} S_\nu \cap (E_p \times E_q)$ $(\nu = 0, 1)$ — расшифровка завершена.

Шаг 2. Алгоритмом $\mathscr{A}_3'$ построим правильные отсечения вершин $R_0$ и $R_1$ и выберем из них отсечение, проходящее через бóльшее число точек из $\Phi \cap (E_p \times E_q)$, где $\Phi = R_0R_1R_2R_3$. Пусть $i$ — номер соответствующей выбранному отсечению вершины, а $s_\mu$ — число лежащих на нем целочисленных внутренних точек области $\Phi$. Если $s_\mu = 0$, то по лемме 2.15 фигура $\Phi$ вообще не содержит внутренних целочисленных точек, $M_\nu(f) = \operatorname{Conv} S_\nu \cap (E_p \times E_q)$ $(\nu = 0, 1)$ — расшифровка завершена. В противном случае дихотомией найдем две соседние целочисленные точки $R_0'$, $R_1'$, лежащие на построенном отсечении, такие, что $f(R_0') \neq f(R_1')$. Аналогичную процедуру проведем с отсечением вершины $R_{3-i}$: дихотомией найдем лежащие на этом отсечении соседние целочисленные точки $R_2'$, $R_3'$, такие, что $f(R_0') = f(R_3')$, $f(R_1') = f(R_2')$ (см. рис 2.2).

Шаг 3. Для всех $i \in \{0, \ldots, 3\}$ положим $R_i := R_i'$. Добавим $R_0$ и $R_3$ к $S_\nu$, а $R_1$ и $R_2$ к $S_{1-\nu}$, где $\nu = f(R_0)$. Увеличим $\mu$ на 1 и перейдем на шаг 2.

Очевидно, что за конечное число шагов алгоритм $\mathscr{A}_2$ остановится, при этом $M_\nu(f) = \operatorname{Conv} S_\nu \cap \mathbb{Z}^2$ — функция $f$ расшифрована. Сами коэффициенты порогового неравенства можно вычислить алгоритмом, подобным процедуре из теоремы 2.5.

Оценим оракульную сложность алгоритма $\mathscr{A}_2$.

Шаг 0 требует 4 обращения к оракулу.

Дихотомический поиск на шаге 1 использует не более $2\lfloor \log(k-2) \rfloor + 2$ обращений к оракулу.

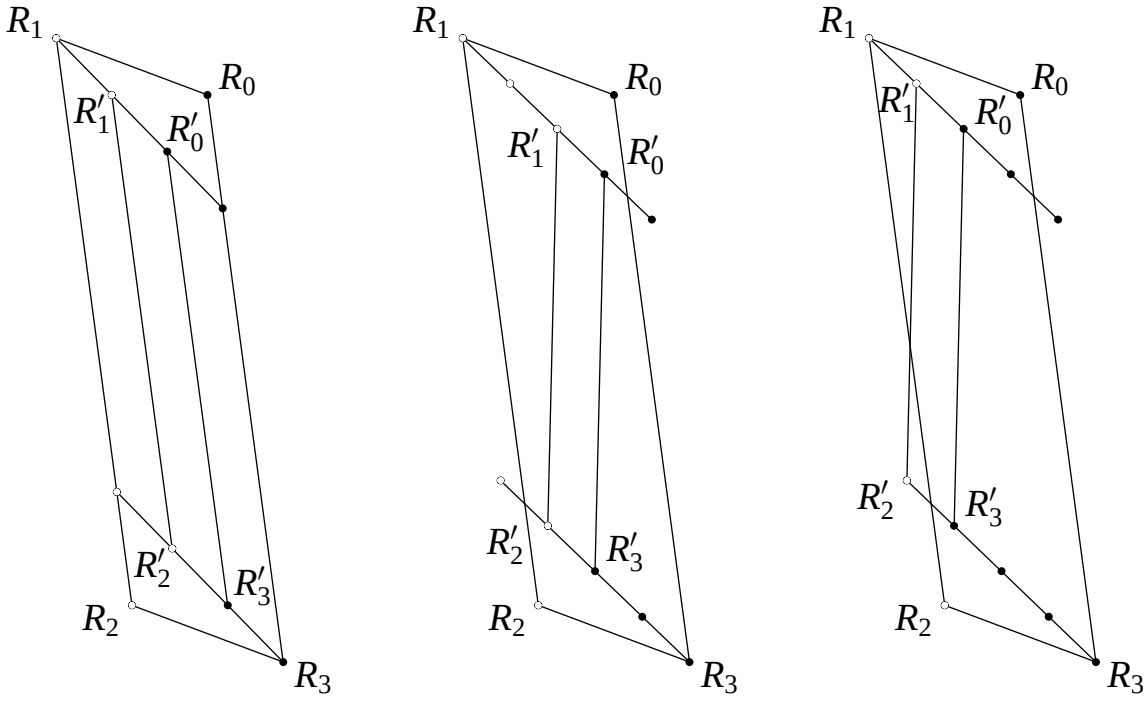


Рис. 2.2

Количество обращений на шаге 2 алгоритма не превосходит величины $2\lceil\log(s_\mu + 1)\rceil$ $(\mu = 1, \ldots, p)$, где $p$ — число итераций шага 2.

Оценим $p$. Из леммы 2.15 следует, что на каждой итерации шага 2 алгоритма $\mathscr{A}_3$ выполняется неравенство $\operatorname{Area} R'_0R'_1R'_2R'_3 < \frac{1}{2} \operatorname{Area} R_0R_1R_2R_3$, таким образом, площадь области Ф уменьшается более, чем в 2 раза. Так как при первом обращении к шагу 2 алгоритма $\operatorname{Area}(\Phi) \leq k - 1$, то из леммы 2.16 получаем: $p \leq \lfloor\log(k-1)\rfloor$. Кроме того, на шаге 2 в силу свойств правильных отсечений имеем

$$s_1 \leq k - 2, \qquad s_\mu \leq \frac{k-2}{s_1 \cdot \ldots \cdot s_{\mu-1}} \qquad (\mu = 2, \ldots, p).$$

Таким образом, при $k \geq 3$ общее число обращений к оракулу на всех итерациях шага 2 не превосходит величины

$$2\sum_{\mu=1}^{p-1}\lceil\log(s_\mu+1)\rceil = 2(p-1) + 2\sum_{\mu=1}^{p-1}\lfloor\log s_\mu\rfloor \leq 2(p-1) + 2\log\prod_{\mu=1}^{p-1} s_\mu \leq$$

$$\leq 2(p-1) + 2\log(k-2) \leq 4\log(k-1) - 2.$$

Складывая оценки на количество обращений к оракулу на шагах 0, 1, 2, получаем:

$$\tau(\mathscr{A}_2) \leq 4 + 2\log(k-2) + 4\log(k-1) - 2 \leq 6\log(k-1) + 4.$$

Учитывая полиномиальность всех используемых в алгоритме $\mathscr{A}_2$ вспомогательных процедур, получаем, что $\rho(\mathscr{A}_2)$ ограничено некоторым полиномом от $\log k$. ∎

Связь задачи расшифровки пороговой функции двух переменных с задачей нахождения диофантового приближения установлена в главе 4.

## 2.6. Расшифровка пороговых функций, заданных расширенным оракулом

В настоящем разделе мы исследуем задачу расшифровки пороговой функции, заданной более информативным — «*расширенным*» — оракулом, который в отличие от «обычного» оракула принимает на вход произвольные точки из $\mathbb{Q}^n$, а не только из $M$. Расширенный оракул связан с конкретным пороговым неравенством (1.2) функции $f$. По заданной точке $x \in \mathbb{Q}^n$ он возвращает 0, если неравенство (1.2) выполнено, и 1 в противном случае (если ясно, о каком пороговом неравенстве идет речь, будем писать тогда $f(x) = 0$ и $f(x) = 1$ соответственно). Под *расшифровкой пороговой функции* $f$, *заданной с помощью расширенного оракула*, будем понимать процедуру восстановления коэффициентов ее любого возможного порогового неравенства с помощью обращений к этому оракулу.

Ниже будет описан алгоритм $\mathscr{A}_{\text{ext}}$ расшифровки пороговой функции $k$-значной логики,зависящей от $n$ переменных, заданной с помощью

расширенного оракула. При фиксированном $n$ алгоритм имеет полиномиальную от $\log k$ вычислительную трудоемкость и использует асимптотически не более $\frac{n^4}{2}\log(n+1) + 2n^3 \log k$ обращений к оракулу.

Обозначим

$$\Xi = \frac{(n+1)^{\frac{n}{2}+1}}{2^n}(k-1)^n. \tag{2.16}$$

Обозначим через $e_j$ вектор в $\mathbb{R}^n$, все компоненты которого равны 0, кроме $j$-й, равной 1.

Пусть $\mathfrak{T}_+(E_k^n)$ — множество тех функций из $\mathfrak{T}(E_k^n)$, для каждой из которых $f(0) = 0$. Из леммы 1.11 легко получается

**Лемма 2.18.** *Для любой функции $f \in \mathfrak{T}_+(E_k^n)$ найдется пороговое неравенство* (1.2)*, в котором $a_0, a_1, \ldots, a_n$ — целые, причем $a_0 > 0$ и*

$$\begin{aligned} a_j > 0, &\text{ если } f(-\Xi e_j) < f(-\Xi e_j);\\ a_j = 0, &\text{ если } f(-\Xi e_j) = f(-\Xi e_j);\\ a_j < 0, &\text{ если } f(-\Xi e_j) > f(-\Xi e_j). \end{aligned}$$

**Лемма 2.19.** *Пусть $y^{(j)} = \beta_j e_j \in \mathbb{R}^n$, $z^{(j)} = \gamma_j e_j \in \mathbb{R}^n$ $(j = 1, 2, \ldots, n)$, причем $\gamma_j > 0$, $\beta_j > 0$, $0 \le \gamma_j - \beta_j \le \varepsilon$, где*

$$\varepsilon = \frac{2^{n-1}}{(k-1)^{n-1}(n+1)^{\frac{n+1}{2}}}. \tag{2.17}$$

*Тогда множество $D = E_k^n \cap \operatorname{Conv}\left\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}, z^{(1)}, z^{(2)}, \ldots, z^{(n)}\right\}$ либо пусто, либо найдется гиперплоскость, на которой располагаются все точки из $D$.*

*Доказательство.* Если $\operatorname{Affdim} D < n$, то утверждение леммы очевидно. В противном случае в $D$ найдется аффинно независимая система точек $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$. Коэффициенты гиперплоскости $\sum\limits_{j=1}^{n} a_j x_j = a_0$, проходящей через эти точки, определяются единственным образом с точностью до постоянного множителя. Их можно выбрать так, что $a_j$ с точностью

до знака равно минору, полученному вычеркиванием $j$-го столбца из матрицы, составленной из компонент точек $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$ и дополненной столбцом из единиц. Пользуясь оценкой определителя с неотрицательными элементами (см., например, [60]), получаем

$$a_0 \le \frac{(k-1)^n (n+1)^{(n+1)/2}}{2^n},$$

$$a_j \le \frac{(k-1)^{n-1} (n+1)^{(n+1)/2}}{2^n} = \frac{1}{2\varepsilon} \qquad (j = 1, 2, \ldots, n).$$

Так как $a_j \in \mathbb{Z}$ по построению, то область $R$, заданная неравенствами $a_0 - 1 \le \sum\limits_{j=1}^{n} a_j x_j \le a_0 + 1$, не содержит других точек из $E_k^n$, кроме точек, лежащих на гиперплоскости $a_0 - 1 \le \sum\limits_{j=1}^{n} a_j x_j \le a_0 + 1$.

Покажем, что $D \subset R$. Для всякого $j = 1, 2, \ldots, n$ рассмотрим точки

$$v^{(j)} = \frac{a_0}{a_j} \cdot e_j, \qquad u^{(j)} = \frac{a_0 - 1}{a_j} \cdot e_j, \qquad w^{(j)} = \frac{a_0 + 1}{a_j} \cdots e_j.$$

Точка $v^{(j)}$, очевидно, принадлежит гиперплоскости $\sum\limits_{j=1}^{n} a_j x_j = a_0$ и отрезку $[y^{(j)}, z^{(j)}]$. Точки $y^{(j)}, z^{(j)}, v^{(j)}$ принадлежат отрезку $[u^{(j)}, w^{(j)}]$. Так как длина отрезка $[y^{(j)}, z^{(j)}]$ не превосходит $\varepsilon$, а длина отрезка $[u^{(j)}, w^{(j)}]$ равна $2/a_j \ge 4\varepsilon > 2\varepsilon$, то делаем вывод, что $y^{(j)}$ и $z^{(j)}$ принадлежат $R$ для каждого $j = 1, 2, \ldots, n$, откуда $D \subset R$. ∎

**Теорема 2.20.** *Существует алгоритм $\mathscr{A}_{\text{ext}}$ расшифровки функции $f \in \mathfrak{T}(E_k^n)$, заданной расширенным оракулом. При любом фиксированном $n$ алгоритм $\mathscr{A}_{\text{ext}}$ является полиномиальным от $\log k$ и использует*

$$\tau(\mathscr{A}_{\text{ext}}) \le \frac{(6n^2 + n + 11)(n+1)n}{12} \log(n+1) + n^2(2n-1) \log k$$

*обращений к расширенному оракулу функции $f$.*

*Доказательство.* Опишем алгоритм $\mathscr{A}_{\text{ext}}$ расшифровки функции $f \in \mathfrak{T}(E_k^n)$, заданной расширенным оракулом.

Шаг 1. Обращаемся к оракулу в точке 0. Если $f(0) = 0$, то $f \in \mathfrak{T}_+(E_k^n)$. Далее будем считать, что это условие выполнено, так как в противном случае функцию $f$ можно заменить на $1 - f \in \mathfrak{T}_+(E_k^n)$.

Шаг 2. С помощью $2n$ обращений к оракулу найдем значения функции $f$ в точках $\pm\Xi e_j$ ($j = 1, 2, \ldots, n$), где $\Xi$ определяется формулой (2.16). Если $f(\Xi e_j) = f(-\Xi e_j)$ для некоторого $j$, то ввиду леммы 2.18 найдется пороговое неравенство функции $f$, в котором $a_j = 0$, т. е. переменная $x_j$ является несущественной и задача расшифровки сводится к задаче меньшей размерности. Для всякого $j$, такого, что $f(-\Xi e_j) > f(\Xi e_j)$, выполним замену переменных $x_j \mapsto k - 1 - x_j$, тем самым сводя задачу к расшифровке пороговой функции, в которой для любого ее порогового неравенства выполнено

$$a_j > 0 \qquad (j = 0, 1, \ldots, n), \tag{2.18}$$

т. е. такой монотонной пороговой функции, в которой все переменные существенные. Далее будем предполагать, что свойство (2.18) выполнено.

Шаг 3. Для каждого $j = 1, 2, \ldots, n$ с помощью дихотомии на отрезке $[0, \Xi e_j]$ находим такие $y^{(j)}$, $z^{(j)}$, для которых $|y^{(j)} - z^{(j)}| \leq \varepsilon$, где $\varepsilon$ определяется формулой (2.17). Согласно лемме 2.19, в результате получим многогранную область $P$, такую, что $D = P \cap E_k^n$ либо пусто, либо найдется гиперплоскость, на которой располагаются все точки из $D$. Определить, какой случай имеет место, и (если $D \neq \varnothing$) построить эту гиперплоскость можно с помощью полиномиального при фиксированном $n$ алгоритма построения вершин выпуклой оболочки целочисленных решений заданной системы линейных неравенств (см. [105, теорема 5.7, С. 111]).

Если $D = \varnothing$, то процедура расшифровки закончена. Действительно, если $K_0, K_1$ — множества точек, в которых в ходе работы алгоритма происходило обращение к оракулу и в которых значение $f$ равно 0 и 1 соответственно, то, легко видеть, что $M_0(f) = \operatorname{Conv} K_0 \cap E_k^n$, $M_1(f) = K_1 \cap E_k^n$.

Если $D \neq \varnothing$, то задача сводится к расшифровке функции из класса $\mathfrak{T}(E_{k'}^{n-1})$, где $k' \leq k\sqrt{n}$.

На шагах 1 и 2 алгоритма $\mathscr{A}_{\text{ext}}$ происходит $2n + 1$ обращений к оракулу. Процедура дихотомии на шаге 3 для каждого $j = 1, 2, \ldots, n$ использует

$$\left\lceil \log \frac{\Xi}{\varepsilon} \right\rceil = \left\lceil \log \frac{(n+1)^{n+3/2}}{2^{2n-1}} (k-1)^{2n-1} \right\rceil$$

обращений к оракулу. Обозначая через $\eta(n, k)$ максимально возможное число обращений к оракулу при расшифровке функции из класса $\mathfrak{T}(E_k^n)$, получаем

$$\eta(n,k) \leq 2n+1+$$
$$\left( \left( n + \frac{3}{2} \right) \log(n+1) - 2n + 2 + (2n-1)\log(k-1) \right) + \eta(n-1, k\sqrt{n}),$$

откуда

$$\eta(n,k) \leq \sum_{m=1}^{n} \left( m \left( m + \frac{3}{2} \right) \log(m+1) - m(2m-1) \right) +$$
$$+ n(2n-1) \left( n \log k + \sum_{m=1}^{n} \frac{m}{2} \log n \right).$$

После преобразований имеем

$$\eta(n,k) \leq \frac{(6n^2+n+11)(n+1)n}{12} \log(n+1) - \frac{(4n-1)(n+1)n}{6} + n^2(2n-1)\log k,$$

откуда получаем требуемое.

Так как все вспомогательные процедуры на каждом шаге алгоритма можно выполнить за время, полиномиальное от $\log k$ (при фиксированном $n$), то вычислительная трудоемкость алгоритма при фиксированном $n$ также ограничена некоторым полиномом от $\log k$. ∎

# Глава 3

# Нижние оценки сложности расшифровки пороговых функций

## 3.1. Введение

В данной главе устанавливаются нижние оценки сложности расшифровки пороговых функций. Под *сложностью расшифровки* в некотором классе $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ понимается величина

$$\tau(\mathfrak{F}') = \min_{\mathscr{A}} \tau(\mathscr{A}) = \min_{\mathscr{A}} \max_{f \in \mathfrak{F}'} \tau(\mathscr{A}, f),$$

где минимум берется по всем алгоритмам $\mathscr{A}$ расшифровки в классе $\mathfrak{F}'$. Другими словами, сложность расшифровки — это сложность наилучшего (по числу обращений к оракулу) алгоритма расшифровки в данном классе.

Следуя [47–49, 51], множество $T \subseteq M$ назовем *разрешающим* для $f$ относительно класса $\mathfrak{F}'$, если для любой функции $g \in \mathfrak{F}' \setminus \{f\}$, найдется по крайней мере одна точка $z \in T$, такая, что $g(z) \neq f(z)$. Разрешающее множество, никакое собственное подмножество которого не является разрешающим для $f$, называется *минимальным* или *тупиковым*. Разрешающее множество минимальной мощности назовем *наименьшим*. Его мощность обозначим через $\sigma(\mathfrak{F}', f)$. Заметим, что

$$\sigma(\mathfrak{F}', f) = \min_{\mathscr{A}} \tau(\mathscr{A}, f), \tag{3.1}$$

где минимум берется по всем алгоритмам $\mathscr{A}$ расшифровки в классе $\mathfrak{F}'$. Очевидно, наименьшее разрешающее множество является минимальным. *Длиной обучения* (teaching dimension [132]) в классе $\mathfrak{F}'$ назовем

величину

$$\sigma(\mathfrak{F}') = \max_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f) = \max_{f \in \mathfrak{F}'} \min_{\mathscr{A}} \tau(\mathscr{A}, f).$$

*Средней мощностью минимального разрешающего множества* в классе $\mathfrak{F}'$ называется

$$\overline{\sigma}(\mathfrak{F}') = \frac{1}{|\mathfrak{F}'|} \sum_{f \in \mathfrak{F}'} \sigma(\mathfrak{F}', f).$$

Точка $z \in M$ называется *существенной* для функции $f \in \mathfrak{F}'$ относительно класса $\mathfrak{F}'$, если существует функция $g \in \mathfrak{F}' \setminus \{f\}$, такая, что $f(z) \neq g(z)$ и $f(x) = g(x)$ для всех $x \in M \setminus \{z\}$. Очевидно, что любая существенная точка функции $f$ принадлежит каждому разрешающему множеству этой функции.

В [2, 51] исследуется задача расшифровки в классах монотонных булевых и монотонных многозначных функций. Там показано, что в этих случаях минимальным разрешающим множеством является множество верхних нулей и нижних единиц функции, т. е. в точности множество всех существенных точек.

Очевидно, что для расшифровки функции $f$ в классе $\mathfrak{F}'$ необходимо обратиться к оракулу в точках некоторого разрешающего множества; заметим, что это утверждение равносильно (3.1). Отсюда сразу получаем

**Утверждение 3.1.** *Для любого класса* $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ *справедливо неравенство* $\tau(\mathfrak{F}') \geq \sigma(\mathfrak{F}')$.

**Утверждение 3.2.** *Для любых* $M$ *и* $\mathfrak{F}' \subseteq \mathfrak{F}(M)$ *справедливо неравенство* $\tau(\mathfrak{F}') \geq \log |\mathfrak{F}'|$.

*Доказательство. Деревом решений* $T$ для класса $\mathfrak{F}'$ называется корневое бинарное дерево со следующими свойствами:

- каждая неконцевая вершина помечена некоторой точкой $x \in M$ (и представляет собой обращение к оракулу в точке $x$);

- из каждой неконцевой вершины выходит 2 ребра, помеченных числами $0, 1$ (ребра соответствуют возможным ответам оракула);

- каждый лист помечен конкретной функцией $f \in \mathfrak{F}'$, таким образом, что каждая функция встречается в этих пометках ровно один раз и все пометки вдоль простого пути из корня в лист согласованы с пометкой данного листа (последнее означает, что для любой внутренней вершины $v$, любого выходящего из него ребра $r$ и любого листа $w$, в который из $v$ через $r$ ведет простой путь, выполняется равенство $f(x) = \nu$, где $f$, $x$ и $\nu$ — метки вершин $w, v$ и ребра $r$ соответственно).

Таким образом, на дерево решений $T$ для класса $\mathfrak{F}'$ можно смотреть как на способ описания некоторого алгоритма $\mathscr{A}$ расшифровки в классе $\mathfrak{F}'$. Очевидно, что $\tau(\mathscr{A})$ совпадает с высотой дерева (количеством ребер в самом длинном простом пути из корня в лист), а $|\mathfrak{F}'|$ — с числом листьев дерева $T$. Воспользовавшись известной нижней оценкой высоты бинарного дерева, получаем: $\tau(\mathscr{A}) \geq \log|\mathfrak{F}'|$ для любого алгоритма $\mathscr{A}$ расшифровки в классе $\mathfrak{F}'$. ∎

Для класса пороговых функций $\mathfrak{T}(M)$ будем использовать следующие сокращенные обозначения:

$$\tau(M) = \tau\big(\mathfrak{T}(M)\big), \qquad \sigma(f) = \sigma\big(\mathfrak{T}(M),\ f\big),$$

$$\sigma(M) = \sigma\big(\mathfrak{T}(M)\big), \qquad \overline{\sigma}(M) = \overline{\sigma}\big(\mathfrak{T}(M)\big).$$

В разделе 3.2 получены некоторые вспомогательные результаты. На основе анализа структуры разрешающего множества пороговой функции, проведенного в разделе 3.3, в разделе 3.4 получены верхние и

нижние оценки длины обучения, в частности, показано, что при фиксированном $n$

$$\tau(E_k^n) \geq \sigma(E_k^n) = \Omega(\log^{n-2} k).$$

Другая характеризация минимального разрешающего множества пороговой функции приведена в разделе 3.5. На основе этих результатов в разделе 3.6 построена неулучшаемая (с точностью до порядка при фиксированном $n$) верхняя оценка мощности минимального разрешающего множества для одного подкласса пороговых функций. В разделе 3.7 получена верхняя оценка для числа неприводимых точек политопа. Неулучшаемая (с точностью до порядка при фиксированном $n$) верхняя оценка длины обучения в классе пороговых функций выводится в разделе 3.8, а именно, установлено, что

$$\sigma(E_k^n) = O(\log^{n-2} k).$$

В 3.9 предлагается процедура нахождения минимального разрешающего множества пороговой функции по известным коэффициентам порогового неравенства; на ее основе улучшается алгоритм расшифровки $\mathscr{A}_1$. Оркульная сложность нового алгоритма $\mathscr{A}_1^{\circ}$ отличается от сложности оптимального алгоритма расшифровки не более, чем в $O\left(n^3 \log(n\gamma)\right)$ раз. Для класса $\mathfrak{T}(E_k^n)$ сложность алгоритма $\mathscr{A}_1^{\circ}$ отличается от сложности оптимального алгоритма не более, чем в $O\left(n^2 \log(nk)\right)$ раз. При фиксированном $n$

$$\tau(E_k^n) \leq \tau(\mathscr{A}_1^{\circ}) = O(\log^{n-1} k).$$

В разделе 3.10 рассматривается случай пороговых функций двух переменных. В частности, для длины обучения в классе $\mathfrak{T}(E_k^2)$ установлено точное значение

$$\sigma(E_k^2) = 4$$

и получена асимптотика среднего значения мощности минимального разрещающего множества:

$$\overline{\sigma}(E_k^2) = \frac{7}{2} + O\left(\frac{1}{k}\right).$$

Пороговые булевы функции рассматриваются в разделе 3.11. В разделе 3.12 полученные результаты о верхних и нижних оценках сложности расшифровки применяются к анализу оракульной сложности задачи о рюкзаке.

Результаты разделов 3.2–3.4 опубликованы в работах [28, 36, 109, 161]; разделов 3.5, 3.6 — в [32]; разделов 3.7, 3.8 — в [33]; раздела 3.9 — в [24]; раздела 3.10 — в [26]; раздела 3.11 — в [109]; раздела 3.12 — в [27].

## 3.2. Свойства конуса разделяющих функционалов

Вернемся к изучению свойств конуса $K(f)$, описываемого системой линейных неравенств (1.6). Полиэдральный (многогранный) конус $K$ называется *телесным*, если его размерность совпадает с размерностью пространства.

**Лемма 3.3.** *Для любой* $f \in \mathfrak{T}(M)$ *конус* $K(f)$ *— телесный.*

*Доказательство.* Предположим вначале, что для $f \in \mathfrak{T}(M)$ существует пороговое неравенство (1.2) с коэффициентом $a_0 > 0$. Множество всех таких функций обозначим $\mathfrak{T}_+(M)$. Пусть $a_0, \ldots, a_n$ — коэффициенты порогового неравенства (1.2), существование которых утверждается в следствии 1.9, причем $a_0 > 0$. Положим $w = (w_1, \ldots, w_n)$, где $w_j = 2a_j/(2a_0 + 1)$ $(j = 1, \ldots, n)$. В лемме 2.6 показано, что для любого $(x_1, \ldots, x_n) \in M_0(f)$ выполняется неравенство $\sum\limits_{j=1}^{n} w_j x_j < 1$, а для

любого $(x_1, \ldots, x_n) \in M_1(f)$ — неравенство $\sum_{j=1}^{n} w_j x_j > 1$. Отсюда получаем, что для каждой $f \in \mathfrak{T}_+(M)$ найдется такое $w_{n+1} > 0$, что $\sum_{j=1}^{n} w_j x_j > 1 + w_{n+1}$ для всех $(x_1, \ldots, x_n) \in M_1(f)$. Мы доказали существование вектора $(1, w_1, \ldots, w_{n+1})$, строго удовлетворяющего всем неравенствам системы (1.6). Таким образом, $\operatorname{Affdim} K(f) = n + 2$ для любой $f \in \mathfrak{T}_+(M)$.

Предположим теперь, что для $f \in \mathfrak{T}(M)$ существует пороговое неравенство (1.2) с коэффициентом $a_0 < 0$. Не нарушая общности, можно считать, что $a_j \in \mathbb{Q}$ $(j = 0, 1, \ldots, n)$. Домножив коэффициенты $a_j$ на наименьшее общее кратное их знаменателей, получим пороговое неравенство с целыми коэффициентами и $a_0 \leq -1$. Положим $w = (w_1, \ldots, w_n)$, где $w_j = -2a_j/(2a_0 + 1)$ $(j = 1, \ldots, n)$. Заметим, что $2a_0 + 1 \leq -1$ и поэтому $\sum_{j=1}^{n} w_j x_j = -\sum_{j=1}^{n} \frac{2a_j}{2a_0+1} x_j = -\frac{2}{2a_0+1} \sum_{j=1}^{n} a_j x_j \leq -\frac{2a_0}{2a_0+1} < -1$ для любого $(x_1, \ldots x_n) \in M_0(f)$. Так как для любого $(x_1, \ldots x_n) \in M_1(f)$ $\sum_{j=1}^{n} a_j x_j \geq a_0 + 1$, то $\sum_{j=1}^{n} w_j x_j = -\sum_{j=1}^{n} \frac{2a_j}{2a_0+1} x_j \geq -\frac{2(a_0+1)}{2a_0+1} > -1$. Снова получаем, что $\operatorname{Affdim} K(f) = n + 2$.

Осталось предположить, что для функции $f \in \mathfrak{T}(M)$ во всех возможных пороговых неравенствах $a_0 = 0$. По лемме 1.9, не нарушая общности, можно считать, что $a_j \in \mathbb{Z}$ $(j = 1, \ldots, n)$. Тогда для любого $(x_1, \ldots, x_n) \in M_0(f)$ выполняется неравенство $\sum_{j=1}^{n} a_j x_j \leq 0$ и для любого $(x_1, \ldots, x_n) \in M_1(f)$ — неравенство $\sum_{j=1}^{n} a_j x_j \geq 1$. Очевидно, что неравенство $\sum_{j=1}^{n} a_j x_j \leq \frac{1}{2}$ является пороговым для функции $f$, так как выполняется для всех $(x_1, \ldots, x_n) \in M_0(f)$ и не выполняется ни для какого $(x_1, \ldots, x_n) \in M_1(f)$. Полученное противоречие завершает доказательство леммы. ∎

Полиэдральный конус $K \subseteq \mathbb{R}^n$ называется *острым*, если он не содержит ненулевых подпространств.

**Лемма 3.4.** *Если* $\operatorname{Affdim} M = n$, *то для любой функции* $f \in \mathfrak{T}(M)$ *конус* $K(f)$ *— острый.*

*Доказательство.* Покажем, что если $a = (a_0, a_1, \ldots, a_n, a_{n+1}) \in K(f)$ и $-a \in K(f)$, то $a = 0$. Из рассмотрения системы (1.6) получаем, что в этом случае $a_{n+1} = 0$, и, следовательно, $M \subseteq \left\{ x = (x_1, x_2, \ldots, x_n) : \sum\limits_{i=1}^{n} a_i x_i = a_0 \right\}$. Так как $\operatorname{Affdim} M = n$, то среди $a_i$ $(i = 0, \ldots, n)$ нет ненулевых чисел. ∎

Используя леммы 3.3 и 3.4, из теории линейных неравенств получаем следующий результат.

**Лемма 3.5.** *Пусть* $\operatorname{Affdim} M = n$, *тогда для любой* $f \in \mathfrak{T}(M)$ *справедливы следующие утверждения:*

1) *конус* $K(f)$ *имеет единственное с точностью до положительных множителей минимальное порождающее множество (остов)*

$$\{\widetilde{b^{(i)}} = (b_0^{(i)}, b_1^{(i)}, \ldots, b_n^{(i)}, b_{n+1}^{(i)}),\ i = 1, \ldots, s\}; \tag{3.2}$$

2) *существуют определяемые единственным образом такие множества* $T_\nu(f) \subseteq M_\nu(f)$ $(\nu = 0, 1)$, *что система* (1.6) *эквивалентна системе*

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{при всех } (x_1, \ldots, x_n) \in T_0(f); \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{при всех } (x_1, \ldots, x_n) \in T_1(f); \\ a_{n+1} \ge 0, \end{cases} \tag{3.3}$$

*никакая подсистема системы* (3.3) *не эквивалентна исходной системе;*

3) *для любой точки* $x = (x_1, \ldots, x_n) \in T_0(f)$ *существует такое подмножество* $I$ *множества* $\{1, \ldots, s\}$, *что* $|I| = n + 1$, *подсистема*

*векторов* $\{\widetilde{b^{(i)}},\ i \in I\}$ *линейно независима и*

$$\sum_{j=1}^{n} b_j^{(i)} x_j = b_0^{(i)}\ (i \in I),\ \sum_{i \in I} b_{n+1}^{(i)} > 0; \tag{3.4}$$

4) *для любой точки* $x = (x_1, \ldots, x_n) \in T_1(f)$ *существует такое подмножество* $I$ *множества* $\{1, \ldots, s\}$, *что* $|I| = n + 1$, *подсистема векторов* $\{\widetilde{b^{(i)}},\ i \in I\}$ *линейно независима и*

$$\sum_{j=1}^{n} b_j^{(i)} x_j = b_0^{(i)} + b_{n+1}^{(i)}\ (i \in I),\ \sum_{i \in I} b_{n+1}^{(i)} > 0.$$

**Замечание 3.6.** Так как для истинности утверждения 2 леммы 3.5 достаточно, чтобы конус $K(f)$ был телесным, то это утверждение выполняется для любого $M$, даже если $\operatorname{Affdim} M < n$.

## 3.3. Структура разрешающего множества пороговой функции

Для произвольных $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$ рассмотрим следующую подсистему системы (1.6):

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j \le a_0 & \text{при всех } (x_1, \ldots, x_n) \in T_0; \\ \sum\limits_{j=1}^{n} a_j x_j \ge a_0 + a_{n+1} & \text{при всех } (x_1, \ldots, x_n) \in T_1; \\ a_{n+1} \ge 0. \end{cases} \tag{3.5}$$

**Теорема 3.7.** *Для того, чтобы множество* $T = T_0 \cup T_1$, $T_\nu \subseteq M_\nu(f)$ $(\nu = 0, 1)$ *было разрешающим для* $f \in \mathfrak{T}(M)$, *необходимо и достаточно, чтобы система неравенств* (3.5) *была эквивалентна системе неравенств* (1.6).

*Доказательство.* Поскольку достаточность условий очевидна, докажем их необходимость. Предположим, что нашлось решение $b = (b_0, \ldots, b_{n+1})$

системы (3.5), не принадлежащее конусу $K(f)$. По лемме 3.3 и п. 2 леммы 3.5 можно считать, что $b_{n+1} > 0$. Неравенство $\sum_{j=1}^{n} b_j x_j \leq b_0$ определяет некоторую функцию $g \in \mathfrak{T}(M)$, а так как $b \notin K(f)$, то $g \neq f$. Однако $g(x) = f(x)$ для всех $x \in T$. Следовательно, $T$ не является разрешающим множеством. ∎

Из теоремы 3.7 и п. 2 леммы 3.5 получаем

**Следствие 3.8.** *Для любой функции $f \in \mathfrak{T}(M)$ множество $T = T_0 \cup T_1$, где $T_\nu \subseteq M_\nu(M)$ $(\nu = 0, 1)$, является минимальным разрешающим тогда и только тогда, когда $T_\nu = T_\nu(f)$ $(\nu = 0, 1)$.*

Из следствия 3.8, п. 2 леммы 3.5 и замечания 3.6 вытекает

**Следствие 3.9.** *Для любой функции $f \in \mathfrak{T}(M)$ существует единственное минимальное разрешающее множество. Это множество в точности совпадает со множеством всех существенных для $f$ точек относительно класса $\mathfrak{T}(M)$.*

Теорема 3.7, следствия 3.8 и 3.9 являются обобщениями известных утверждений о пороговых булевых функциях [39].

Минимальное разрешающее множество функции $f$ обозначим через $T(f) = T_0(f) \cup T_1(f)$. Из леммы 1.6 получаем следующий результат.

**Теорема 3.10.** (Ср. [104]) *Для любой $f \in \mathfrak{T}(M)$ справедливо включение $T(f) \subseteq N_0(f) \cup N_1(f)$.*

Пусть $\operatorname{Affdim} M = n$ и $f \in \mathfrak{T}(M)$. Не нарушая общности, будем считать, что в (3.2) $b_{n+1}^{(i)} > 0$ при $i = 1, \ldots, \mu$ и $b_{n+1}^{(i)} = 0$ при $i = \mu + 1, \ldots, s$. Пусть $a = (a_1, \ldots a_n) \in \mathbb{Z}^n$,

$$M_0(f, a) = \left\{ (y_1, \ldots, y_n) \in M : \sum_{j=1}^{n} a_j y_j = \max_{x \in M_0(f)} \sum_{j=1}^{n} a_j x_j \right\},$$

$$M_1(f,a)=\left\{(y_1,\dots,y_n)\in M:\ \sum_{j=1}^{n}a_jy_j=\min_{x\in M_1(f)}\sum_{j=1}^{n}a_jx_j\right\}.$$

Обозначим $N_\nu(f,a)=\operatorname{Vert}M_\nu(f,a)$ $(\nu=0,1)$.

**Теорема 3.11.** *Пусть* $\operatorname{Affdim}M=n$*, тогда для любой функции* $f\in\mathfrak{T}(M)$

$$T(f)=\bigcup_{i=1}^{\mu}\left(N_0(f,\widetilde{b^{(i)}})\cup N_1(f,\widetilde{b^{(i)}})\right)=\bigcup_{a}\big(N_0(f,a)\cup N_1(f,a)\big),$$

*в последнем случае объединение берется по всем таким векторам* $a=(a_1,\dots,a_n)\in\mathbb{Z}^n$*, что неравенство*

$$\sum_{j=1}^{n}a_jx_j\le\max_{x\in M_0(f)}\sum_{j=1}^{n}a_jx_j$$

*является пороговым для функции* $f$*.*

*Доказательство.* Вначале докажем, что

$$T(f)\subseteq\bigcup_{i=1}^{\mu}\left(N_0(f,\widetilde{b^{(i)}})\cup N_1(f,\widetilde{b^{(i)}})\right).$$

Пусть $y=(y_1,\dots y_n)\in T_0(f)$. По 3-му утверждению леммы 3.5 найдется такое $i\in\{1,\dots,\mu\}$, что $\sum\limits_{j=1}^{n}b_j^{(i)}y_j=b_0^{(i)}$. Так как $b_{n+1}^{(i)}>0$, то коэффициенты $b_j^{(i)}$ $(j=0,1,\dots,n)$ задают пороговое неравенство для функции $f$ и $\max\limits_{x\in M_0(f)}\sum\limits_{j=1}^{n}x_jb_j^{(i)}=b_0^{(i)}$. Отсюда следует, что $y\in M_0(f,\widetilde{b^{(i)}})$. Предположив, что $y\notin N_0(f,\widetilde{b^{(i)}})$, т. е. $y=\sum\limits_{q=1}^{p}\alpha_qy^{(q)}$ для некоторых $p>1$, $\alpha_q>0$, $\sum\limits_{q=1}^{p}\alpha_q=1$, $y\ne y^{(q)}\in M_0(f,\widetilde{b^{(i)}})$ $(q=1,\dots,p)$, получаем $y\notin N_0(f)$ и по теореме 3.10 $y\notin T_0(f)$. Полученное противоречие показывает, что $y\in N_0(f,\widetilde{b^{(i)}})$. Пусть теперь $y\in T_1(f)$. По 4-му утверждению леммы 3.5 найдется такое $i\in\{1,\dots\mu\}$, что $\sum\limits_{j=1}^{n}b_j^{(i)}y_j=b_0^{(i)}+b_{n+1}^{(i)}$. Так как $b_{n+1}^{(i)}>0$, то коэффициенты $b_j^{(i)}$ $(j=0,1,\dots n)$ задают пороговое неравенство для функции $f$ и $\min\limits_{x\in M_1(f)}\sum\limits_{j=1}^{n}x_jb_j^{(i)}=b_0^{(i)}+b_{n+1}^{(i)}$. Отсюда получаем, что $y\in M_1(f,\widetilde{b^{(i)}})$ и по теореме 3.10 $y\in N_1(f,\widetilde{b^{(i)}})$.

Теперь докажем, что $\bigcup\limits_{a}(N_0(f,a)\cup N_1(f,a))\subseteq T(f)$.

Пусть $a=(a_1,\ldots,a_n)\in\mathbb{Z}^n$, $a_0=\max\limits_{x\in M_0(f)}\sum\limits_{j=1}^{n}a_jx_j$, $\sum\limits_{j=1}^{n}a_jx_j\le a_0$ — пороговое неравенство для функции $f$. Для любой точки $z\in N_0(f,a)$ определим функцию $g$ следующим образом: $M_0(g)=M_0(f)\setminus\{z\}$, $M_1(g)=M_1(f)\bigcup\{z\}$. Докажем, что $g\in\mathfrak{T}(M)$. Предположим противное, тогда $P_0(g)\cap P_1(g)\neq\varnothing$. Это означает, что найдутся такие точки $x^{(1)},\ldots,x^{(p)}$ из $M_0(g)$, $y^{(0)},\ldots,y^{(q)}$ из $M_1(g)$ и такие положительные числа $\alpha_1,\ldots\alpha_p$, $\beta_0,\ldots\beta_q$, что

$$x=(x_1,\ldots,x_n)=\sum_{r=1}^{p}\alpha_rx^{(r)}=\sum_{t=0}^{q}\beta_ty^{(t)},\tag{3.6}$$

$\sum\limits_{r=1}^{p}\alpha_r=1$, $\sum\limits_{t=0}^{q}\beta_t=1$. Очевидно, что среди $y^{(0)},\ldots,y^{(q)}$ есть точка $z$, иначе 3.6 означало бы, что $P_0(f)\cap P_1(f)\neq\varnothing$, что невозможно, так как $f\in\mathfrak{T}(M)$. Будем считать, что $z=y^{(0)}$. Имеем $\sum\limits_{j=1}^{n}a_jx_j=\sum\limits_{r=1}^{p}\alpha_r\sum\limits_{j=1}^{n}a_jx_j^{(r)}=\sum\limits_{t=1}^{q}\beta_t\sum\limits_{j=1}^{n}a_jy_j^{(t)}+\beta_0\sum\limits_{j=1}^{n}a_jz_j$. В последнем равенстве центральная часть не превосходит $a_0$; в правой части первое слагаемое больше $a_0$, а второе — равно $a_0$. Для равенства необходимо, чтобы $q=0$ и $\sum\limits_{j=1}^{n}a_jx_j^{(r)}=a_0$ $(r=1,\ldots,p)$. Таким образом, $\beta_0=1$, $z=x$. Из (3.6) теперь получаем: $z\notin N_0(f,a)$, что противоречит условию. Таким образом, $g$ — пороговая. Так как значения функций $f$ и $g$ отличаются лишь в точке $z$, то $z\in T(f)$.

Пусть теперь $a=(a_1,\ldots,a_n)\in\mathbb{Z}^n$, $a_0=\min\limits_{x\in M_1(f)}\sum\limits_{j=1}^{n}a_jx_j$. Неравенство $\sum\limits_{j=1}^{n}a_jx_j\ge a_0$ выполняется для каждой точки из $M_1(f)$ и не выполняется ни для какой точки из $M_0(f)$. Для произвольной $z\in N_1(f,a)$ проведем следующие рассуждения, аналогичные приведенным выше.

Определим функцию $g$ так, чтобы $M_0(g)=M_0(f)\cup\{z\}$, $M_1(g)=M_1(f)\setminus\{z\}$. Докажем, что $g\in\mathfrak{T}(M)$. Предположим противное, тогда $P_0(g)\cap P_1(g)\neq\varnothing$. Это означает, что найдутся такие точки $x^{(0)},\ldots,x^{(p)}$ из $M_0(g)$, $y^{(1)},\ldots,y^{(q)}$ из $M_1(g)$ и такие положительные числа $\alpha_0,\ldots\alpha_p$,

$\beta_1, \ldots \beta_q$, что

$$x = (x_1, \ldots, x_n) = \sum_{r=0}^{p} \alpha_r x^{(r)} = \sum_{t=1}^{q} \beta_t y^{(t)}, \tag{3.7}$$

$\sum_{r=0}^{p} \alpha_r = 1$, $\sum_{t=1}^{q} \beta_t = 1$. Очевидно, что среди $x^{(0)}, \ldots, x^{(p)}$ есть точка $z$, иначе мы бы получили $P_0(f) \cap P_1(f) \neq \varnothing$, что невозможно, так как $f \in \mathfrak{T}(M)$. Будем считать, что $z = x^{(0)}$. Имеем $\sum_{j=1}^{n} a_j x_j = \sum_{r=1}^{p} \alpha_r \sum_{j=1}^{n} a_j x_j^{(r)} + \alpha_0 \sum_{j=1}^{n} a_j z_j = \sum_{t=1}^{q} \beta_t \sum_{j=1}^{n} a_j y_j^{(t)}$. В последнем равенстве правая часть больше или равна $a_0$; в центральной части первое слагаемое строго меньше $a_0$, а второе — равно $a_0$. Для равенства необходимо, чтобы $p = 0$ и $\sum_{j=1}^{n} a_j y_j^{(t)} = a_0$ $(t = 1, \ldots, q)$. Таким образом, $\alpha_0 = 1$, $z = x$. Из (3.7) теперь получаем: $z \notin N_1(f, a)$, что противоречит условию. Таким образом, $g$ — пороговая. Так как значения функций $f$ и $g$ отличаются лишь в точке $z$, то $z \in T(f)$.

Очевидно, $\bigcup_{i=1}^{\mu} \left( N_0(f, \widetilde{b^{(i)}}) \cup N_1(f, \widetilde{b^{(i)}}) \right) \subseteq \bigcup_{a} (N_0(f, a) \cup N_1(f, a))$. Последнее включение завершает доказательство теоремы. ∎

В качестве иллюстрации к теореме рассмотрим

**Пример 3.12.** Пусть функция $f \in \mathfrak{T}(E_k^3)$, $k \geq 9$, задана пороговым неравенством $20x_1 + 28x_2 + 35x_3 \leq 140$. Перепишем систему (3.3) в виде $aQ \geq 0$, где $a = (a_0, \ldots, a_{n+1})$ — строка переменных, а $Q$ — матрица, составленная из компонент точек разрешающего множества $T(f)$. Коэффициенты векторов $\widetilde{b^{(i)}}$, порождающих конус $K(f)$, запишем построчно в матрицу $B$. Для анализа структуры множества $T(f)$ рассмотрим таблицу

| | $Q$ |
|---|---|
| $B$ | $S$ |

, (3.8)

где $S = BQ$, а $E$ — единичная матрица. Таблица (3.8) представлена на рис. 3.1 (точки соответствуют нулевым значениям). Имеем $\mu = 3$,

$$N_0(f, \widetilde{b^{(1)}}) = \{p^{(1)}, p^{(3)}\}, \quad N_1(f, \widetilde{b^{(1)}}) = \{q^{(1)}, q^{(2)}\},$$

| | | | | | 1 | 1 | 1 | −1 | −1 | −1 | · |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | −7 | · | · | 4 | 3 | 2 | · |
| | | | | | · | −5 | · | 1 | 3 | · | · |
| | | | | | · | · | −4 | 1 | · | 3 | · |
| | | | | | · | · | · | −1 | −1 | −1 | 1 |
| 56 | 8 | 11 | 14 | 1 | · | 1 | · | · | · | 1 | 1 |
| 70 | 10 | 14 | 17 | 1 | · | · | 2 | · | 1 | · | 1 |
| 140 | 20 | 28 | 35 | 3 | · | · | · | · | 1 | 2 | 3 |
| 140 | 20 | 28 | 35 | · | · | · | · | 3 | 4 | 5 | · |
| 105 | 15 | 21 | 25 | · | · | · | 5 | 1 | 3 | · | · |
| 84 | 12 | 16 | 21 | · | · | 4 | · | 1 | · | 3 | · |
| 80 | 11 | 16 | 20 | · | 3 | · | · | · | 1 | 2 | · |
| 50 | 7 | 10 | 12 | · | 1 | · | 2 | · | 1 | · | · |
| 36 | 5 | 7 | 9 | · | 1 | 1 | · | · | · | 1 | · |
| 21 | 3 | 4 | 5 | · | · | 1 | 1 | · | · | · | · |

Рис. 3.1

$$N_0(f, \widetilde{b^{(2)}}) = \{p^{(1)}, p^{(2)}\}, \quad N_1(f, \widetilde{b^{(2)}}) = \{q^{(1)}, q^{(3)}\},$$

$$N_0(f, \widetilde{b^{(3)}}) = \{p^{(1)}, p^{(2)}, p^{(3)}\}, \quad N_1(f, \widetilde{b^{(1)}}) = \{q^{(1)}\},$$

где $p^{(1)} = (7, 0, 0)$, $p^{(2)} = (0, 5, 0)$, $p^{(3)} = (0, 0, 4)$, $q^{(1)} = (4, 1, 1)$, $q^{(2)} = (3, 3, 0)$, $q^{(3)} = (2, 0, 3)$, $\widetilde{b^{(1)}} = (56, 8, 11, 14, 1)$, $\widetilde{b^{(2)}} = (70, 10, 14, 17, 1)$, $\widetilde{b^{(3)}} = (140, 20, 28, 35, 140)$. По теореме 3.11 $T_\nu(f) = \bigcup_{i=1}^{3} N_\nu(f, \widetilde{b^{(i)}}\ \nu = 0, 1)$. В рассматриваемом примере в объединении достаточно оставить 2 члена: $T_0(f) = N_0(f, \widetilde{b^{(3)}}) = N_0(f, \widetilde{b^{(1)}}) \cup N_0(f, \widetilde{b^{(2)}})$, $T_1(f) = N_1(f, \widetilde{b^{(1)}}) \cup N_1(f, \widetilde{b^{(2)}})$.

## 3.4. Оценки длины обучения в классе пороговых функций

Из теоремы 3.10 и формулы (1.11) получаем

**Следствие 3.13.** *Для любого фиксированного $n$ и любого $M \in \mathfrak{M}(n, l, \gamma)$*

$$\sigma(M) = O\left(l^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} \gamma\right).$$

Далее (см. следствие 3.16) мы покажем, что в общем случае эту оценку нельзя улучшить.

Обозначим $N = \operatorname{Vert} M$. Справедливо следующее

**Утверждение 3.14.** *Для функции $f$, тождественно равной константе, верно равенство $T(f) = N$.*

*Доказательство.* Предположим, что для $f \equiv \nu$ нашлась точка $x \in N \setminus T(f)$. Рассмотрим функцию $g$, для которой $M_\nu(g) = M \setminus \{x\}$, $M_{1-\nu}(g) = \{x\}$. Так как $x \in N$, то, очевидно, $g$ — пороговая. Имеем $M_\nu(g) = M_\nu(f) \setminus \{x\}$, $M_{1-\nu}(g) = M_{1-\nu}(f) \cup \{x\}$, следовательно, $x \in T(f)$. Итак, $N \subseteq T(f)$. Обратное включение следует из теоремы 3.10. ∎

**Следствие 3.15.** *Для любых $k \geq 2$ и $n \geq 1$ выполняется неравенство $\tau(E_k^n) \geq \sigma(E_k^n) \geq 2^n$.*

*Доказательство.* Рассмотрим функцию $f \equiv 0$. Согласно утверждению 3.14 имеем $\sigma(f) = 2^n$, отсюда $\sigma(E_k^n) \geq 2^n$. ∎

Таким образом, полиномиального от $n$ алгоритма расшифровки в классе $\mathfrak{T}(E_k^n)$ не существует [104].

Аналогом следствия 3.15 для класса $\mathfrak{T}(M)$, где $M \in \mathfrak{M}(n, l, \gamma)$, является

**Следствие 3.16.** *Для любых натуральных $n \geq 2$ и $l > n$ найдется такое $\gamma_0$, что для всех $\gamma \geq \gamma_0$ существует политоп $P \in \mathfrak{P}(n, l, \gamma)$, такой, что*

$$\tau(M) \geq \sigma(M) = \Omega\left(l^{\lfloor n/2 \rfloor} \log^{n-1} \gamma\right),$$

*где $M = P \cap \mathbb{Z}^n$ (асимптотика при фиксированном $n$).*

*Доказательство.* В [10, 93] для любых фиксированных $n \geq 2$ и $l > n$ и любого достаточно большого $\gamma$ доказано существование такого политопа $P \in \mathfrak{P}(n, l, \gamma)$, для которого

$$|\operatorname{Vert}(P \cap \mathbb{Z}^n)| = \Omega\Big(l^{\lfloor n/2 \rfloor} \log^{n-1} \gamma\Big).$$

Для завершения доказательства следствия осталось обратиться к утверждению 3.14. ∎

Вернемся теперь к исследованию сложности расшифровки в классе $\mathfrak{T}(E_k^n)$.

**Теорема 3.17.** *При любых $n \geq 3$, $k \geq 2$*

$$\sigma(E_k^n) \geq \frac{\big(\frac{1}{2}\log k - n - 3 - (n-1)\log(n-2)\big)^{n-2}}{4(n-1)3^{n-1}(n-2)^{n-2}\big((n-2)!\big)^2}. \tag{3.9}$$

*Доказательство.* Для каждого целого $\Delta \geq 2$ определим множество

$$\Phi(n, \Delta) = \{(a_0, \ldots, a_{n-1}) : \ 0 \leq a_j \leq \Delta - 1 \ (j = 0, \ldots, n-1)\}.$$

Пусть $(a_0, \ldots, a_{n-1}) \in \Phi(n, \Delta)$. Обозначим через $V(a_0, \ldots, a_{n-1}, \Delta)$ множество вершин выпуклой оболочки множества решений системы

$$\sum_{j=1}^{n-1} a_j x_j + x_j \equiv a_0 \,(\mathrm{mod}\, \Delta), \quad x_j \in \mathbb{Z}, \quad x_j \geq 0 \quad (j = 1 \ldots n). \tag{3.10}$$

В [8] (см. также [10, 105, § 3.5]) установлена верхняя оценка для среднего числа вершин:

$$\varphi(n, \Delta) = \Delta^{-n} \sum_{(a_0, \ldots, a_{n-1}) \in \Phi(n, \Delta)} |V(a_0, \ldots, a_{n-1}, \Delta)|.$$

**Лемма 3.18.** [8] *При любых целых $n \geq 2$ и $\Delta \geq 2$ справедливо неравенство*

$$\varphi(n, \Delta) \geq c_n\big(\log \Delta - n - 2 - n\log(n-1)\big)^{n-1},$$

*где* $c_n = \Big(4n3^n(n-1)^{n-1}\big((n-1)!\big)^2\Big)^{-1}$.

Обозначим через $N(a_0, \ldots, a_n)$ множество вершин выпуклой оболочки решений системы

$$\begin{cases} \sum\limits_{j=1}^{n} a_j x_j = a_0, \\ x_j \geq 0, \quad x_j \in \mathbb{Z} \qquad (j = 1, 2, \ldots, n). \end{cases}$$

Используя лемму 3.18, докажем следующее вспомогательное утверждение.

**Лемма 3.19.** *При любых целых* $n \geq 3$ *и* $k \geq 2$ *найдутся* $a_0 \in \mathbb{Z}$ *и* $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ *такие, что* $0 < a_j < k$ $(j = 0, 1, \ldots, n)$ *и*

$$|N(a_0, \ldots, a_n)| \geq c_{n-1} \left( \frac{1}{2} \log k - n - 3 - (n-1) \log(n-2) \right)^{n-2},$$

*где* $c_n$ *— величина, определенная в лемме* 3.18.

*Доказательство.* Пусть

$$\Delta(\Delta - 1) \leq a_0 \leq \Delta^2 - 1, \quad 0 \leq a_j \leq \Delta - 1 \quad (j = 1, \ldots, n-1).$$

По теореме 3.35 из [105] имеем $N' \subseteq N(a_0, \ldots, a_{n-1}, \Delta)$, где $N'$ — множество вершин выпуклой оболочки целочисленных решений системы

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} + \Delta x_n = a_0, \quad x_j \geq 0 \quad (j = 1, \ldots, n-1).$$

Легко видеть, что $N'$ взаимно однозначно отображается в множество вершин выпуклой оболочки неотрицательных решений сравнения

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} \equiv a_0 \pmod{\Delta},$$

или ему эквивалентного

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} \equiv a_0 - \Delta(\Delta - 1) \pmod{\Delta}. \tag{3.1}$$

Для завершения доказательства леммы 3.19 осталось сравнить (3.1) с (3.10), положить $k = \Delta^2$ и воспользоваться леммой 3.18. ∎

Заметим, что доказательство леммы 3.19 построено на основе доказательства аналогичного результата из [8] о нижней оценке величины $N(a_0, \ldots, a_n)$.

Продолжим доказательство теоремы 3.17.

Пусть $a_0, \ldots, a_n$ — величины, существование которых утверждается в лемме 3.19. Рассмотрим пороговую функцию $f$ с пороговым неравенством

$$\sum_{j=1}^{n} a_j x_j \leq a_0.$$

По теореме 3.11 имеем $N(a_0, \ldots, a_n) \subseteq T_0(f)$. Теперь нижняя оценка длины обучения следует из леммы 3.19. Теорема 3.17 доказана полностью. ∎

**Следствие 3.20.** *При любом фиксированном* $n \geq 3$

$$\tau(E_k^n) \geq \sigma(E_k^n) = \Omega(\log^{n-2} k), \qquad (k \to \infty).$$

**Замечание 3.21.** При $n = 3$ коэффициенты порогового неравенства функции $f$, на которой достигается нижняя оценка в следствии 3.20, можно указать в явном виде. Положим

$$\beta_1 = 1, \qquad \beta_2 = 2, \qquad \gamma_2 = \gamma_2' = 1$$

и для каждого натурального $s \geq 2$

$$\beta_{s+1} = 2\beta_s + \beta_{s-1}, \qquad \gamma_{s+1} = \beta_s + \gamma_s', \qquad \gamma_{s+1}' = \beta_s + \beta_{s+1} + \gamma_s.$$

Если теперь взять

$$k = a_1 = \beta_s, \qquad a_2 = \beta_s + 1, \qquad a_3 = \beta_s + \beta_{s-1}$$

и при четном $s$ выбрать $a_0 = a_3\gamma_s$, а при нечетном — $a_0 = a_3\gamma_s'$, то [11, 105] $|N(a_0, a_1, a_2, a_3)| \geq s$ и $s$ пропорционально $\log k$.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 1 | 1 | 1 | −1 | −1 | −1 | · |
| | | | | | −3 | −7 | −6 | · | 2 | 10 | · | · |
| | | | | | −9 | −4 | −1 | · | 10 | · | 4 | · |
| | | | | | · | −1 | −4 | −9 | · | 2 | 6 | · |
| | | | | | · | · | · | · | −1 | −1 | −1 | 1 |
| 153 | 12 | 13 | 17 | 1 | · | · | · | · | · | · | · | 1 |
| 154 | 12 | 13 | 17 | · | 1 | 1 | 1 | 1 | · | · | · | · |
| 450 | 35 | 38 | 50 | · | 3 | 3 | 2 | · | · | · | 2 | · |
| 522 | 41 | 44 | 58 | · | 3 | 1 | · | · | · | 4 | 2 | · |
| 190 | 15 | 16 | 21 | · | 1 | · | · | 1 | · | 2 | · | · |
| 153 | 12 | 13 | 17 | · | · | · | · | · | 1 | 1 | 1 | · |
| 270 | 21 | 23 | 30 | · | · | 1 | 1 | · | 2 | · | 2 | · |
| 282 | 22 | 24 | 31 | · | · | 1 | 2 | 3 | 2 | · | · | · |
| 318 | 25 | 27 | 35 | · | · | · | 1 | 3 | 2 | 2 | · | · |

Рис. 3.2

**Пример 3.22.** В частности, при $s = 4$ получаем пороговое неравенство $12x_1 + 13x_2 + 17x_3 \leq 153$. Для данного случая таблица (3.8) представлена на рис. 3.2. Здесь $\mu = 1$ и $b^{(1)} = (153, 12, 13, 17, 1)$. При $p^{(1)} = (3, 9, 0)$, $p^{(2)} = (7, 4, 1)$, $p^{(3)} = (6, 1, 4)$, $p^{(4)} = (0, 0, 9)$, $q^{(1)} = (2, 10, 0)$, $q^{(2)} = (10, 0, 2)$, $q^{(3)} = (0, 4, 6)$ имеем: $T_0(f) = (p^{(1)}, p^{(2)}, p^{(3)}, p^{(4)})$, $T_1(f) = (q^{(1)}, q^{(2)}, q^{(3)})$.

В [138] на основе [103, 127] получена верхняя оценка

$$\sigma(E_k^n) = O(\log^{n-1} k) \tag{3.11}$$

при любом фикисрованном $n$. Действительно, по теореме 3.10 имеем $T(f) \subseteq N_0(f) \cup N_1(f)$, но из утверждения 1.18 получаем

$$|N_0(f)| + |N_1(f)| = O(\log^{n-1} k),$$

откуда и следует (3.11). В разделе 3.8 для $\sigma(E_k^n)$ будет получена более сильная верхняя оценка, при фиксированном $n$ по порядку совпадающая с нижней оценкой из следствия 3.20.

## 3.5. Другая характеризация минимального разрешающего множества пороговой функции

Пусть $f \in \mathfrak{T}(M)$. В настоящем разделе получим новую характеризацию множества $T(f)$.

Введем обозначения: $Q(f) = \operatorname{Cone}\Big(M_0(f) - M_1(f)\Big)$; если $f$ — тождественная константа, то $Q(f) = \{o\}$;

$$R_0(f) = \operatorname{Conv}\Big(M_0(f)\Big) + Q(f), \qquad R_1(f) = \operatorname{Conv}\Big(M_1(f)\Big) - Q(f).$$

**Пример 3.23.** На рис. 3.3 изображены множества $R_0(f)$ и $R_1(f)$ для функция $f \in \mathfrak{T}(E_4^2)$, заданной пороговым неравенством $2x_1 + x_2 \leq 3$. Обозначим

$$x^{(1)} = (0,3), \quad x^{(2)} = (1,1), \quad y^{(1)} = (1,2), \quad y^{(2)} = (2,0). \tag{3.2}$$

Имеем $Q(f) = \operatorname{Cone}\{r^{(1)}, r^{(2)}\}$,

$$R_0(f) = \operatorname{Conv}\{x^{(1)}, x^{(2)}\} + Q(f), \quad R_1(f) = \operatorname{Conv}\{y^{(1)}, y^{(2)}\} - Q(f),$$

где $r^{(1)} = x^{(1)} - y^{(2)} = (-2,3)$, $r^{(2)} = x^{(2)} - y^{(1)} = (0,-1)$.

Ниже (см. теорему 3.25) мы дадим описание минимального разрешающего множества $T(f)$ в терминах множеств $R_\nu(f)$ ($\nu = 0,1$).

**Лемма 3.24.** *Пусть $X$, $Y$ — конечные множества точек из $\mathbb{R}^n$, причем* $\operatorname{Conv} X \cap \operatorname{Conv} Y = \varnothing$. *Тогда*

$$X' = \operatorname{Conv} \operatorname{Vert} X' + \operatorname{Cone}(\operatorname{Vert} X' - \operatorname{Vert} Y').$$

*где* $X' = \operatorname{Conv} X + \operatorname{Cone}(X - Y)$, $Y' = \operatorname{Conv} Y + \operatorname{Cone}(Y - X)$.

*Доказательство.* Докажем включение

$$\operatorname{Conv} X + \operatorname{Cone}(X - Y) \subseteq \operatorname{Conv} \operatorname{Vert} X' + \operatorname{Cone}(\operatorname{Vert} X' - \operatorname{Vert} Y').$$

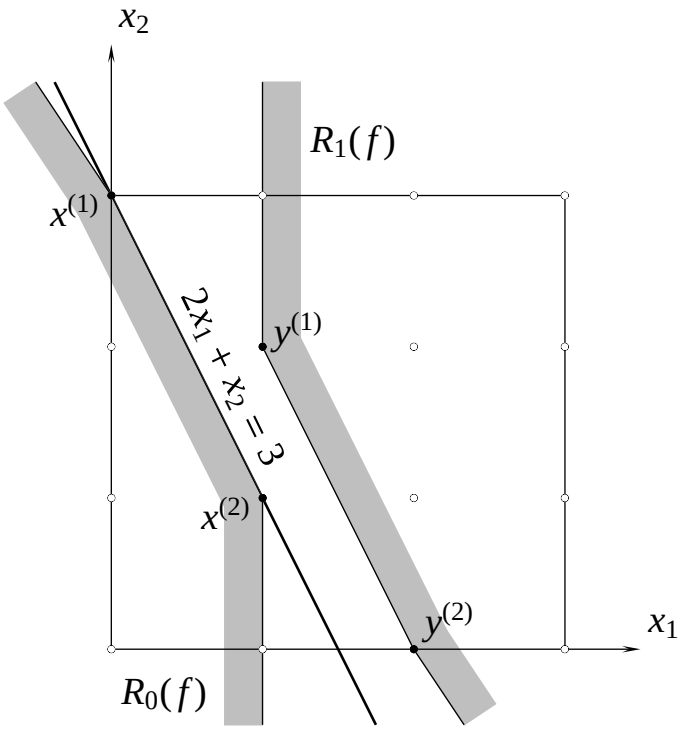


Рис. 3.3

Обратное включение очевидно.

Достаточно показать, что для произвольного экстремального вектора $r$ конуса $\mathrm{Cone}(X - Y)$ рецессивных направлений множества $X'$ справедливо $r \in \mathrm{Cone}(\mathrm{Vert}\, X' - \mathrm{Vert}\, Y')$. Пусть $a(x - v) = 0$ — опорная гиперплоскость для экстремального луча $v + \mathrm{Cone}\{r\}$, т. е. $v \in \mathrm{Vert}\, X'$, $a \in \mathbb{R}^n$, $a \neq o$, $ar = 0$, $a(x - v) < 0$ для всех $x \in X' \setminus (v + \mathrm{Cone}\{r\})$.

Предположим, что нашлась точка $y \in Y'$, такая, что $a(y - v) < 0$. Рассмотрим $z = 2v - y$. Так как $v - y \in \mathrm{Cone}(X' - Y') = \mathrm{Cone}(X - Y)$, то из определения $X'$ следует $z \in X'$. Однако $a(z - v) = a(v - y) > 0$, следовательно, $z \notin X'$. Противоречие.

Предположим теперь, что $a(y - v) > 0$ для всех $y \in Y'$. Тогда для любых $x \in X'$ и $y \in Y'$ выполняется $a(x - y) = a(x - v) + a(v - y) < 0$. Так как $r = \alpha(x - y)$ для некоторых $\alpha > 0$, $x \in X'$, $y \in Y'$, то $ar < 0$. Противоречие.

Таким образом, $a(y-v) \geq 0$ для всех $y \in Y'$, причем найдется точка $y' \in Y'$, такая, что $a(y'-v) = 0$. Заметим, что $y' \in v - \mathrm{Cone}\{r\}$. Действительно, в противном случае в качестве опорной для экстремального луча $v + \mathrm{Cone}\{r\}$ гиперплоскости $a(x-v) = 0$ можно взять такую, что $a(y'-v) < 0$ и, следовательно, $y' \notin Y'$. Приходим к выводу, что найдется такая точка $w \in \mathrm{Vert}\, Y'$, что $w - \mathrm{Cone}\{r\} \subseteq Y'$. Получаем, что $r = \beta(v-w)$ для некоторого $\beta > 0$. ∎

**Теорема 3.25.** *Если* $f \in \mathfrak{T}(M)$, *то* $T_\nu(f) = \mathrm{Vert}\, R_\nu(f)$ $(\nu = 0, 1)$.

*Доказательство.* Если $f$ — тождественная константа, то доказываемое равенство очевидно. Пусть $f$ не является константой.

Вначале докажем, что имеет место включение $T_\nu(f) \subseteq \mathrm{Vert}\, R_\nu(f)$ $(\nu = 0, 1)$, т. е. $\mathrm{Vert}\, R_0(f) \cup \mathrm{Vert}\, R_1(f)$ — разрешающее множество для $f$.

Рассмотрим произвольную точку $z \in M_0(f)$. Пусть $T' = \{x^{(1)}, \ldots, x^{(s)}\}$, $T'' = \{y^{(1)}, \ldots, y^{(t)}\}$ — некоторые множества точек из $M$. По лемме Фаркаша (см., например, [81]), для того, чтобы неравенство $az \leq a_0$ являлось следствием системы (2.10), необходимо и достаточно, чтобы существовали неотрицательные числа $\alpha_1, \ldots, \alpha_s$, $\beta_1, \ldots, \beta_t$, такие, что не все $\alpha_1, \ldots, \alpha_s$ равны 0 и

$$z = \sum_{i=1}^{s} \alpha_i x^{(i)} - \sum_{j=1}^{t} \beta_j y^{(j)}, \qquad \sum_{i=1}^{s} \alpha_i - \sum_{j=1}^{t} \beta_j = 1.$$

Обозначим $\alpha = \sum\limits_{i=1}^{s} \alpha_i$, $\beta = \sum\limits_{j=1}^{t} \beta_j$, $\gamma_i = \alpha_i/\alpha$ $(i = 1, 2, \ldots, s)$, $\delta_j = \beta_j/\beta = \beta_j/(\alpha - 1)$ $(j = 1, 2, \ldots, t)$, тогда $\alpha \geq 1$, $\beta \geq 0$, $\sum\limits_{i=1}^{s} \gamma_i = 1$, $\sum\limits_{j=1}^{t} \delta_j = 1$,

$$z = \sum_{i=1}^{s} \gamma_i x^{(i)} + (\alpha - 1) \left( \sum_{i=1}^{s} \gamma_i x^{(i)} - \sum_{j=1}^{t} \delta_j y^{(j)} \right).$$

Получаем, что для того, чтобы неравенство $az \leq a_0$ являлось следствием системы (2.10), необходимо и достаточно, чтобы $z \in \mathrm{Conv}\, T' + \mathrm{Cone}(T' -$

$T''$). Аналогично можно показать, что если $z \in M_1(f)$, то для того, чтобы неравенство $az > a_0$ являлось следствием системы (2.10), необходимо и достаточно, чтобы $z \in \operatorname{Conv} T'' + \operatorname{Cone}(T'' - T')$. Теперь из следствия 3.8 и леммы 3.24 получаем, что $\operatorname{Vert} R_0(f) \cup \operatorname{Vert} R_1(f)$ — разрешающее множество пороговой функции $f$, т. е. $T_\nu(f) \subseteq \operatorname{Vert} R_\nu(f)$ $(\nu = 0, 1)$.

Теперь покажем, что $\operatorname{Vert} R_\nu(f) \subseteq T_\nu(f)$ $(\nu = 0, 1)$, т. е. множество $\operatorname{Vert} R_0(f) \cup \operatorname{Vert} R_1(f)$ — *минимальное* разрешающее. Для этого рассмотрим произвольную точкум $v \in \operatorname{Vert} R_0(f)$. Пусть $a(x - v) = 0$ — опорная для $R_0(f)$ гиперплоскость в вершине $v$, т. е. $a \in \mathbb{R}^n$, $a \neq o$ и $a(x - v) < 0$ для всех $x \in R_0(f) \setminus \{v\}$.

Докажем, что $a(x - v) \leq 0$ — пороговое неравенство для $f$. Так как $M_0(f) \subset R_0(f)$, то $a(x - v) \leq 0$ для всех $x \in M_0(f)$. Предположим теперь, что $a(y - v) \leq 0$ для некоторой $y \in M_1(f)$. Рассмотрим точку $z = 2v - y$. Имеем $z \in R_0(f)$, $x \neq z$ и $a(z - v) = a(v - y) \geq 0$, что противоречит тому, что $a(x - v) = 0$ — опорная для $R_0(f)$ гиперплоскость. Таким образом, $a(y - v) > 0$ для всех $y \in M_1(f)$.

Итак, неравенство $a(x-v) \leq 0$ — пороговое для $f$, причем $a(x-v) < 0$ для всех $x \in M_0(f) \setminus \{v\}$. Пусть $\varepsilon = \max\{a(x - v) : \ x \in M_0(f), \ x \neq v\}$. Неравенство $a(x - v) \leq \varepsilon$ задает пороговую функцию $f'$, отличную от $f$ только в точке $v$. Это доказывает, что $v$ принадлежит любому разрешающему множеству функции $f$, и, следовательно, $v \in T_0(f)$. Таким образом, $\operatorname{Vert} R_0(f) \subseteq T_0(f)$.

Аналогичные рассуждения можно провести для произвольной точки из $\operatorname{Vert} R_1(f)$, поэтому $\operatorname{Vert} R_1(f) \subseteq T_1(f)$. ∎

Проиллюстрируем теорему на примерах.

**Пример 3.26.** Для пороговой функции $f \in \mathfrak{T}(E_4^2)$, заданной пороговым неравенством $2x_1 + x_2 \leq 3$ из примера 3.23 (см. рис. 3.3), вершины множе-

ства $R_0(f)$ суть $x^{(1)}$, $x^{(2)}$, а вершины множества $R_1(f)$ суть $y^{(1)}, y^{(2)}$, поэтому $T_0(f) = \{x^{(1)}, x^{(2)}\}$, $T_1(f) = \{y^{(1)}, y^{(2)}\}$, где $x^{(1)}$, $x^{(2)}$, $y^{(1)}$, $y^{(2)}$ определены в (3.2).

**Пример 3.27.** Рассмотрим функцию $f \in \mathfrak{T}(E_{10}^3)$ с пороговым неравенством $20x_1 + 28x_2 + 35x_3 \leq 140$ из примера 3.12. Экстремальные лучи конуса $Q(f)$ определяются векторами

$$(5, 0, -3),\ (4, -3, 0),\ (-2, 5, -3),\ (-4, 4, -1),\ (-4, -1, 3),\ (-3, -3, 4).$$

Далее,

$$R_0(f) = \mathrm{Conv}\{x^{(1)},\ x^{(2)},\ x^{(3)}\} + Q(f),\ R_1(f) = \mathrm{Conv}\{y^{(1)},\ y^{(2)},\ y^{(3)}\} - Q(f),$$

где

$$x^{(1)} = (7, 0, 0), \quad x^{(2)} = (0, 5, 0), \quad x^{(3)} = (0, 0, 4),$$

$$y^{(1)} = (4, 1, 1), \quad y^{(2)} = (3, 3, 0), \quad y^{(3)} = (2, 0, 3).$$

Таким образом (ср. с примером 3.12), $T_0(f) = \{x^{(1)},\ x^{(2)},\ x^{(3)}\}$, $T_1(f) = \{y^{(1)},\ y^{(2)},\ y^{(3)}\}$.

**Следствие 3.28.** *Пусть* $f \in \mathfrak{T}(M)$, $x, y \in T_\nu(f)$ $(\nu = 0, 1)$, $x \neq y$. *Тогда* $2x - y \notin R_0(f) \cup R_1(f)$.

*Доказательство.* Пусть $x, y \in T_0(f)$. Обозначим $z = 2x - y$.

Если $z \in R_0(f)$, то $x = (y + z)/2$, поэтому $x \notin \mathrm{Vert}\, R_0(f) = T_0(f)$.

Если $z \in R_1(f)$, то рассмотрим $y' = y + (x - z)$. Так как $y \in M_0(f)$, а $x - z \in Q(f)$, то $y' \in R_0(f)$. Имеем $y = (x + y')/2$, откуда получаем $y \notin \mathrm{Vert}\, R_0(f) = T_0(f)$.

Случай $x, y \in T_1(f)$ рассматривается аналогично. ∎

## 3.6. Верхняя оценка мощности минимального разрешающего множества для одного подкласса пороговых функций

В общем случае удобного описания множеств $R_\nu(f)$ $(\nu = 0, 1)$, которое позволило бы достаточно точно оценить $|\operatorname{Vert} R_\nu(f)|$, не известно. Рассмотрим однако множество $\mathfrak{T}'(E_k^n)$ таких пороговых функций $f$, для каждой из которых найдется пороговое неравенство $ax \leq a_0$, где $a = (a_1, a_2, \ldots, a_n)$ и

$$a_0 \in \mathbb{Z}, \quad a_j \in \mathbb{Z}, \quad 0 < a_0 < a_j(k-1) \qquad (j = 1, 2, \ldots, n). \tag{3.3}$$

Например, функция $f$ из примеров 3.23, 3.26 не принадлежит множеству $\mathfrak{T}'(E_4^2)$, а функция из примера 3.27 принадлежит $\mathfrak{T}'(E_{10}^3)$.

Легко видеть, что разделяющая гиперплоскость функции $f \in \mathfrak{T}'(E_k^n)$ пересекает только те ребра гиперкуба $E_k^n$, которые инцидентны вершине $o = (0, \ldots, 0)$. Кроме того, для любой точки $x = (x_1, \ldots, x_n) \in M_0(f)$ имеем $x_j \leq k - 2$ $(j = 1, 2, \ldots, n)$, так как $a_j x_j \leq ax \leq a_0 < a_j(k-1)$.

Класс $\mathfrak{T}'(E_k^n)$ является достаточно «естественным». В частности, для любой $f \in \mathfrak{T}'(E_k^n)$ множество $M_0(f)$ представляет собой множество допустимых точек некоторой задачи о рюкзаке (без ограничений на количество предметов данного типа), и, наоборот, для любой задачи о рюкзаке (с $a_j > 0$) найдутся такое $k$ и такая функция $f \in \mathfrak{T}'(E_k^n)$, что множество $M_0(f)$ есть множество ее допустимых точек. При этом $\operatorname{Conv} M_0(f)$ есть полиэдр (многогранник) задачи о рюкзаке, представляющий большой интерес в целочисленном линейном программировании (см., например, [105]). Кроме того, по-видимому, что предлагаемый здесь подход для получения оценок мощности $|T(f)|$, где $f \in \mathfrak{T}'(E_k^n)$, удастся в дальнейшем применить к произвольным пороговым функциям.

Обозначим $\mathbb{Z}_+^n$ множество векторов из $\mathbb{Z}^n$ с неотрицательными компонентами. Говорят, что множество $G \subset \mathbb{Z}_+^n$ обладает *свойством разделенности*, если из условий $x, y \in G$, $x \neq y$ следует $2x - y \notin \mathbb{Z}_+^n$ [100]. Покажем, что если $f \in \mathfrak{T}'(E_k^n)$, то множества $T_0(f)$ и $T_1(f)$ обладают свойством разделенности. Ниже для оценок их мощностей воспользуемся подходом [100, 105].

**Лемма 3.29.** *Если $f \in \mathfrak{T}'(E_k^n)$, то каждое из множеств $T_0(f)$ и $T_1(f)$ обладает свойством разделенности.*

*Доказательство.* Покажем, что если $f \in \mathfrak{T}'(E_k^n)$, то $\mathbb{Z}_+^n \subseteq R_0(f) \cup R_1(f)$.

Пусть $ax \leq a_0$ — пороговое неравенство, коэффициенты которого удовлетворяют (3.3). Рассмотрим точки $x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})$, $y^{(i)} = (y_1^{(i)}, \ldots, y_n^{(i)})$, где

$$x_j^{(j)} = \left\lfloor \frac{a_0}{a_j} \right\rfloor, \quad y_j^{(j)} = \left\lfloor \frac{a_0}{a_j} \right\rfloor + 1, \quad x_j^{(i)} = y_j^{(i)} = 0 \quad (i, j = 1, \ldots, n;\ i \neq j).$$

Легко видеть, что $x^{(j)} \in M_0(f)$ и, ввиду (3.3), $y^{(j)} \in M_1(f)$ $(j = 1, 2, \ldots, n)$. Обозначим $Q' = \mathrm{Cone}\{x^{(1)} - y^{(1)},\ x^{(2)} - y^{(2)}, \ldots, x^{(n)} - y^{(n)}\}$. Получаем, что $-\mathbb{Z}_+^n = Q' \subseteq Q(f)$.

Рассмотрим произвольную точку $x \in \mathbb{Z}_+^n$. Если $ax \leq a_0$, то $x \in M_0(f) \subseteq R_0(f)$. Если $ax > a_0$, то $x \in M_1(f) + \mathbb{Z}_+^n = M_1(f) - Q' \subseteq M_1(f) - Q(f) = R_1(f)$.

Итак, $\mathbb{Z}_+^n \subseteq R_0(f) \cup R_1(f)$, поэтому, согласно следствию 3.28, множества $T_0(f)$ и $T_1(f)$ обладают свойством разделенности. ∎

**Лемма 3.30.** *Пусть $f \in \mathfrak{T}'(E_k^n)$ и $ax \leq a_0$ — пороговое неравенство для $f$, для которого справедливо* (3.3)*. Для любого $x = (x_1, x_2, \ldots, x_n) \in T_0(f)$ существует $j$, такое, что*

$$\frac{a_0}{na_j} - \frac{1}{n} < x_j \leq \frac{a_0}{a_j}.$$

*Для любого* $x = (x_1, x_2, \ldots, x_n) \in T_1(f)$ *существует* $j$*, такое, что*

$$\frac{a_0}{na_j} < x_j \leq \frac{a_0}{a_j} + 1.$$

*Доказательство.* Пусть $x \in T_0(f)$. Выберем $j$ так, чтобы

$$a_j x_j \geq a_i x_i \quad (i = 1, 2, \ldots, n). \tag{3.4}$$

Рассмотрим точку $y$, полученную из $x$ увеличением ее $j$-й компоненты на 1. В силу (3.3) имеем $y \in E_k^n$. Если $y \in M_0(f)$, то, легко видеть, что $x \notin \operatorname{Vert} R_0(f)$, что противоречит условию $x \in T_0(f)$. Следовательно, $y \in M_1(f)$, откуда $ax + a_j = ay > a_0$, поэтому $ax > a_0 - a_j$. Ввиду (3.4), имеем $na_j x_j \geq ax > a_0 - a_j$, откуда получаем $x_j > a_0/(na_j) - 1/n$.

С другой стороны, $ax \leq a_0$, поэтому $a_j x_j \leq a_0$, откуда $x_j \leq a_0/a_j$.

Пусть теперь $x \in T_1(f)$. Снова выберем $j$ согласно (3.4). Заметим, что $x_j \geq 1$, так как в противном случае получили бы, что $x = o$, откуда, в силу (3.3), $M_0(f) = \varnothing$. Рассмотрим точку $y$, полученную из $x$ уменьшением ее $j$-й компоненты на 1. Если $y \in M_1(f)$, то получили бы, что $x \notin \operatorname{Vert} R_1(f) = T_1(f)$ — противоречие, поэтому $y \in M_0(f)$. Следовательно, $ax - a_j = ay \leq a_0$, откуда $a_j x_j \leq ax \leq a_0 + a_j$, поэтому $x_j \leq 1 + a_0/a_j$.

С другой стороны, используя (3.4), получаем $na_j x_j \geq ax > a_0$, откуда $x_j > a_0/(na_j)$. ∎

**Лемма 3.31.** [100, 105] *Пусть множество* $G \subset \mathbb{Z}_+^n$ *обладает свойством разделенности и для каждого* $x = (x_1, x_2, \ldots, x_n) \in G$ *выполнено* $\alpha_i \leq x_i \leq \beta_i$ $(i = 1, \ldots, n-1)$*, где* $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, $\beta_1, \beta_2, \ldots, \beta_{n-1}$ *— неотрицательные числа, тогда*

$$|G| \leq \prod_{i=1}^{n-1} \left\lfloor 1 + \log \frac{\beta_i + 2}{\alpha_i + 1} \right\rfloor.$$

**Теорема 3.32.** *Для любой* $f \in \mathfrak{T}'(E_k^n)$ *при* $n \geq 2$

$$|T_\nu(f)| \leq n(1+\log n)\Big(1+\log(k+1)\Big)^{n-2} \qquad (\nu = 0,1). \qquad (3.5)$$

*Доказательство.* Известно [26, 109], что $|T_\nu(f)| \leq 2$ для любой $f \in \mathfrak{T}(E_k^2)$. Таким образом, при $n = 2$ неравенство (3.5) выполнено. Далее считаем, что $n \geq 3$.

Пусть $ax \leq a_0$ — пороговое неравенство функции $f$, для которого выполнено (3.3). Обозначим $T_{\nu j}$ $(\nu = 0,1;\ j = 1,2,\ldots,n)$ множество точек из $T_\nu(f)$, $j$-я компонента которых удовлетворяет неравенствам леммы 3.30. По лемме 3.29 множество $T_\nu(f)$ обладает свойством разделенности, поэтому тем же свойством обладают и его подмножества $T_{\nu j}$.

Используя лемму 3.31, оценим $|T_{0j}|$. При этом применим первое неравенство из леммы 3.30 и $n-2$ неравенств $0 \leq x_i \leq k-2$ $(i \neq j)$. Учитывая, что $n \geq 3$, получаем

$$|T_{0j}| \leq \left(1+\log\frac{\dfrac{a_0}{a_j}+2}{\dfrac{a_0}{na_j}-\dfrac{1}{n}+1}\right)\cdot(1+\log k)^{n-2} =$$

$$= \left(1+\log\frac{n(a_0+2a_j)}{a_0+(n-1)a_j}\right)(1+\log k)^{n-2} \leq (1+\log n)(1+\log k)^{n-2}.$$

Теперь, используя лемму 3.31, оценим $|T_{1j}|$. При этом применим второе неравенство из леммы 3.30 и $n-2$ неравенств $0 \leq x_i \leq k-1$ $(i \neq j)$. Учитывая, что $n \geq 3$, получаем

$$|T_{1j}| \leq \left(1+\log\frac{\dfrac{a_0}{a_j}+3}{\dfrac{a_0}{na_j}+1}\right)\cdot\Big(1+\log(k+1)\Big)^{n-2} =$$

$$= \left(1+\log\frac{n(a_0+3a_j)}{a_0+na_j}\right)\Big(1+\log(k+1)\Big)^{n-2} \leq (1+\log n)\Big(1+\log(k+1)\Big)^{n-2}.$$

Суммируя по $j$, получаем оценки (3.5). ∎

## 3.7. Неприводимые целочисленные точки политопов

В настоящем разделе получены верхние оценки количества неприводимых точек в полиэдре. Далее, в разделе 3.8, эти оценки используются для получения верхней оценки $\sigma(E_k^n) = O(\log^{n-2} k)$ при фиксированном $n \geq 2$.

Пусть $P$ — полиэдр в $\mathbb{R}^n$. Точка $x \in P \in \mathbb{Z}^n$ называется *неприводимой* в $P$ (а, точнее, в $P \cap \mathbb{Z}^n$), если $x$ нельзя представить в виде $x = \frac{1}{2}(y+z)$ ни для каких двух различных $y$ и $z$ из $P \cap \mathbb{Z}^n$.

Легко видеть, что любая вершина выпуклой оболочки множества $P \cap \mathbb{Z}^n$ является также неприводимой точкой в $P \cap \mathbb{Z}^n$. Обратное, в общем случае не верно. Пусть, например, $P = \{x \in \mathbb{R}^2 : \ x_1 + x_2 \geq 1, \ 2x_1 - x_2 \leq 2, \ -x_1 + 2x_2 \leq 2\}$. Точка $(1,1)$ является неприводимой в $P \cap \mathbb{Z}^n$, однако не является вершиной его выпуклой оболочки. Тем не менее, эти два свойства близки, о чем свидетельствует близость оценок на число вершин и число неприводимых точек [100].

Пусть $P$, $P_1, P_2, \ldots, P_s$ — политопы (т. е. ограниченные полиэдры) в $\mathbb{R}^n$. Если $P = \cup_{i=1}^s P_i$, то $\{P_1, P_2, \ldots, P_s\}$ называется *покрытием* политопа $P$. Если пересечение любых двух политопов в покрытии либо пусто, либо является их общей гранью, то покрытие называется *правильным разбиением*. Если все политопы в правильном разбиении — симплексы, то разбиение называется *триангуляцией*.

Основная идея нашего метода получения верхней оценки числа неприводимых точек в политопе заключается в следующем. Вначале оцениваем число неприводимых точек в параллелепипеде (см. раздел 3.7.1). В разделе 3.7.2 для произвольного политопа $P$ строим его покрытие параллелепипедами $P_1, P_2, \ldots, P_s$. Для этого сначала строится триангуляция политопа, а затем каждый симплекс триангуляции покрывается

параллелепипедами. Легко видеть, что любая неприводимая в $P \cap \mathbb{Z}^n$ точка $x$ неприводима и в $P_i \cap \mathbb{Z}^n$ для любого $i$, если $x \in P_i$. Это свойство позволяет (в разделе 3.7.3) оценить количество неприводимых точек в $P$. А именно, доказано (см. теорему 3.38), что если $P$ можно задать системой $m$ линейных неравенств и $P \cap \mathbb{Z}^n \subseteq E_k^n$, то количество неприводимых в $P \cap \mathbb{Z}^n$ точек есть $O(m^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} k)$.

### 3.7.1. Неприводимые точки в параллелепипеде

В настоящем разделе предлагаются верхние оценки количества неприводимых целых точек в параллелепипеде.

Пусть $A \in \mathbb{Z}^{n \times n}$ — невырожденная матрица, $c = (c_1, c_2, \ldots, c_n) \in \mathbb{Z}^n$, $b = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}^n$, $b < c$. Рассмотрим параллелепипед

$$P(A, b, c) = \{x \in \mathbb{R}^n : \ b \leq Ax \leq c\}.$$

Обозначим $M(A, b, c) = P(A, b, c) \cap \mathbb{Z}^n$.

**Теорема 3.33.** *Пусть $N$ — множество неприводимых точек в $M(A, b, c)$, где $A \in \mathbb{Z}^{n \times n}$ — невырожденная матрица, $c \in \mathbb{Z}^n$, $b \in \mathbb{Z}^n$, тогда*

$$|N| \leq 2 \prod_{i=1}^{n-1} \left(3 + 2 \log \left(1 + \frac{c_i - b_i}{3}\right)\right). \tag{3.6}$$

*Доказательство.* Обозначим

$$s_i = \left\lceil \log \left(1 + \frac{c_i - b_i}{3}\right) \right\rceil \qquad (i = 1, 2, \ldots, n-1). \tag{3.7}$$

Отсюда получаем

$$3 \cdot 2^{s_i - 1} - 3 < c_i - b_i \leq 3 \cdot 2^{s_i} - 3. \tag{3.8}$$

Обозначим $a^{(1)}, a^{(2)}, \ldots, a^{(n)}$ строки матрицы $A$. Пусть $j_1, j_2, \ldots, j_{n-1}$ — некоторые числа, такие, что $j_i \in \{0, \ldots, 2s_i\}$ $(i = 1, \ldots, n-1)$. Пусть

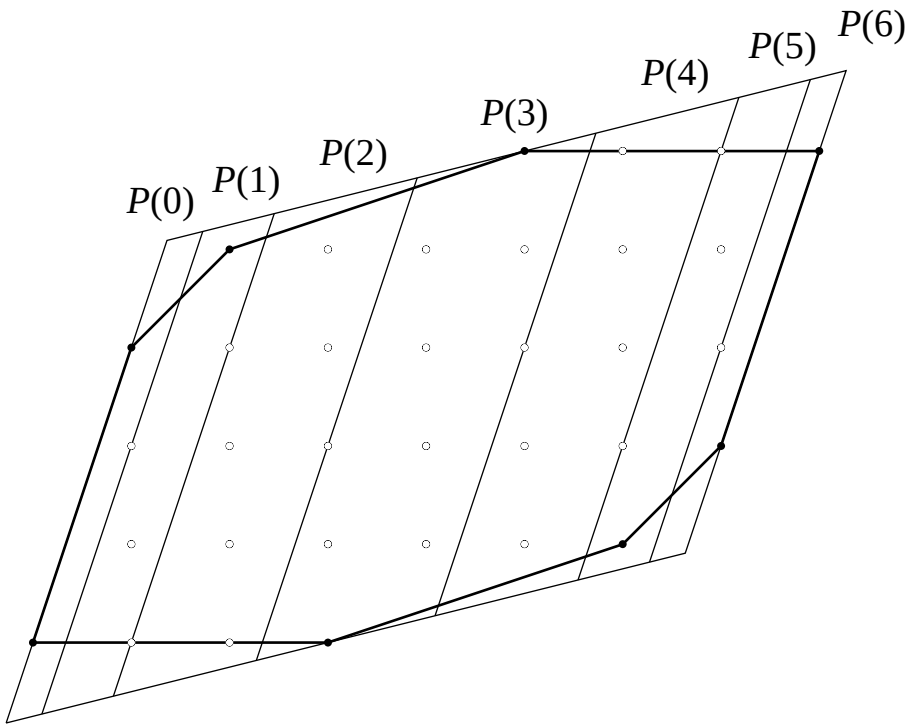


Рис. 3.4

$P(j_1, j_2, \ldots, j_{n-1})$ — множество точек из $\mathbb{R}^n$, удовлетворяющих следующим условиям: для всех $i = 1, 2, \ldots, n-1$

$$\begin{aligned} b_i + 2^{j_i} - 1 \le a^{(i)}x < b_i + 2^{j_i+1} - 1 \quad & (j_i = 0, 1, \ldots, s_i - 1), \\ b_i + 2^{j_i} - 1 \le a^{(i)}x \le c_i - 2^{j_i} + 1 \quad & (j_i = s_i), \\ c_i - 2^{j_i - s_i} + 1 < a^{(i)}x \le c_i - 2^{j_i - 1 - s_i} + 1 \quad & (j_i = s_i + 1, \ldots, 2s_i), \\ b_n \le a^{(n)}x \le c_n. & \end{aligned} \tag{3.9}$$

Легко видеть, что множество параллелепипедов $P(j_1, j_2, \ldots, j_{n-1})$, где $0 \le j_i \le 2s_i$ $(i = 1, \ldots, n-1)$, образуют покрытие параллелепипеда $P(A, b, c)$. Это иллюстрируется на рис. 3.4, где все неприводимые точки суть вершины выпуклой оболочки множества $M(A, b, c)$.

Покажем, что каждый $P(j_1, j_2, \ldots, j_{n-1})$ содержит не более 2 различных точек из $N$. Предположим противное: пусть $x, y, z$ — попарно

различные точки, $x, y, z \in P(j_1, j_2, \ldots, j_{n-1})$, причем

$$b_n \le a^{(n)}x \le a^{(n)}y \le a^{(n)}z \le c_n. \tag{3.10}$$

Возможны два случая:

$$a^{(n)}y - a^{(n)}x \le a^{(n)}z - a^{(n)}y \tag{3.11}$$

или

$$a^{(n)}y - a^{(n)}x > a^{(n)}z - a^{(n)}y. \tag{3.12}$$

В случае (3.11) рассмотрим точку $x' = 2y - x$ и покажем, что $x' \in P(A, b, c)$.

Условия $b_n \le a^{(n)}x' \le c_n$ выполнены, так как, учитывая (3.10), получаем

$$a^{(n)}x' = 2a^{(n)}y - a^{(n)}x \ge a^{(n)}y \ge b_n,$$

$$a^{(n)}x' = 2a^{(n)}y - a^{(n)}x \le 2a^{(n)}z - a^{(n)}y \le c_n.$$

Теперь проверим условия $b_i \le a^{(i)}x' \le c_i$ $(i = 1, 2, \ldots, n-1)$. Если $0 \le j_i \le s_i - 1$, то, учитывая (3.8) и (3.9), получаем

$$a^{(i)}x' \le 2(b_i + 2^{j_i+1} - 2) - (b_i + 2^{j_i} - 1) \le b_i + 3 \cdot 2^{s_i-1} - 3 < c_i,$$

$$a^{(i)}x' \ge 2(b_i + 2^{j_i} - 1) - (b_i + 2^{j_i+1} - 2) = b_i.$$

Если $j_i = s_i$, то

$$a^{(i)}x' \le 2(c_i - 2^{s_i} + 1) - (b_i + 2^{s_i} - 1) \le c_i,$$

$$a^{(i)}x' \ge 2(b_i + 2^{s_i} - 1) - (c_i - 2^{s_i} + 1) \ge b_i.$$

Если $s_i + 1 \le j_i \le 2s_i$, то

$$a^{(i)}x' \le 2(c_i - 2^{j_i-1-s_i+1} + 1) - (c_i - 2^{j_i-s_i} + 2) = c_i,$$

$$a^{(i)}x' \ge 2(c_i - 2^{j_i-s_i} + 2) - (c_i - 2^{j_i-1-s_i} + 1) \ge c_i + 3 - 3 \cdot 2^{s_i-1} > b_i.$$

Итак, $x' \in M(A,b,c)$ и $y = \frac{1}{2}(x + x')$, следовательно, $y \notin N$. Противоречие.

В случае (3.11) рассматриваем точку $z' = 2y - z$. Проводя аналогичные рассуждения, можно показать, что $z' \in M(A,b,c)$ и $y = \frac{1}{2}(z + z') \notin N$.

Итак, каждый параллелепипед $P(j_1, j_2, \ldots, j_{n-1})$ содержит не более 2 точек из $N$, поэтому $|N| \leq 2\prod_{i=1}^{n-1}(1 + 2s_i)$, откуда, используя (3.7), получаем (3.6). ∎

### 3.7.2. Покрытие политопа параллелепипедами

Наш метод покрытия политопа (т. е. ограниченного полиэдра) параллелепипедами заключается в его предварительной триангуляции, а затем покрытии параллелепипедами каждого симплекса триангуляции.

**Лемма 3.34.** ([92], см. [10, 105]) *Для произвольного $n$-мерного политопа с $m$ фасетами существует триангуляция не более чем из $n!\xi_n(m)$ симплексов.*

Следующее утверждение является уточнением результата [96].

**Лемма 3.35.** *Произвольный $n$-мерный симплекс $S$ можно покрыть не более $(n+1)\cdot\binom{n^2-2}{n-1}$ $n$-мерными параллелепипедами.*

*Доказательство.* Не нарушая общности, рассмотрим симплекс

$$S = \left\{ x \in \mathbb{R}^n : \ \sum_{j=1}^{n} x_j \leq n^2 - 1, \ x_j \geq 0 \ (j = 1, 2, \ldots, n) \right\}.$$

Рассмотрим множество

$$Y = \left\{ x \in \mathbb{Z}^n : \ \sum_{j=1}^{n} y_j \leq n^2 - 1, \ y_j \geq 1 \ (j = 1, 2, \ldots, n) \right\}.$$

Для каждого вектора $y \in Y$ рассмотрим параллелепипед

$$\Pi(y) = \{ x \in \mathbb{R}^n : \ 0 \leq x_j \leq y_j \ (j = 1, 2, \ldots, n) \}.$$

Пусть

$$S' = \left\{ x \in \mathbb{R}^n : \ \sum_{j=1}^{n} x_j \le n^2 - n, \ x_j \ge 0 \ (j = 1, 2, \ldots, n) \right\}.$$

Докажем, что

$$S' \subseteq \bigcup_{y \in Y} \Pi(y) \subseteq S. \tag{3.13}$$

Второе включение очевидно. Для доказательства первого включения рассмотрим произвольный вектор $x \in S'$. Пусть $z = \lceil x \rceil$. Тогда

$$\sum_{j=1}^{n} z_j = \sum_{j=1}^{n} \lceil x_j \rceil < n^2 - n + n = n^2.$$

Учитывая, что все компоненты вектора $z$ целые, получаем

$$\sum_{j=1}^{n} z_j \le n^2 - 1.$$

Увеличивая (при необходимости) компоненты вектора $z$, получим вектор $y \in Y$, такой, что $z \in \Pi(y)$ и, следовательно, $x \in \Pi(y)$.

Итак, мы построили семейство параллелепипедов $\{\Pi(y) : \ y \in Y\}$, удовлетворяющих (3.13) и содержащих определенную вершину (вершину $o$) симплекса $S$. Выполняя аналогичные построения для каждой вершины симплекса, получим его покрытие.

Действительно, пусть $v_0, v_1, \ldots, v_d$ — вершины симплекса $S$, причем $v_0 = o$, а при $i \ge 1$ все компоненты вектора $v_i$ равны 0, кроме $i$-й, равной $n^2 - 1$. Для произвольной точки $x \in S$ найдутся числа $\alpha_0, \alpha_1, \ldots, \alpha_d$, такие, что

$$x = \sum_{i=0}^{n} \alpha_i v_i, \qquad \sum_{i=0}^{n} \alpha_i = 1, \qquad \alpha_i \ge 0 \qquad (i = 0, 1, \ldots, n).$$

Не нарушая общности, будем считать, что $\alpha_0 \ge \frac{1}{n+1}$, поэтому

$$\sum_{i=1}^{n} \alpha_i \le \frac{n}{n+1},$$

откуда

$$\sum_{j=1}^{n} x_j = (n^2-1)\sum_{i=1}^{n} \alpha_i \le n^2 - n.$$

Таким образом, $x \in S'$. Теперь из (3.13), получаем, что построенное семейство из $(n+1)|Y| = (n+1)\binom{n^2-2}{n-1}$ параллелепипедов образует покрытие симплекса. ∎

**Лемма 3.36.** *Пусть политоп $P$ задан как множество решений системы неравенств $Ax \le b$, где $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$, $b = (b_i) \in \mathbb{Z}^m$, $|a_{ij}| \le \alpha$, $|b_i| \le \beta$, тогда существует покрытие этого политопа не более чем*

$$\eta_n(m) = n!\,\xi_n(m)\,(n+1)\binom{n^2-2}{n-1} \tag{3.14}$$

*параллелепипедами $\Pi_\mu = \{x \in \mathbb{R}^n : b^{(\mu)} \le A^{(\mu)}x \le c^{(\mu)}\}$ $(\mu = 1, \ldots, \eta_n(m))$, где $A^{(\mu)} \in \mathbb{Z}^{n\times n}$, $b^{(\mu)} = (b_i^{(\mu)}) \in \mathbb{Z}^n$, $c^{(\mu)} = (b_i^{(\mu)}) \in \mathbb{Z}^n$, такими, что*

$$|c_i^{(\mu)} - b_i^{(\mu)}| \le 2\alpha^{n^2}\beta^n(\sqrt{n})^{n^2+2n+2}. \tag{3.15}$$

*Доказательство.* Требуемое покрытие построим следующим образом. Вначале политоп $P$ триангулируем согласно лемме 3.34, затем по лемме 3.35 построим покрытие параллелепипедами каждого симплекса в построенной триангуляции. Верхняя оценка (3.14) на общее число параллелепипедов получается как произведение верхней границы количества сиплексов в триангуляции и количества параллелепипедов в покрытии симплекса.

Теперь получим неравенство (3.15). Вначале оценим величину коэффициентов систем неравенств, которыми можно описать симплексы в триангуляции. Хорошо известно, что компоненты каждой вершины $v$ политопа $P$ (и, следовательно, симплексов в его триангуляции) можно получить, обращая соответствующие $n$ неравенств системы $Ax \le b$ в равенства. Из правила Крамера и неравенства Адамара (см., например,

[60]) получаем, что $v = 1/q \cdot (p_1, p_2, \ldots, p_n)$, где $p_j \in \mathbb{Z}$ $(j = 1, 2, \ldots, n)$, $q \in \mathbb{Z}$.

$$|q| \leq \alpha^n (\sqrt{n})^n, \qquad |p_j| \leq \alpha^{n-1}\beta(\sqrt{n})^n \qquad (j = 1, 2, \ldots, n). \tag{3.16}$$

Если $v^{(1)}, v^{(2)}, \ldots, v^{(n)}$ — некоторые вершины симплекса, причем

$$v^{(i)} = \frac{1}{q^{(i)}} \cdot (p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}),$$

то коэффициенты уравнения $a_1x_1 + a_2x_2 + \ldots a_nx_n = a_0$, определяющего гиперплоскость, проходящую через эти вершины, можно можно вычислить по формулам:

$$a_0 = \det(p_1, p_2, \ldots, p_n),$$

$$a_j = (-1)^{j+1} q_j \det(\mathbf{1}, p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n) \qquad (j = 1, 2, \ldots, n),$$

где $\mathbf{1}$ — столбец из единиц. Из неравенства Адамара, используя (3.16), теперь получаем:

$$|a_0| \leq \left((\alpha\sqrt{n})^{n-1}\beta\sqrt{n} \cdot \sqrt{n}\right)^n = \alpha^{n(n-1)}\beta^n(\sqrt{n})^{n^2+n},$$

$$|a_j| \leq (\alpha\sqrt{n})^n \sqrt{n} \left((\alpha\sqrt{n})^{n-1}\beta\sqrt{n} \cdot \sqrt{n}\right)^{n-1} = \alpha^{n^2-n+1}\beta^{n-1}(\sqrt{n})^{n^2+n}, \tag{3.17}$$

что дает оценки на величину коэффициентов систем неравенств, описывающих симплексы в триангуляции.

Теперь перейдем к оценке коэффициентов $c_i^{(\mu)}$, $b_i^{(\mu)}$ систем неравенств, описывающих параллелепипеды в покрытии симплексов. Заметим, что метод построения покрытия, описанный в лемме 3.35, дает параллелепипеды, грани которых параллельны граням соответствующих симплексов, следовательно, коэффициенты левой части уравнений этих граней, т. е. коэффициенты матриц $A^{(\mu)}$, удовлетворяют неравенству

(3.17). Для оценивания $b_i^{(\mu)}|$, $|c_i^{(\mu)}|$ подставим координаты вершины $v$ симплекса в уравнение грани. Из (3.16) и (3.17) вытекает

$$|b_i^{(\mu)}| \le n \cdot \alpha^{n-1}\beta(\sqrt{n})^n \cdot \alpha^{n^2-n+1}\beta^{n-1}(\sqrt{n})^{n^2+n} = \alpha^{n^2}\beta^n(\sqrt{n})^{n^2+2n+2}.$$

Такое же неравенство справедливо и для $|c_i^{(\mu)}|$, откуда получаем (3.15). ∎

### 3.7.3. Неприводимые точки в политопе

Здесь на основе результатов разделов 3.7.2, 3.7.1 мы получим оценку числа неприводимых целых точек в произвольном политопе.

**Теорема 3.37.** *Пусть политоп $P$ задан как множество решений системы неравенств $Ax \le b$, где $A = (a_{ij}) \in \mathbb{Z}^{m\times n}$, $b = (b_i) \in \mathbb{Z}^m$, $|a_{ij}| \le \alpha$, $|b_i| \le \beta$. Пусть $N$ — множество неприводимых точек в $P \cap \mathbb{Z}^n$, тогда*

$$|N| \le 2n!\,\xi_n(m)\,(n+1)\binom{n^2-2}{n-1}\left(3 + 2\log\left(1 + \frac{2}{3}\alpha^{n^2}\beta^n n^{\frac{n^2+2n+2}{2}}\right)\right)^{n-1}. \tag{3.18}$$

*Доказательство.* По лемме 3.36 построим покрытие политопа $P$ параллелепипедами. Очевидно, что $N$ содержится в объединении множеств неприводимых целых точек во всех параллелепипедах. Оценить количество неприводимых точек в параллелепипеде позволяет теорема 3.33. Подставляя (3.15) в (3.6) и умножая полученный результат на $\eta_n(m)$ из (3.14), получаем неравенство (3.18). ∎

**Теорема 3.38.** *Пусть $A \in \mathbb{R}^{m'\times n}$, $b \in \mathbb{R}^{m'}$, $P = \{x \in \mathbb{R}^n : Ax \le b\}$, причем $P \cap \mathbb{Z}^n \subseteq E_k^n$. Если $N$ — множество неприводимых точек в $P \cap \mathbb{Z}^n$, тогда для $|N|$ справедливо неравенство (3.18), где $m = m' + 2n$,*

$$\alpha \le \frac{(k-1)^{n-1}(n+1)^{\frac{n+1}{2}}}{2^n}, \qquad \beta \le \frac{(k-1)^n(n+2)^{\frac{n+2}{2}}}{2^{n+1}}.$$

*Доказательство.* Для неравенства $ax \le a_0$, где $a \in \mathbb{R}^n$, $a_0 \in \mathbb{R}$ рассмотрим систему из $k^n + 1$ однородных линейных неравенств относительно неизвестных $b_0 \in \mathbb{R}$, $b \in \mathbb{R}^n$, $b_{n+1} \in \mathbb{R}$:

$$\begin{cases} b_0 - bx \ge 0 & \text{для всех } x, \text{ таких, что } ax \le a_0, \\ -b_0 + bx - b_{n+1} \ge 0 & \text{для всех } x, \text{ таких, что } ax > a_0, \\ b_{n+1} \ge 0. \end{cases} \tag{3.19}$$

Множество $K$ ее решений есть полиэдральный (многогранный) конус в $\mathbb{R}^{n+2}$. Очевидно, что любой вектор, принадлежащий $K$, при $b_{n+1} > 0$ имеет компоненты $b_0$, $b$, $b_{n+1}$, такие, что $\{x \in E_k^n : \ ax \le a_0\} = \{x \in E_k^n : \ bx \le b_0\}$.

Докажем, что конус $K$ острый, т. е. не содержит ненулевых подпространств. Предположим, что оба вектора $\pm(b_0, b, b_{n+1})$ принадлежат $K$. Из последнего неравенства в (3.19) получаем тогда, что $b_{n+1} = 0$, откуда из остальных неравенств следует $bx = b_0$ для всех $x \in E_k^n$. Так как $k \ge 2$, то аффинная размерность множества $E_k^n$ равна $n$, поэтому $b_0 = b = b_{n+1} = 0$. Итак, $K$ не содержит ненулевых подпространств.

Из теории систем линейных неравенств (см., например, [88]) теперь вытекает, что множество экстремальных векторов $g^{(1)}, g^{(2)}, \ldots, g^{(s)}$ конуса $K$ образует ее порождающую систему, т. е. $K = \mathrm{Cone}\{g^{(1)}, g^{(2)}, \ldots, g^{(s)}\}$. Более того, для каждого $i = 1, 2, \ldots, s$ найдется подсистема системы (3.19), обращающаяся на векторе $g^{(i)}$ в систему равенств, причем коэффициенты этой подсистемы образуют матрицу $T_i$ ранга $n + 1$. Отсюда получаем, что $g^{(i)}$ может быть выбран целочисленным, причем его $j$-я компонента с точностью до знака будет равна минору $(n+1)$-го порядка, получающемуся вычеркиванием $j$-го столбца из матрицы $T_i$.

Оценим величину этого минора. Умножая на $-1$ его строки, соответствующие $x$, для которых $ax > a_0$, а также столбцы, соответствующие переменным $b$, получим минор с неотрицательными элементами.

Воспользовавшись известной оценкой определителя с неотрицательными компонентами (см., например, [60]), получаем следующие оценки величины компонент вектора $g^{(i)} = (g_0^{(i)}, g_1^{(i)}, \ldots, g_n^{(i)}, g_{n+1}^{(i)})$:

$$|g_0^{(i)}| \le \frac{(k-1)^n (n+2)^{\frac{n+2}{2}}}{2^{n+1}}, \quad |g_j^{(i)}| \le \frac{(k-1)^{n-1}(n+1)^{\frac{n+1}{2}}}{2^n} \quad (j = 1, \ldots, n).$$

Среди векторов $g^{(1)}, g^{(2)}, \ldots, g^{(s)}$ найдется вектор $(b_0, b, b_{n+1})$, для которого $b_{n+1} > 0$. Неравенство $bx \le b_0$ назовем приближением к неравенству $ax \le a_0$.

Все неравенства, определяющие $P$, заменим на их приближения и добавим $2n$ неравенств $0 \le x_j \le k-1$ $(k = 1, 2, \ldots, n)$. Доказываемое неравенство следует теперь из теоремы 3.37. ∎

Заметим, что оценки мощности $|N|$ в теоремах 3.37 и 3.38 при фиксированном $n$ имеют соответственно вид

$$|N| = O\left(m^{\lfloor \frac{n}{2} \rfloor} \log^{n-1}(\alpha\beta)\right), \quad |N| = O(m^{\lfloor \frac{n}{2} \rfloor} \log^{n-1} k).$$

## 3.8. Верхние оценки длины обучения в классе пороговых функций

В настоящем разделе найдем неулучшаемую верхнюю оценку длины обучения в классе пороговых функций.

**Теорема 3.39.** *При любом фиксированном* $n \ge 2$

$$\sigma(E_k^n) = O(\log^{n-2} k) \qquad (k \to \infty).$$

*Доказательство.* Не нарушая общности, предположим, что коэффициенты порогового неравенства функции $f \in \mathfrak{T}(E_k^n)$ удовлетворяют неравенствам $a_1 \ge a_2 \ge \cdots \ge a_n \ge 0$.

Если $a_0 \leq (k-1)a_n$, то из теоремы 3.32 следует, что $|T(f)| = O(\log^{n-2} k)$. Рассмотрим случай, когда $a_0 > (k-1)a_n$. Если $e_n \notin K(f)$, то из $x \in T_\nu(f)$ следует $x_n = 0$ или $x_n = k-1$, поэтому $|T_\nu(f)| \leq 2\sigma(n-1,k)$.

Обозначим через $e_j$ вектор, все компоненты которого равны 0, кроме $j$-й, равной 1. Пусть $e_n \in K(f)$. Положим

$$T_0'(f) = \{x \in T_0(f) : \sum_{j=1}^{n-1} a_j x_j \leq a_0 - (k-1)a_n\},$$

$$T_0''(f) = \{x \in T_0(f) : \sum_{j=1}^{n-1} a_j x_j > a_0 - (k-1)a_n\},$$

$$T_1'(f) = \{x \in T_1(f) : \sum_{j=1}^{n-1} a_j x_j > a_0\},$$

$$T_1''(f) = \{x \in T_1(f) : \sum_{j=1}^{n-1} a_j x_j \leq a_0\}.$$

Если $x \in T_\nu'(f)$ $(\nu = 0,1)$, то $x_n = 0$ или $x_n = k-1$, следовательно, $|T_\nu'(f)| \leq 2\sigma(n-1,k)$.

Пусть

$$P = \left\{ x \in E_k^n : \ a_0 - (k-1)a_n < \sum_{j=1}^{n-1} a_j x_j \leq a_0, \ x_n = 0 \right\}.$$

Если $y \in P$, то учитывая, что $e_n \in K(f)$, получаем:

$$\{y + \alpha e_n : \ \alpha \in Z\} \subset R_0(f) \cup R_1(f).$$

Поэтому, согласно следствию 3.28, $|T_\nu''(f)|$ не превосходит количества неприводимых точек в $P$. Поскольку размерность полиэдра $\operatorname{Conv} P$ не выше $n-1$, то по теореме 3.38 количество неприводимых точек в $P$ при фиксированном $n$ есть $O(\log^{n-2} k)$. ∎

Объединяя нижнюю (теорема 3.17) и верхнюю (теорема 3.39) оценки длины обучения, получаем

**Следствие 3.40.** *При фиксированном* $n \geq 2$

$$\sigma(E_k^n) = \Theta(\log^{n-2} k) \quad (k \to \infty).$$

В [117] исследуется средняя мощность $\overline{\sigma}(E_2^n)$ минимального разрешающего множества пороговой функции двух переменных. В частности, доказано, что

$$\overline{\sigma}(E_2^n) \leq \log |\mathfrak{T}(E_2^n)| < n^2.$$

Аргументы из [117] можно обобщить (см. [12]) на случай произвольного $M$. Таким образом,

$$\overline{\sigma}(M) \leq \log |\mathfrak{T}(M)|.$$

В частности, учитывая оценки из раздела 1.4, получаем для произвольного $k \geq 2$

$$\overline{\sigma}(E_k^n) \leq \log |\mathfrak{T}(E_k^n)| < n^2 \log k.$$

Ю. А. Зуев [38] ввел понятие *графа* (булевых) *пороговых функций*. Это понятие легко обобщается на случай пороговых функций $k$-значной логики, а также на любой другой класс $\mathfrak{F}' \subseteq \mathfrak{F}(M)$). Пусть $f \in \mathfrak{F}(M)$, $g \in \mathfrak{F}(M)$,

$$\operatorname{dist}(f, g) = |\{x \in M : \ f(x) \neq g(x)\}|.$$

*Графом класса* $\mathfrak{F}'$ называется простой граф, в котором множество вершин есть $\mathfrak{F}'$, а $\{f, g\}$ является ребром тогда и только тогда, когда $\operatorname{dist}(f, g) = 1$.

Среди задач, связанных с пороговыми функциями и представляющими наибольший интерес, Ю. А. Зуев [38] называет исследование свойств графа пороговых функций. Результаты, касающиеся $\sigma(M)$ и $\overline{\sigma}(M)$ можно интерпретировать в этих терминах: $\sigma(M)$ есть максимальная, а $\overline{\sigma}(M)$ — средняя степень вершины графа.

## 3.9. Построение минимального разрешающего множества пороговой функции

В этом разделе предлагается алгоритм нахождения минимального разрешающего множества $T(f)$ пороговой функции $f \in \mathfrak{T}(M)$, где $M = P \cap \mathbb{Z}^n$, по известным коэффициентам порогового неравенства (1.2) и по известной системе, описывающей политоп $P$. Далее будет показано, как изменить алгоритм $\mathscr{A}_1$, чтобы сложность нового алгоритма $\mathscr{A}_1^{\circ}$ отличалась бы от сложности оптимального (по числу обращений к оракулу в худшем случае) алгоритма расшифровки не более, чем в $O\left(n^3 \log(n\gamma)\right)$ раз. Для класса $\mathfrak{T}(E_k^n)$ сложность алгоритма $\mathscr{A}_1^{\circ}$ отличается от сложности оптимального алгоритма не более, чем в $O\left(n^2 \log(nk)\right)$ раз и при фиксированном $n \geq 2$

$$\tau(E_k^n) \leq \tau(\mathscr{A}_1^{\circ}) = O(\log^{n-1} k).$$

Рассмотрим задачу $\mathfrak{G}_2$ определения множеств $T_\nu(f)$ $(\nu = 0, 1)$ для функции $f \in \mathfrak{T}(M)$, $M = P \cap \mathbb{Z}^n$, по заданным коэффициентам $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ порогового неравенства (1.2) функции $f$ и заданным коэффициентам целочисленной системы линейных неравенств, описывающей политоп $P$. Пусть $\alpha = \max\{a_0, \ldots, a_n\}$, тогда справедлива

**Теорема 3.41.** *При любом фиксированном* $n$ *существует полиномиальный от* $\log\alpha$, $\log\gamma$, $l$ *алгоритм решения задачи* $\mathfrak{G}_2$.

*Доказательство.* Для решения задачи $\mathfrak{G}_2$ с помощью алгоритма из леммы 1.21 найдем множества крайних точек $N_0(f)$ и $N_1(f)$. При фиксированном $n$ это можно сделать с полиномиальной от $\log\alpha$, $\log\gamma$, $l$ трудоемкостью. По лемме 3.10 $T_\nu(f) \subseteq N_\nu(f)$ $(\nu = 0, 1)$, следовательно, для нахождения $T(f)$ необходимо из системы (1.7) исключить все неравенства–следствия. Из утверждения 1.18 и леммы 1.7 следует, что число

неравенств в системе (1.7) и коэффициенты этой системы при любом фиксированном $n$ ограничены полиномами от $l$ и $\log\gamma$. Для завершения доказательства теоремы осталось заметить, что выделить в (1.7) минимальную эквивалентную подсистему при фиксированном $n$ можно за полиномиальное от $l$ и $\log\gamma$ число шагов (см. [81], а также раздел 1.6). ∎

По следствию 1.10 для любой $f \in \mathfrak{T}(M)$ существует такое пороговое неравенсто, что $\log\alpha$ при фиксированном $n$ ограничен полиномом от $\log\gamma$. При условии, что на вход задачи $\mathfrak{G}_2$ подается пороговое неравенство, удовлетворяющее этому условию, алгоритм из теоремы 3.41 при любом фиксированном $n$ полиномиален от $\log\gamma$ и $l$.

В алгоритме $\mathscr{A}_1$ заменим шаг 2 на шаг 2′. Полученный таким образом алгоритм обозначим через $\mathscr{A}_1^{\mathrm{o}}$.

Шаг 2′. (Проверить гипотезу.) Найдем множества $T_\nu^{(i)} = T_\nu(f_i)$ $(\nu = 0, 1)$ для функции $f_i$, заданной пороговым неравенством $\sum\limits_{j=1}^{n} x_j a_j^{(i)} \leq 1$. Для каждого $\nu = 0, 1$ и каждого $x \in T_\nu^{(i)}$ выполним следующие действия: с помощью оракула найдем $f(x)$; если $f(x) = 1 - \nu$ (т. е. $f(x) \neq f_i(x)$), то присоединим $x$ к $S_\nu$. Если точек $x$, таких, что $x \in T_\nu^{(i)}$, $f(x) = 1 - \nu$, не нашлось, т. е. $f(x) = f_i(x)$ для всех $x \in T_0^{(i)} \cup T_1^{(i)}$, то стоп: $a^{(i)} \in W(f)$, процесс расшифровки закончен. В противном случае увеличим $i$ на 1 и перейдем на шаг 1.

Так как множество $T^{(i)} = T_0^{(i)} \cup T_1^{(i)}$ является разрешающим для $f_i$, то процесс расшифровки заканчивается тогда и только тогда, когда $f \equiv f_i$, в противном случае найдется некоторый $x \in T_\nu^{(i)}$, такой, что $f(x) = 1 - \nu$ и итерация повторится.

Таким образом, алгоритм $\mathscr{A}_1^{\mathrm{o}}$ расшифровывает любую функцию из класса $\mathfrak{F}_+(M)$. Все оценки вычислительной трудоемкости и сложности

переносятся на этот случай. Заметим, что на вход задачи $\mathfrak{G}_2$ подаются рациональные коэффициенты $a_j^i$ порогового неравенства, между тем, как в теореме 3.41 они должны быть целыми. Полученное пороговое неравенство, однако, домножением его коэффициентов на их наименьшее общее кратное легко преобразуется к требуемому виду. В обоих случаях длина двоичной записи этих коэффициентов при фиксированном $n$ будет ограничена полиномом от $l$ и $\log\gamma$.

Пусть $\mathfrak{P}(n,\gamma)$ — множество политопов $P \subseteq \mathbb{R}^n$, каждый из которых можно задать системой линейных неравенств с целочисленными коэффициентами, ограниченными по абсолютной величине числом $\gamma$. Пусть $\mathscr{A}^*$ — оптимальный алгоритм расшифровки функций из класса $\mathfrak{T}(M)$, т. е. $\tau(\mathscr{A}^*) = \tau(M)$. Рассмотрим величину $\tau(\mathscr{A}_1^{\mathrm{o}})/\tau(M)$, показывающую, во сколько раз сложность алгоритма $\mathscr{A}_1^{\mathrm{o}}$ отличается от сложности оптимального алгоритма $\mathscr{A}^*$. Так как $\tau(\mathscr{A}_1^{\mathrm{o}}) \le S_{\max}\sigma(M)$, где величина $S_{\max}$ выражает верхнюю границу числа гипотез в алгоритме $\mathscr{A}_1^{\mathrm{o}}$ и определяется формулой (2.10), и по утверждению 3.1 $\tau(M) \ge \sigma(M)$, то из (2.11) получаем

**Следствие 3.42.** *Для $P \in \mathfrak{P}(n,\gamma)$ и $M = P \cap \mathbb{Z}^n$ справедливо соотношение*

$$\frac{\tau(\mathscr{A}_1^{o})}{\tau(M)} = O(n^3 \log(n\gamma)).$$

Оценим $S_{\max}$ для случая пороговых функций $k$-значной логики. Как и в лемме 2.6, для функции $f \in \mathfrak{T}(E_k^n)$ получаем:

$$\operatorname{Vol} W(f) \ge \frac{1}{(a_0+1)^n n^n k^n}.$$

Из леммы 1.11 имеем $|a_0| \le (n+1)^{1+n/2} 2^{-n-1}(k-1)^{n-1}$. Последняя величина при $k \ge 2$ и достаточно большом $n$ превосходит $n$. Следовательно, начиная с некоторого $n$, выполняется неравенство

$$\operatorname{Vol} W(f) \ge \frac{2^{n^2+n}}{e(n+1)^{n^2/2+n}(k-1)^{n^2-n} n^n k^n}.$$

С другой стороны, $\operatorname{Vol} W_0 \leq 6^n(n+1)^{n^2/2+n}2^{-n^2-n}(k-1)^{n^2-n}$. Таким образом,

$$S_{\max} \lesssim \frac{n^2 \log n + 2n^2 \log k}{\log \dfrac{e}{e-1}},$$

откуда получаем

**Следствие 3.43.** *Справедливо соотношение*

$$\frac{\tau(\mathscr{A}_1^o)}{\tau(E_k^n)} = O\big(n^2 \log(nk)\big).$$

В частности, при любом фиксированном $n$ алгоритм $\mathscr{A}_1^{\mathrm{o}}$ отличается от оптимального не более, чем в $O(\log k)$ раз.

Учитывая верхнюю оценку $\sigma(E_k^n) = O(\log^{n-2} k)$ из теоремы 3.39, получаем

**Следствие 3.44.** *При любом фиксированном $n \geq 2$*

$$\tau(\mathscr{A}_1^o) = O(\log^{n-1} k).$$

## 3.10. Минимальное разрешающее множество пороговой функции двух переменных

В настоящем разделе исследуется строение и мощностные свойства минимального разрешающего множества пороговой функции, зависящей от двух переменных. В разделе 3.10.1 устанавливается асимптотическое равенство $\tau(E_k^2) \asymp \log k$ (при $k \to \infty$) и доказывается, что $\sigma(E_k^2) = 4$ при $k \geq 2$. В разделе 3.10.2 мы исследуем среднее значение мощности минимального разрешающего множества для функций из $\mathfrak{T}(E_k^2)$. Геометрические следствия этих результатов получены в разделе 3.10.3.

### 3.10.1. Мощность разрешающего множества

**Следствие 3.45.** *Справедливы следующие асимптотические неравенства:*

$$4\log k \lesssim \tau(E_k^2) \lesssim 6\log k \qquad (k \to \infty).$$

*Доказательство.* Верхнюю оценку дает алгоритм $\mathscr{A}_2$ из теоремы 2.17. Нижняя оценка следует из неравенства (1.18) и утверждения 3.2. ∎

**Лемма 3.46.** *Выпуклый четырехугольник* $\Phi \subset \mathbb{R}^2$ *с целочисленными вершинами, не содержащий других целочисленных точек, является параллелограммом.*

*Доказательство.* Пусть $R_0, R_1, R_2, R_3$ — вершины четырехугольника $\Phi$ (в положительном направлении обхода). Определим $a = R_1 - R_0$, $b = R_3 - R_0$, $c = R_2 - R_0$. Так как $\Phi$ не содержит внутренних целочисленных точек, то по формуле Пика (лемма 2.12)

$$|\det(a,b)| = |\det(a,c)| = |\det(c,b)| = 1. \tag{3.12}$$

Отсюда в частности получаем, что каждая из систем векторов $\{a,b\}$, $\{a,c\}$ и $\{c,b\}$ является базисом решетки $\mathbb{Z}^2$ и поэтому найдутся такие $\alpha,\beta \in \mathbb{Z}$, что $c = \alpha a + \beta b$. Так как система $\{R_i : \ i = 0,\dots,3\}$ выпукло не зависима, то $\alpha,\beta \in \mathbb{N}$. Площадь четырехугольника $\Phi$, очевидно, равна $\frac{1}{2}|\det(a,c) + \det(c,b)|$. Применяя свойства определителя, получаем: $\det(a,c) + \det(c,b) = (\alpha+\beta)\det(a,b)$. Равенство (3.12) приводит к соотношению $\alpha + \beta = 2$. Так как $\alpha,\beta \in \mathbb{N}$, то $\alpha = \beta = 1$, $c = a + b$, то получаем, что $\Phi$ — параллелограмм. ∎

Прямую $L$ будем называть *разделяющей* для функции $f \in \mathfrak{T}(E_p \times E_q)$, если для некоторого $\nu \in \{0,1\}$ и для одной из открытых полуплоскостей $\Pi'$, на которые делит прямая $L$ всю плоскость $\mathbb{R}^2$, выполняется равенство

$M_\nu(f) = (\Pi' \cup L) \cap E_p \times E_q$. Из теоремы 3.11 получаем, что в $T_\nu(f)$ ($\nu = 0, 1$) войдут те и только те вершины многоугольника $P_\nu(f)$, для которых найдется проходящая через них опорная к $P_\nu(f)$ прямая, являющаяся также разделяющей для функции $f$. В частности, множеству $T_\nu(f)$ будут принадлежать все вершины многоугольника $P_\nu(f)$, инцидентные сторонам, таким, что проходящая через них прямая — разделяющая для $f$.

**Теорема 3.47.** *При $p \geq 2$, $q \geq 2$ справедливо равенство $\sigma(E_p \times E_q) = 4$.*

*Доказательство.* Если $f \equiv \nu$ для некоторого $\nu \in \{0, 1\}$, то по утверждению 3.14 имеем $\sigma(f) = 4$. Покажем, что для любой другой функции $f \in \mathfrak{T}(E_p \times E_q)$ выполняется неравенство $\sigma(f) \leq 4$. Если $f \in \mathfrak{T}(E_p \times E_q)$ не равна тождественно константе, то найдутся две стороны прямоугольника $E_p \times E_q$, в концах которых функция принимает различные значения (см. шаг 1 в описании алгоритма $\mathscr{A}_2$). Далее, на каждой из этих сторон найдется пара соседних целочисленных точек $R_0, R_1$ и $R_2, R_3$ соответственно, таких, что $f(R_0) = f(R_3) = \nu$, $f(R_1) = f(R_2) = 1 - \nu$. Если $R_0 = R_3$, то, очевидно, $R_0$ — вершина квадрата $E_p \times E_q$ и $T_\nu(f) = \{R_0\}$, $T_{1-\nu}(f) = \{R_1, R_2\}$. Если $R_1 = R_2$, то $R_1$ — вершина квадрата $E_p \times E_q$ и $T_\nu(f) = \{R_0, R_3\}$, $T_{1-\nu}(f) = \{R_1\}$. В обоих случаях $\sigma(f) = 3$. Если четырехугольник $R_0R_1R_2R_3$ не содержит внутренних целочисленных точек, то, очевидно, $T(f) = \{R_0, R_1, R_2, R_3\}$ и $\sigma(f) = 4$.

Рассмотрим случай, когда $R_0R_1R_2R_3$ содержит внутренние целочисленные точки. Мы докажем, что возможны лишь 2 случая:

а) для каждого $\nu = 0, 1$ существует ровно одна сторона многоугольника $P_\nu(f)$, разделяющая множества $M_0(f)$, $M_1(f)$;

б) для некоторого $\nu \in \{0, 1\}$ найдется две стороны многоугольника $P_\nu(f)$, каждая из которых разделяет $M_0(f)$, $M_1(f)$, при этом в $P_{1-\nu}(f)$ таких сторон нет.

Возможны два варианта:

1) для каждого $\nu = 0, 1$ выполнено $|T_\nu(f)| \geq 2$;

2) для некоторого $\nu \in \{0, 1\}$ выполнено $|T_{1-\nu}(f)| = 1$.

Рассмотрим каждый из них.

1) Для каждого $\nu = 0, 1$ имеем $|T_\nu(f)| \geq 2$. В этом случае докажем, что $|T_\nu(f)| = 2$ ($\nu = 0, 1$).

   Предположим противное: пусть для некоторого $\nu \in \{0, 1\}$ выполнено $|T_\nu(f)| \geq 3$. Из теоремы 3.11 тогда следует, что в многоугольнике $P_\nu(f)$ найдутся две смежные стороны $L_1$, $L_2$, а в $P_{1-\nu}(f)$ — по крайней мере одна сторона $L_3$, такие, что прямые, проходящие через них, разделяют множества $M_\nu(f)$ и $M_{1-\nu}(f)$ (см. рис. 3.5). Общую вершину сторон $L_1$, $L_2$ обозначим через $R_4$. Очевидно, $R_4 \in T_\nu(f)$. Соседние с $R_4$ целочисленные точки, лежащие на $L_1$ и $L_2$ обозначим соответственно через $R_5, R_6$. Так как $L_1$ и $L_2$ — стороны многоугольника $P_\nu(f)$, то $R_5, R_6 \in E_p \times E_q$.

   Рассмотрим произвольную пару $R_7, R_8$ соседних целочисленных точек на стороне $L_3$. $\mathrm{Conv}\{R_4, R_5, R_7, R_8\}$ не содержит внутренних целочисленных точек и по лемме 3.46 является либо параллелограммом, либо треугольником. В последнем случае, очевидно, одна из прямых, $L_1$ или $L_3$, не является разделяющей для множеств $M_\nu(f)$ и $M_{1-\nu}(f)$. Следовательно, $\mathrm{Conv}\{R_4, R_5, R_7, R_8\}$ — параллелограмм. Аналогично $\mathrm{Conv}\{R_4, R_6, R_7, R_8\}$ не содержит внутренних целочисленных точек, а значит является параллелограммом. Получаем, что $R_4 \in [R_5, R_6]$, что не возможно, так как $R_4 \in T_\nu(f)$. Таким образом, предположение $|T_\nu(f)| \geq 3$ не верно.

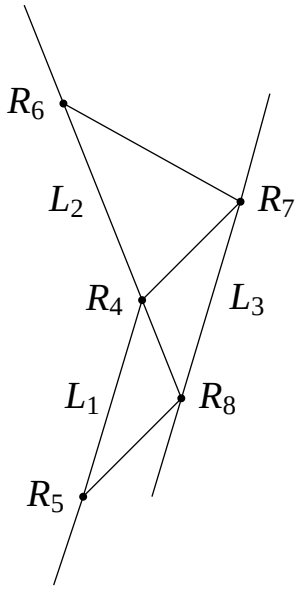


Рис. 3.5

2) Пусть теперь для некоторого $\nu \in \{0, 1\}$ выполнено $|T_{1-\nu}(f)| = 1$. Докажем, что тогда $T_\nu(f) \leq 3$. Предположив противное, получаем, что в $P_\nu(f)$ найдутся стороны $L_1, L_2, L_3$, такие, что $L_1, L_2$ и соответственно $L_1, L_3$ — смежные и, кроме того, каждая из прямых $L_1, L_2, L_3$ разделяет множества $M_\nu(f)$ и $M_{1-\nu}(f)$ (см. рис. 3.6). Пусть $R_4$, $R_5$ являются общими вершинами сторон $L_1, L_2$ и $L_1, L_3$ соответственно, $R_6$ — соседняя с $R_4$ по стороне $L_2$ целочисленная точка, $R_7$ — соседняя с $R_5$ по стороне $L_3$ целочисленная точка, $T_{1-\nu}(f) = \{R_8\}$, $L_4, L_5$ — стороны многоугольника $P_{1-\nu}(f)$, инцидентные вершине $R_8$, а $R_9, R_{10}$ — целочисленные точки, соседние с $R_8$ по сторонам $L_4$ и $L_5$ соответственно (см. рис. 3.6). Так как $P_\nu(f)$ — выпуклый, а $L_2$ и $L_3$ — прямые, разделяющие множества $M_\nu(f)$, $M_{1-\nu}(f)$, то по крайней мере один из многоугольников $R_4R_8R_9R_6$ или $R_5R_7R_{10}R_8$ выпуклый и не содержит внутренних целочисленных точек. Пусть, для определенности, этот многоугольник — $R_4R_8R_9R_6$. По лемме 3.46 он является параллелограммом и, следовательно, стороны $L_2$,

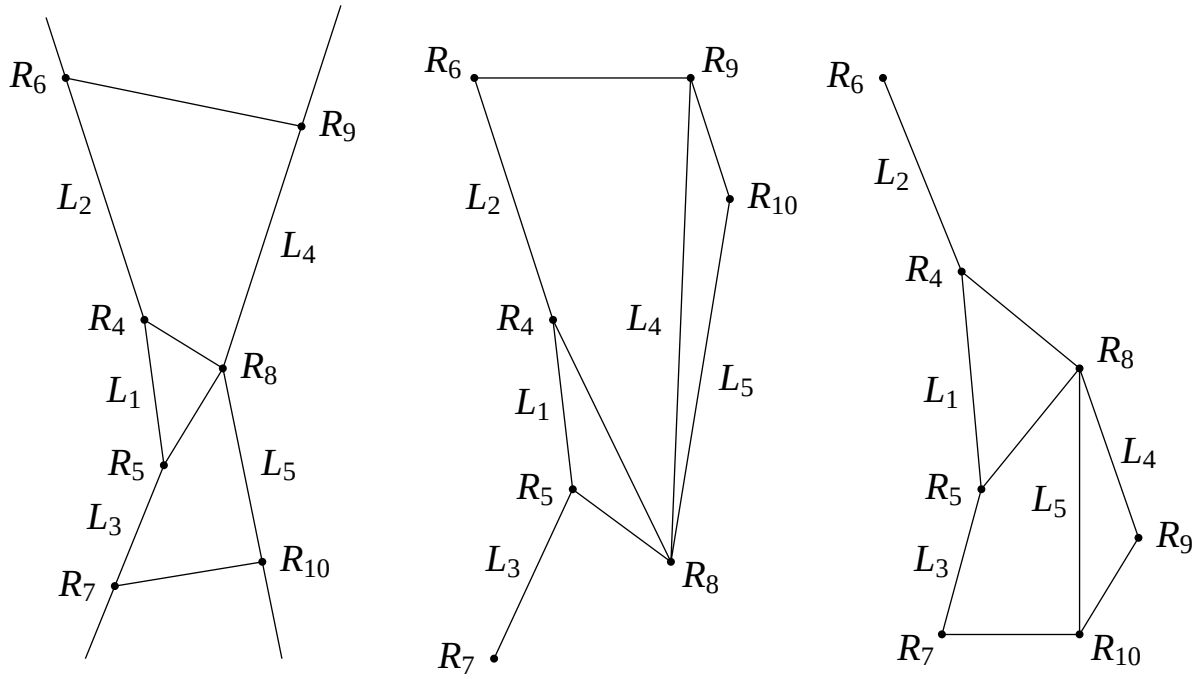


Рис. 3.6

$L_4$ параллельны. Так как $L_2$ разделяет $M_\nu(f)$ и $M_{1-\nu}(f)$, то прямая $L_4$ также будет разделять эти множества, поэтому на ней помимо точки $R_8$ найдется еще одна точка из $T_{1-\nu}(f)$. Следовательно, $|T_{1-\nu}(f)| = 2$, что противоречит предположению.

Таким образом, для любой функции $f \in \mathfrak{T}(E_p \times E_q)$ выполняется неравенство $T(f) \leq 4$, причем существуют такие $f$, для которых $T(f) = 4$. Следовательно, $\sigma(E_p \times E_q) = 4$. ∎

**Пример 3.48.** Рассмотрим функцию $f \in \mathfrak{T}(E_k^2)$ (для произвольного $k \geq 5$), определяемую пороговым неравенством $3x_1 + 2x_2 \leq 6$. В этом случае (рис. 3.7 а) множество $T(f)$ содержит 3 точки: $(2, 0)$, $(0, 3)$, $(1, 2)$. Точка $(0, 4)$, например, не принадлежит $T(f)$, так как никакая опорная к $P_1(f)$ прямая, проходящая через $(0, 4)$, не является разделяющей для $M_0(f)$, $M_1(f)$.

Для функции $g \in \mathfrak{T}(E_k^2)$, $k \geq 8$, определяемой пороговым неравенством $3x_1 + 2x_2 \leq 13$, разрешающее множество $T(g)$ состоит из 4 точек: $(3, 2)$, $(1, 5)$, $(4, 1)$, $(0, 7)$ (см. рис. 3.7 б).

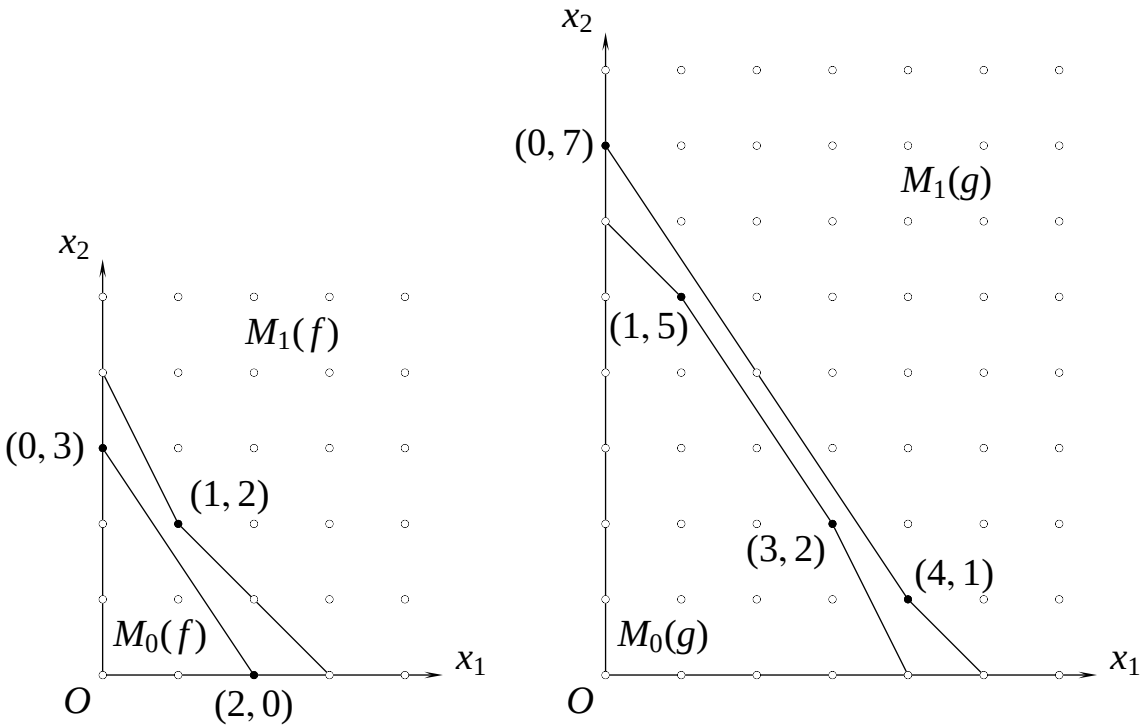


Рис. 3.7

### 3.10.2. Среднее значение мощности минимального разрешающего множества пороговой функции двух переменных

В настоящем разделе исследуется средняя мощность $\overline{\sigma}(E_p \times E_q)$ минимального разрешающего множества пороговой функции двух переменных.

Определим

$$r_s(p,q) = \sum_{\substack{-p<i<p \\ -q<j<q \\ \text{НОД}(i,j)=s}} (p-|i|)(q-|j|).$$

Две различные точки $R_1, R_2$ в $E_p \times E_q$ называются *соседними*, если отрезок $[R_1, R_2]$ не содержит других точек из $E_p \times E_q$. Легко видеть, что $r_1(p,q)$ равно числу упорядоченных пар $(R_1, R_2)$ соседних точек из $E_p \times E_q$.

**Лемма 3.49.** [136] *При* $p \le q$

$$r_s(p,q) = \frac{6}{\pi^2 s^2}(pq)^2 + O(pq^2)$$

Обозначим $\ell(p,q)$ количество различных прямых, проходящих по крайней мере через 2 точки из $E_p \times E_q$.

**Лемма 3.50.** [135, 155]

$$\ell(p,q) = \frac{1}{2}\big(r_1(p,q) - r_2(p,q)\big) \tag{3.20}$$

Заметим, что произвольная прямая $a_1x_1 + a_2x_2 = a_0$ (где $a_1$, $a_2$ одновременно не равны 0) определяют две пороговые функции: функцию $f$, для которой $M_0(f) = \{x \in E_p \times E_q :\ a_1x_1 + a_2x_2 \ge a_0\}$, и функцию $f'$, для которой $M_0(f) = \{x \in E_p \times E_q :\ a_1x_1 + a_2x_2 \ge a_0\}$.

Как уже отмечалось в разделе 1.4, справедлива

**Теорема 3.51.** [144]

$$|\mathfrak{T}(E_p \times E_q)| = r_1(p,q) + 2. \tag{3.21}$$

Идея доказательства теоремы заключается в следующем. Следуя [144], каждой упорядоченной паре $R_1$, $R_2$ соседних в $E_p \times E_q$ точек поставим в соответствие пороговую функцию по следующему правилу. Проведем через точки $R_1$, $R_2$ прямую и повернем ее на малый угол по часовой стрелки вокруг $R_1$ (см. рис. 3.8). Полученная прямая задает две пороговые функции. Этой прямой поставим в соответствие функцию, множество нулей которой находится, для определенности, «справа» от вектора $\overrightarrow{R_1R_2}$. Можно показать (см. [144, 162]), что такое сопоставление является биекцией между множеством всех упорядоченных пар точек из $E_p \times E_q$ и множеством всех пороговых функций, не равных тождественно 0 или 1 и заданных на $E_p \times E_q$. Как уже отмечалось, количество упорядоченных пар точек в $E_p \times E_q$ равно $r_1(p,q)$. Добавляя тождественный 0 и тождественную 1, получаем формулу (3.21).

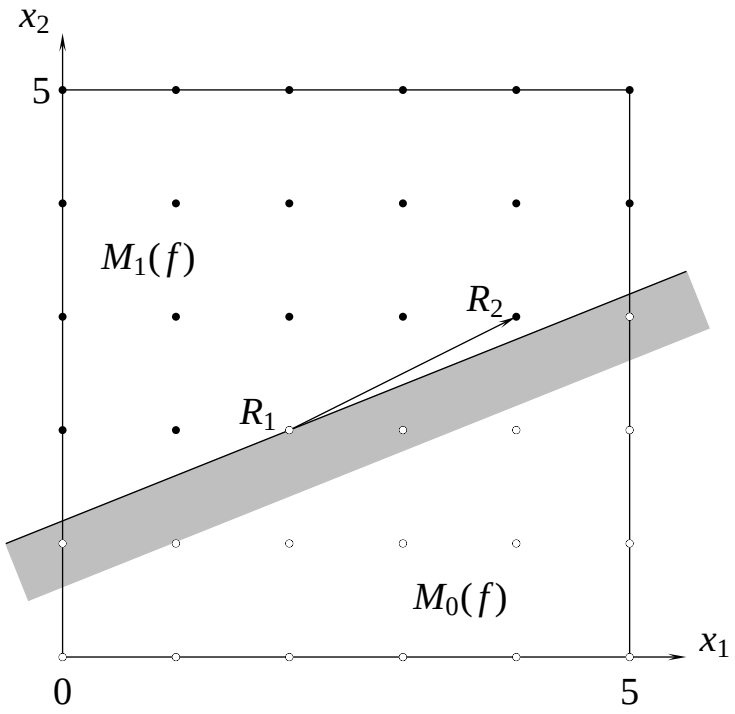


Рис. 3.8

**Следствие 3.52.**

$$|\mathfrak{T}(E_p \times E_q)| = 2 + \sum_{\substack{-p<i<p \\ -q<j<q \\ \text{НОД}(i,j)=1}} (p - |i|)(q - |j|) = \frac{6}{\pi^2}(pq)^2 + O(pq^2). \quad (3.22)$$

*(асимптотика справедлива при* $p \leq q$*).*

Асимптотика (3.22) получена в [136].

Напомним, что точка $x \in E_p \times E_q$ называется *существенной* для функции $f \in \mathfrak{T}(E_p \times E_q)$, если существует функция $f' \in \mathfrak{T}(E_p \times E_q)$, такая, что $f(x) \neq f'(x)$ и $f(y) = f'(y)$ для всех $y \neq x$. Согласно следствию 3.9 множество всех существенных точек есть в точности минимальное разрешающее множество $T(f)$ функции $f$.

**Теорема 3.53.**

$$\overline{\sigma}(p,q) = \frac{4r_1(p,q) - 2f_2(p,q)}{r_1(p,q) + 2}. \quad (3.23)$$

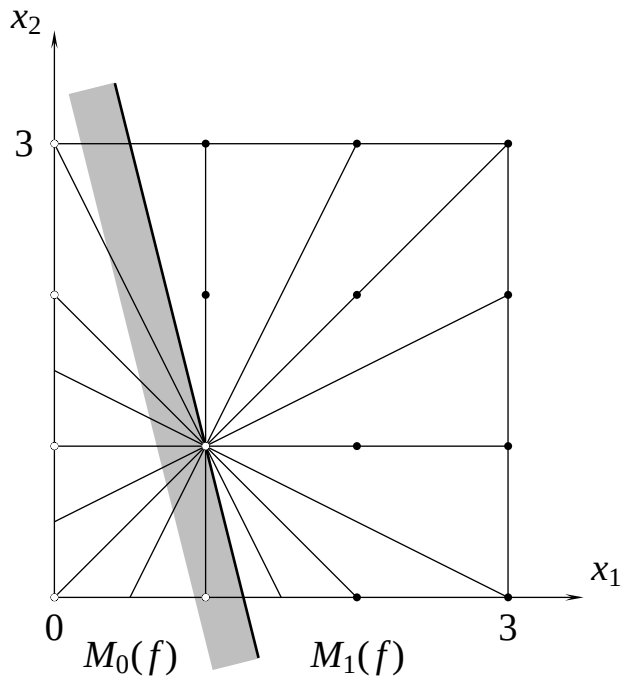


Рис. 3.9

*Доказательство.* Обозначим $h(p, q, i, j)$ количество пороговых функций, определенных на $E_p \times E_q$, для которых точка $(i, j)$ является существенной. Тогда

$$\overline{\sigma}(E_p \times E_q) = \frac{1}{|\mathfrak{T}(E_p \times E_q)|} \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} h(p, q, i, j). \tag{3.24}$$

Рассмотрим все прямые, проходящие через точку $(i, j)$ и по крайней мере еще через одну точку из $E_p \times E_q$. Обозначим $\ell(p, q, i, j)$ количество этих прямых.

Например, на рис. 3.9 изображены все такие прямые, проходящие через точку $(1, 1)$ из $E_4^2$, причем $\ell(4, 4, 1, 1) = 8$.

Эти прямые разбивают плоскость на $2\ell(p, q, i, j)$ секторов.

Легко видеть, что любая новая прямая, проходящая через $(i, j)$ и принадлежащая паре «вертикальных» секторов, но не совпадающая ни с одной из исходных прямых, задает 2 пороговые функции, для которых точка $(i, j)$ является существенной и в которой значение функций равно

0. Очевидно, что прямые, принадлежащие разным парам «вертикальных» секторов, задают разные пороговые функции. Кроме того, других функций, для которых точка $(i, j)$ является существенной и в которой значение функции равно 0, нет.

На рис. 2 изображена одна из таких разделяющих прямых и выбран один из двух возможных способов определения соответсвующей пороговой функции.

Итак, имеем $2l(p, q, i, j)$ пороговых функций, для которых точка $(i, j)$ является существенной и в которой значение функций равно 0. Столько же получаем функций с аналогичным свойством, но которые в точке $(i, j)$ равны 1. Следовательно, $h(p, q, i, j) = 4l(p, q, i, j)$. Теперь из (3.24) получаем

$$\overline{\sigma}(E_p \times E_q) = \frac{4}{|\mathfrak{T}(E_p \times E_q)|} \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \ell(p, q, i, j). \tag{3.25}$$

Обозначим $\mathscr{L}(p, q)$ множество прямых, проходящих по крайней мере через две точки из $E_p \times E_q$. Напомним, что $\ell(p, q) = |\mathscr{L}(p, q)|$. Пусть $L \in \mathscr{L}(p, q)$. Обозначим $z(p, q, L)$ количество точек из $E_p \times E_q$, принадлежащих прямой $L$. Теперь из (3.25) получаем

$$\overline{\sigma}(E_p \times E_q) = \frac{4}{|\mathfrak{T}(E_p \times E_q)|} \sum_{L \in \mathscr{L}(p,q)} z(p, q, L) = 4 \cdot \frac{\ell(m, n) + \frac{1}{2} r_1(p, q)}{|\mathfrak{T}(E_p \times E_q)|}.$$

Подставляя сюда выражения (3.20), (3.21), получаем (3.24). ∎

**Следствие 3.54.** *При* $p \leq q$

$$\overline{\sigma}(E_p \times E_q) = \frac{7}{2} + O\left(\frac{1}{p}\right).$$

Обозначим $t_\mu(p, q)$ количество функций $f \in \mathfrak{T}(E_p \times E_q)$, для которых $|T(f)| = \mu$ $(\mu = 3, 4)$. Из следствия 3.54 получаем, что каждая из величин $t_3(p, q)$ и $t_4(p, q)$ асимптотически равна $\frac{1}{2}|\mathfrak{T}(E_p \times E_q)|$. Получим точные формулы для $t_3(p, q)$ и $t_4(p, q)$.

**Следствие 3.55.**

$$t_3(p,n) = 2r_2(p,q) + 8, \quad t_4(p,q) = r_1(p,q) - 2r_2(p,q) - 6. \tag{3.26}$$

*Доказательство.* Из условий

$$t_3(p,q) + t_4(p,q) = |\mathfrak{T}(E_p \times E_q)|, \qquad \overline{\sigma}(E_p \times E_q) = \frac{3t_3(p,q) + 4t_4(p,q)}{|\mathfrak{T}(E_p \times E_q)|}$$

находим:

$$t_3(p,q) = \big(4 - \overline{\sigma}(E_p \times E_q)\big)|\mathfrak{T}(E_p \times E_q)|,$$

$$t_4(p,q) = \big(\overline{\sigma}(E_p \times E_q) - 3\big)|\mathfrak{T}(E_p \times E_q)|.$$

Подставляя сюда выражения (3.21), (3.23), получаем (3.26). ∎

### 3.10.3. Свойства специальных разбиений плоскости прямыми

Согласно разделу 1.2 для пороговой функции $f \in \mathfrak{T}(E_p \times E_q)$ множество наборов коэффициентов $a_0, a_1, a_2$ ее разделяющей прямой есть полиэдральный конус $K(f)$, определяемый системой линейных неравенств

$$\begin{cases} a_1x_1 + a_2x_2 \le a_0 & \text{для всех } x \in M_0(f), \\ a_1x_1 + a_2x_2 > a_0 & \text{для всех } x \in M_1(f). \end{cases} \tag{3.27}$$

Кроме того, минимальное разрешающее множество $T(f)$ составляют те и только те точки, которые соответствуют неравенствам в (3.27), не являющимися избыточными. Если нас интересуют только те прямые, которые строго разделяют множества $M_0(f)$ и $M_1(f)$, то в (3.27) все неравенства надо заменить на строгие. Таким образом, существует биекция между $\mathfrak{T}(E_p \times E_q)$ и множеством открытых конусов, на которые пространство параметров $a_0, a_1, a_2$ разбивается всеми плоскостей вида $a_1x_1 + a_2x_2 = a_0$, где $(x_1, x_2) \in E_p \times E_q$. Более того, плоскости, составляющие границу каждого получаемого открытого конуса, и только они соответствуют точкам

из $T(f)$. Приведенная конструкция хорошо известна в пороговой логике (см., например, [39]).

Пусть

$$\mathfrak{T}_\nu(E_p \times E_q) = \{ f \in \mathfrak{T}(E_p \times E_q) : \ f(0) = \nu \} \qquad (\nu = 0, 1).$$

Заметим, что между множествами $\mathfrak{T}_0(E_p \times E_q)$, $\mathfrak{T}_1(E_p \times E_q)$ существует биекция, задаваемая формулой $f \leftrightarrow f' = 1 - f$, при этом любое разрешающее множество функции $f$ переходит в разрешающее множество функции $f'$.

Если $f \in \mathfrak{T}_0(E_p \times E_q)$, то, не нарушая общности, можно считать, что $a_0 = 1$, и множество наборов коэффициентов $a_1, a_2$ разделяющей прямой $a_1 x_1 + a_2 x_2 = 1$ есть множество решений системы

$$\begin{cases} a_1 x_1 + a_2 x_2 \le 1 & \text{для всех } x \in M_0(f), \\ a_1 x_1 + a_2 x_2 > 1 & \text{для всех } x \in M_1(f). \end{cases} \tag{3.28}$$

Тем самым устанавливается биекция между множеством открытых многоугольных областей, на которые плоскость параметров $a_1, a_2$ разбивается множеством всех прямых вида $a_1 x_1 + a_2 x_2 = 1$, где $(x_1, x_2) \in E_p \times E_q$, и множеством $f \in \mathfrak{T}_0(E_p \times E_q)$ (см. рис. 3.10). Заметим, что разбиение плоскости прямыми (3.28) получается также в результате пересечения плоскостью $a_0 = 1$ разбиения пространства плоскостями (3.27).

Многоугольник (возможно неограниченный) назовем *обобщенным $m$-угольником*, если его можно получить пересекая $m$-гранный конус с плоскостью, не проходящей через вершину конуса.

Из сделанных замечаний и результатов раздела 3.10.2 получаем

**Следствие 3.56.** *Среди всех областей, получаемых при разбиении плоскости параметров $a_1, a_2$ прямыми $a_1 x_1 + a_2 x_2 = 1$, где $(x_1, x_2) \in E_p \times E_q$, встречаются только обобщенные треугольники и четырехугольники.*

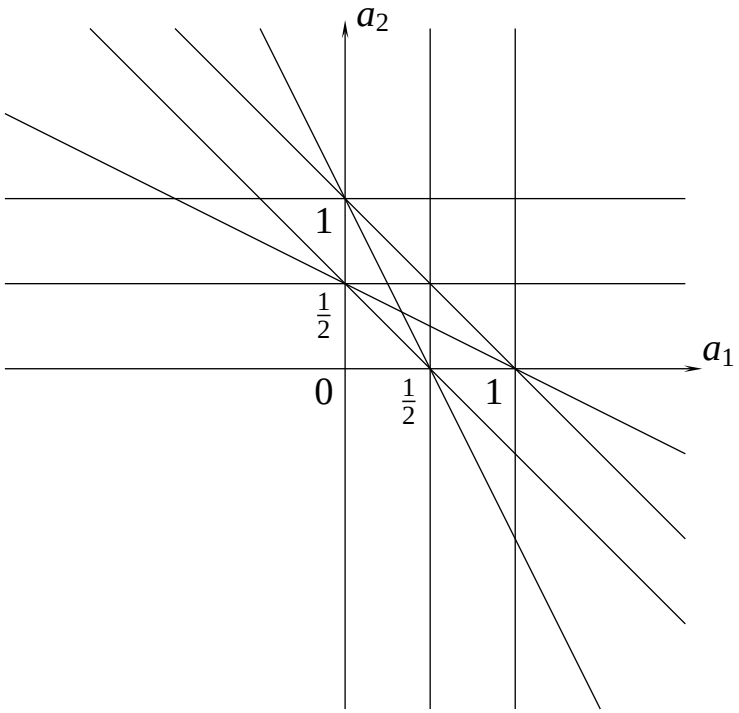


Рис. 3.10

*Причем их количества равны, соответственно,*

$$\frac{1}{2}t_3(p,q) = r_2(p,q) + 4 = \frac{3}{2\pi^2}p^2q^2 + O(pq^2),$$

$$\frac{1}{2}t_4(p,q) = \frac{1}{2}r_1(p,q) - r_2(p,q) - 3 = \frac{3}{2\pi^2}p^2q^2 + O(pq^2).$$

(*асимптотика при* $p \le q$).

Аналогичные результаты можно получить, если разбивать плоскость параметров $a_1, a_2$ прямыми $a_1x_1 + a_2x_2 = 1$, где $(x_1, x_2) \in \{1, 2, \ldots, p\} \times \{1, 2, \ldots, q\}$ и т. п. В частности, на рис. 3.11 представлено разбиение указанными прямыми первой четверти плоскости.

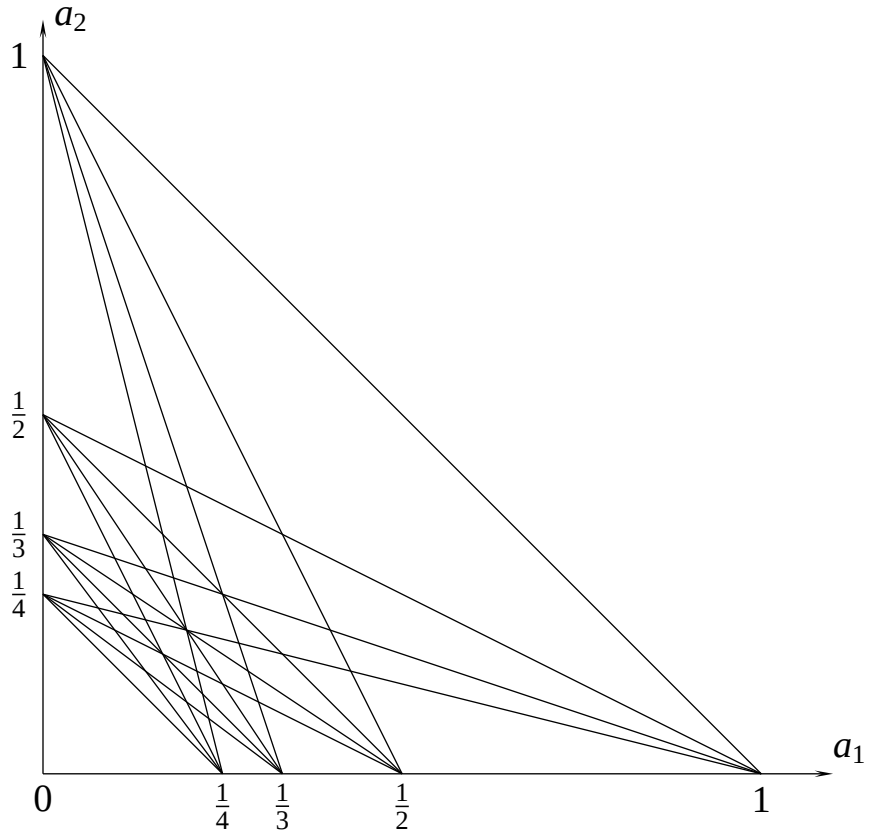


Рис. 3.11

## 3.11. Сложность расшифровки пороговых булевых функций

Для пороговых булевых функций из следствия 3.15 получаем:

$$\sigma(E_2^n) = \tau(E_2^n) = |E_2^n| = 2^n.$$

Обозначим теперь через $\mathfrak{F}_{\mathrm{M}}(n)$ и $\mathfrak{F}_{\mathrm{MT}}(n) = \mathfrak{T}(E_2^k) \cap \mathfrak{F}_{\mathrm{M}}(n)$ соответственно класс монотонных и класс пороговых монотонных функций, отображающих $E_2^n$ в $\{0, 1\}$. Напомним, что функция $f \in \mathfrak{F}(E_2^n)$ называется *монотонной*, если для любых $x, y \in E_2^n$, таких, что $x_j \le y_j$ $(j = 1, \ldots, n)$ выполняется неравенство $f(x) \le f(y)$. Покажем, что сложность расшифровки функций в классах $\mathfrak{F}_{\mathrm{MT}}(n)$ и $\mathfrak{F}_{\mathrm{M}}(n)$ одинакова. Точнее говоря, покажем, что минимальное число вопросов, необходимое для расшифровки

в классе $\mathfrak{F}_{\mathrm{MT}}(n)$ функции $f'$, задаваемой пороговым неравенством

$$\sum_{j=1}^{n} x_j \le \left\lfloor \frac{n}{2} \right\rfloor,$$

равно

$$\binom{n}{\lfloor n/2 \rfloor} + \binom{n}{\lfloor n/2 \rfloor + 1}.$$

Заметим, что $f'$ является монотонной. В [134] приводится алгоритм, позволяющий расшифровать любую функцию из класса $\mathfrak{F}_{\mathrm{M}}(n)$, обращаясь к оракулу не более $\binom{n}{\lfloor n/2 \rfloor} + \binom{n}{\lfloor n/2 \rfloor + 1}$ раз. Кроме того, в [49] показано, что для расшифровки функции $f'$ в классе $\mathfrak{F}_{\mathrm{M}}(n)$ любой алгоритм должен не менее $\binom{n}{\lfloor n/2 \rfloor} + \binom{n}{\lfloor n/2 \rfloor + 1}$ раз обратиться к оракулу.

Легко показать, что $f'$ остается «наихудшей» и при сужении класса от $\mathfrak{F}_{\mathrm{M}}(n)$ до $\mathfrak{F}_{\mathrm{MT}}(n)$. Действительно, на пороговой гиперплоскости, задающей функцию $f'$, находится $\binom{n}{\lfloor n/2 \rfloor}$ точек из $M_0(f')$; на гиперплоскости, описываемой уравнением

$$\sum_{i=1}^{n} x_i = \left\lfloor \frac{n}{2} \right\rfloor + 1$$

находится $\binom{n}{\lfloor n/2 \rfloor + 1}$ точек из $M_1(f')$. По теореме 3.11 получаем, что минимальное число обращений к оракулу равно $\binom{n}{\lfloor n/2 \rfloor} + \binom{n}{\lfloor n/2 \rfloor + 1}$. Таким образом, справедлива

**Теорема 3.57.** *Для любого* $n \ge 2$

$$\tau\left(\mathfrak{F}_{\mathrm{MT}}(n)\right) = \sigma\left(\mathfrak{F}_{\mathrm{MT}}(n)\right) = \binom{n}{\lfloor n/2 \rfloor} + \binom{n}{\lfloor n/2 \rfloor + 1}.$$

Заметим, что теорема 3.57 сформулирована также в [117].

## 3.12. Оракульная сложность задачи о рюкзаке

Одной из важнейших задач целочисленного линейного программирования является *задача о рюкзаке* [81, 105]. Рассмотрим один из ее

вариантов: необходимо найти

$$\max_{x\in\mathscr{C}} \sum_{j=1}^{n} c_j x_j, \tag{3.13}$$

где

$$\mathscr{C} = \left\{ x \in E_k^n : \sum_{j=1}^{n} a_j x_j \le a_0 \right\}.$$

Предположим, что $k \ge 2$, $n \ge 1$, $c = (c_1, c_2, \ldots, c_n) \in \mathbb{Z}^n$ известны, а $\mathscr{C}$ задано с помощью оракула, позволяющего по произвольной точке $x \in E_k^n$ отвечать на вопрос «$x \in \mathscr{C}$?». Заметим, что оракульная постановка задач является достаточно популярной в теории оптимизации, включая дискретную оптимизацию [56, 82, 137, 148]. На связь задачи расшифровки монотонной функции с задачами булева линейного программирования, по-видимому, первым указал В. К. Коробков [50]; см. также [75, 80].

Для решения поставленной задачи можно использовать алгоритм $\mathscr{A}_{\text{опт}}$ (см. стр. 81), оракульная сложность которого в нашем случае при фиксированном $n$ есть $O(\log^n k)$.

Можно использовать алгоритм $\mathscr{A}_1^{\text{o}}$ (см. стр. 154), который найдет множество $N(a_0, a)$ вершин выпуклой оболочки множества $\mathscr{C}$, после чего среди них можно выбрать ту, на которой достигается максимум (3.13). Оракульная сложность этого алгоритма при фиксированном $n \ge 2$ есть $O(\log^{n-1} k)$.

Покажем, что нижняя оценка сложности этой задачи при фиксированном $n \ge 3$ есть $\Omega(\log^{n-2} k)$.

Для этого рассмотрим задачу (3.13), в которой

$$\mathscr{C} = \left\{ x \in E_k^n : \sum_{j=1}^{n} a_j x_j \le a_0 - 1 \right\},$$

$a_0, a_1, \ldots, a_n$ — величины, существование которых утверждается в лемме 3.19, и $c = a$. Так как $1 \le a_j \le k-1$, то $N(a_0, a) \subseteq E_k^n$.

Пусть $v \in N(a_0, a)$. Тогда существуют $b \in \mathbb{Z}^n$ и $b_0 \in \mathbb{Z}$, такие, что $bv = b_0$ и $bx \geq b_0 + 1$ при любом $x \in N(a_0, a) \setminus \{v\}$. Рассмотрим множество

$$\mathscr{C}' = \left\{ x \in E_k^n : \ (a + \beta^{-1} b)x \leq a_0 + \beta^{-1} b_0 \right\},$$

где

$$\beta = \max \left\{ 2(k-1) \sum_{j=1}^{n} |b_j|, \ 2|b_0| \right\}.$$

Так как $b \neq 0$, то $\beta > 0$. Покажем, что $\mathscr{C}' = \mathscr{C} \cup \{v\}$. Действительно, при любом $x \in \mathscr{C}$ имеем

$$ax + \beta^{-1} bx \leq a_0 - 1 + \beta^{-1}(k-1) \sum_{j=1}^{n} |b_j| \leq a_0 - \frac{1}{2} \leq a_0 + \beta^{-1} b_0.$$

Далее,

$$av + \beta^{-1} bv = a_0 + \beta^{-1} b_0.$$

И, наконец, при любом $x \in E_k^n \setminus (\mathscr{C} \cup \{v\})$ имеем

$$ax + \beta^{-1} bx \geq a_0 + \beta^{-1}(b_0 + 1) > a_0 + \beta^{-1} b_0.$$

Таким образом, $\mathscr{C}' = \mathscr{C} \cup \{v\}$. Так как $cv = a_0 > \max\{cx : \ x \in \mathscr{C}\}$, то, очевидно, любой алгоритм, решающий оракульную задачу о рюкзаке с областью допустимых значений $\mathscr{C}$ и вектором целевой функции $c = a$, должен обратиться к оракулу в точке $v$. Нижняя оценка теперь следует из леммы 3.19.

# Глава 4

# Расшифровка пороговых функций и диофантовы приближения

В данной главе показана связь задачи расшифровки пороговой функции двух переменных с проблемой нахождения диофантовых приближений вещественных чисел. Предлагается полиномиальный алгоритм нахождения наилучших приближений алгебраических вещественных чисел, заданных минимальным многочленом.

Результаты данной главы опубликованы в работе [35].

## 4.1. Диофантовы приближения вещественных чисел

В данной главе рассматриваются приближения вещественных чисел рациональными числами с малым знаменателем, т. е. *диофантовы приближения*.

Рассмотрим *задачу нахождения наилучшего рационального приближения*. Пусть $\alpha \in \mathbb{R}$, $\alpha \geq 0$, $Q \in \mathbb{N}$. Требуется среди всех рациональных дробей со знаменателем, не превосходящим $Q$, найти наилучшее приближение $\frac{p}{q}$ к $\alpha$:

$$\left|\alpha - \frac{p}{q}\right| = \min\left\{\left|\alpha - \frac{y}{x}\right| : \ x \in \mathbb{N},\ x \leq Q,\ y \in \mathbb{Z}\right\}.$$

Для нахождения наилучшего приближения используют метод цепных дробей. Разложение вещественного числа $\alpha \geq 0$ в цепную дробь (см., например, [86]) описывается следующим образом.Последовательно

определяем числа $a_0, a_1, a_2, \ldots$ по формулам

$$\begin{aligned} a_0 &= \lfloor \alpha \rfloor, & r_0 &= \alpha - a_0, \\ a_1 &= \lfloor 1/r_0 \rfloor, & r_1 &= 1/r_0 - a_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_i &= \lfloor 1/r_{i-1} \rfloor, & r_i &= 1/r_{i-1} - a_i, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{4.1}$$

Последовательность обрывается, если $\alpha$ рационально. В этом случае имеем:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{i-1} + \cfrac{1}{a_i}}}} \tag{4.2}$$

Для выражения, стоящего справа, введем обозначение $[a_0, a_1, \ldots, a_i]$. Если $\alpha$ иррационально, то последовательность (4.1) не обрывается. В этом случае будем писать

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}} \tag{4.3}$$

или кратко: $\alpha = [a_0, a_1, \ldots, a_j, \ldots]$. Цепная дробь $\alpha = [a_0, a_1, \ldots, a_i]$ задает рациональное число $p_i/q_i$, где НОД$(p_i, q_i) = 1$. Назовем его $i$-й *подходящей дробью* рационального числа (4.2) или иррационального (4.3). Определим также $p_{-2} = 0$, $q_{-2} = 1$, $p_{-1} = 1$, $q_{-1} = 0$. Справедливы следующие утверждения (см., например, [86]):

1) для иррационального $\alpha$

$$\lim_{i\to\infty} \frac{p_i}{q_i} = \alpha;$$

2) $|p_i/q_i - \alpha|$ строго монотонно убывает;

3) $p_{2i}/q_{2i} < \alpha$ и последовательность $p_{2i}/q_{2i}$ строго монотонно возрастает;

4) $p_{2i+1}/q_{2i+1} > \alpha$ и последовательность $p_{2i+1}/q_{2i+1}$ строго монотонно убывает;

5) пусть

$$L = \mathrm{Conv}\{(x,y) \in \mathbb{Z}^2,\ x \geq 0,\ y \geq 0,\ \alpha x - y > 0\},$$

$$G = \mathrm{Conv}\{(x,y) \in \mathbb{Z}^2,\ x \geq 0,\ y \geq 0,\ \alpha x - y < 0\},$$

тогда точки $(q_{2i}, p_{2i})$ являются вершинами $L$, а точки $(q_{2i+1}, p_{2i+1})$ — вершинами $G$ [46];

6) среди всех рациональных чисел со знаменателем, не превосходящим $q_i$, дробь $p_i/q_i$ является наилучшим приближением к $\alpha$;

7) если $p_i/q_i$ — последняя подходящая дробь числа $\alpha$ со знаменателем $q_i \leq Q$ и $j$ — максимальное целое, такое, что

$$q_{i-1} + jq_i \leq Q, \tag{4.4}$$

то

$$\frac{p_{i-1} + jp_i}{q_{i-1} + jq_i} \quad \text{или} \quad \frac{p_i}{q_i}$$

является наилучшим приближением к $\alpha$ среди всех чисел со знаменателем, не превосходящим $Q$ [86].

Если $\alpha$ рациональное, то его разложение в цепную дробь обрывается через полиномиальное время. Очевидно, что также существует полиномиальная процедура для нахождения $j$, удовлетворяющего (4.4). Таким образом, справедливо следующее утверждение.

**Теорема 4.1.** (См., например, [81, С. 101]). *По заданным рациональному $\alpha$ и натуральному $Q$ за время, ограниченное полиномом от размера $\alpha$, алгоритм цепных дробей находит решение задачи о наилучшем приближении.*

## 4.2. Связь задачи расшифровки с задачей приближения

В 4.1 мы рассмотрели алгоритм решения задачи наилучшего приближения к рациональному числу $\alpha$. Предполагалось, что $\alpha$ задано разложением числителя и знаменателя в некоторой позиционной (например, двоичной) системе счисления. Если $\alpha$ вещественное, необходимо использовать другой способ его представления. Возможными моделями вещественных чисел являются модель последовательностей Коши (с вычислительной точки зрения эта модель рассматривается, например, в [148]) и модель сечений Дедекинда. В последней вещественным числом $\alpha$ является оракул, который по заданному $r \in \mathbb{Q}$ отвечает на вопрос, выполняется или нет неравенство $\alpha \leq r$.

Вместе с заданным таким образом вещественным числом $\alpha \geq 0$ рассмотрим функцию $f \in \mathfrak{T}(E_{Q+1} \times E_{\lceil \alpha Q \rceil + 1})$, определяемую пороговым неравенством $\alpha x - y \leq 0$. Очевидно, что оракул этой функции эквивалентен оракулу вещественного числа $\alpha$.

Пусть $p/q$ есть решение задачи наилучшего приближения для вещественного числа $\alpha$, $\text{НОД}(p, q) = 1$. Обозначим $\delta = \lfloor Q/p \rfloor$. Оказывается, что любой алгоритм при расшифровке $f$ должен обратиться к оракулу в

точке $(q, p)$ или в точке $\delta \cdot (q, p)$, а, именно, справедлива

**Лемма 4.2.**

1) *Если* $\alpha > \dfrac{p}{q}$, *то* $(q, p) \in T_1(f)$.

2) *Если* $\alpha \leq \dfrac{p}{q}$, *то* $\delta \cdot (q, p) \in T_0(f)$.

*Доказательство.* 1) Если $\alpha > \frac{p}{q}$, то $(q, p) \in M_1(f)$. Сначала заметим, что в этом случае $\alpha \neq 0$. Действительно, иначе мы бы имели $\frac{p}{q} = 0$ и, следовательно, $(q, p) \in M_0(f)$.

Из того, что $\frac{p}{q}$ есть решение задачи о наилучшем приближении, следует, что *внутри* конуса, натянутого на лучи с угловыми коэффициентами $\alpha - (\alpha - \frac{p}{q})$ и $\alpha + (\alpha - \frac{p}{q})$, нет точек из $E_{Q+1} \times E_{\lceil \alpha Q \rceil + 1}$. Так как НОД$(p, q) = 1$, то отрезок с концами $(0, 0)$, $(q, p)$ также не содержит внутренних целочисленных точек. Отсюда получаем, что неравенству

$$px - qy \leq 0 \tag{4.5}$$

удовлетворяют все точки из $M_0(f)$, причем на прямой $px - qy = 0$ лежит лишь одна такая точка, $(0, 0)$. Кроме того, на этой прямой лежат точки $\beta \cdot (q, p)$ $(\beta \in \mathbb{N})$ и других точек из $M_1(f)$, удовлетворяющих (4.5), нет. Следовательно, неравенству

$$px - qy \leq -1, \tag{4.6}$$

кроме точки $(0, 0)$, удовлетворяют все точки из $M_0(f)$ и ни одна точка из $M_1(f)$, а неравенству

$$px - qy \geq 1, \tag{4.7}$$

кроме точек вида $\beta \cdot (q, p)$ $(\beta \in \mathbb{N})$, удовлетворяют все точки из $M_1(f)$ и ни одна из $M_0(f)$.

Пусть

$$\varepsilon = \min\left\{\frac{1}{\lceil \alpha Q\rceil - p}; \frac{1}{2p}\right\}. \tag{4.8}$$

Так как $\alpha \neq 0$, то знаменатель по крайней мере одной дроби в (4.8) не обращается в нуль, следовательно, min имеет конечное значение. Рассмотрим функцию $g \in F_\pi(E_{Q+1} \times E_{\lceil \alpha Q\rceil+1})$, задаваемую пороговым неравенством

$$px - qy + \varepsilon(y - p) \leq 0. \tag{4.9}$$

Для любой $(x, y) \in M_0(f)$, $(x, y) \neq (0, 0)$, из (4.6) и (4.8) получаем: $px - qy + \varepsilon(y - p) \leq -1 + \frac{1}{\lceil \alpha Q\rceil - p} \cdot (\lceil \alpha Q\rceil - p) \leq 0$. Таким образом, $(x, y)$ удовлетворяет неравенству (4.9). Легко проверить, что этому неравенству удовлетворяет также точка $(0, 0)$.

Если $(x, y) \in M_1(f)$ и не найдется такого $\beta \in \mathbb{N}$, что $(x, y) = \beta \cdot (q, p)$, то из (4.7) и (4.8) получаем: $px - qy + \varepsilon(y - p) \geq 1 + \frac{1}{2p} \cdot (-p) > 0$. Легко проверить, что неравенство (4.9) не выполняется и для всех остальных точек из $M_1(f)$, кроме точки $(q, p)$.

Таким образом, значения функций $f$ и $g$ совпадают во всей области $E_{Q+1} \times E_{\lceil \alpha Q\rceil+1}$, кроме точки $(q, p)$, $(q, p) \in T(f)$.

2) Пусть теперь $(q, p) \in M_0(f)$. Для $\alpha \neq 0$,

$$\varepsilon = \min\left\{\frac{1}{\lceil \alpha Q\rceil - \delta p}; \frac{1}{2\delta p}\right\}$$

рассмотрим функцию $g \in F_\pi(E_{Q+1} \times E_{\lceil \alpha Q\rceil+1})$, задаваемую пороговым неравенством

$$px - qy + \varepsilon(y - \delta p) \leq 0. \tag{4.10}$$

Легко проверить, что этому неравенству удовлетворяют все точки вида $\beta \cdot (q, p)$, где $\beta \in \mathbb{Z}$, $0 \leq \beta < \delta$. Для остальных точек из $M_0(f)$ получаем:

$$px - qy + \varepsilon(y - \delta p) \leq -1 + \frac{1}{\lceil \alpha Q\rceil - \delta p} \cdot (\lceil \alpha Q\rceil - \delta p) \leq 0.$$

Вместе с точками из $M_0(f)$ неравенству (4.10) удовлетворяет точка $\delta(q, p)$. Если $(x, y) \in M_1(f)$ и $(x, y) \neq \delta(q, p)$, тогда

$$px - qy + \varepsilon(y - \delta p) \geq 1 + \frac{1}{2p} \cdot (-\delta p) > 0.$$

Если $\alpha = p = 0$, $q = 1$, то вместо (4.10) рассмотрим пороговое неравенство $2x - 2y \leq 1 - 2Q$. В этом случае $M_1(g)$ содержит только одну точку $(Q, 0)$.

Таким образом, значения функций $f$ и $g$ совпадают во всей области $E_{Q+1} \times E_{\lceil \alpha Q \rceil + 1}$, кроме точки $\delta(q, p)$. Следовательно, $\delta(q, p) \in T(f)$. ∎

Алгоритм расшифровки функции можно использовать для практического нахождения наилучшего приближения к вещественному числу $\alpha$, заданному оракулом. Справедлива

**Теорема 4.3.** *Для произвольных положительных $\alpha \in \mathbb{R}$, $Q \in \mathbb{N}$ алгоритм расшифровки $\mathscr{A}_2$ за $O(\log k)$ обращений к оракулу $\alpha$ и за время, ограниченное полиномом от $\log k$, где $k = \max\{Q, \lceil \alpha Q \rceil\} + 1$, найдет решение $\frac{p}{q}$ задачи о наилучшем приближении к $\alpha$.*

*Доказательство.* Для начала найдем $\lceil \alpha Q \rceil$. Для этого воспользуемся следующей процедурой.

Шаг 1. Положить $p := 0$, $s := 1$.

Шаг 2. Если $\alpha \leq s/Q$, перейти на шаг 4.

Шаг 3. Положить $p := s$, $s := 2s$. Перейти на шаг 2.

Шаг 4. Если $s - p = 1$, тогда $\lceil \alpha Q \rceil = s$, стоп.

Шаг 5. Положить $m := \left\lfloor \frac{s-p}{2} \right\rfloor$.

Шаг 6. Если $\alpha \leq m/Q$, тогда $s := m$, иначе $p := m$. Перейти на шаг 4.

Неравенства на шагах 2 и 6 проверяются посредством обращения к оракулу числа $\alpha$. Очевидно, что за конечное число шагов процедура найдет $s = \lceil \alpha Q \rceil$. Величина всех чисел, участвующих в процедуре, не превосходит $2\lceil \alpha Q \rceil$, а общее число обращений к оракулу не превосходит $\lceil \log 2\lceil \alpha Q \rceil \rceil + \lceil \log \lceil \alpha Q \rceil \rceil = O(\log k)$.

После работы алгоритма расшифровки $\mathscr{A}_2$ необходимо среди точек множества $T(f, \mathscr{A}_2)$ выбрать точку $(q, p) \in E_{Q+1} \times E_{\lceil \alpha Q \rceil + 1}$, соответствующую наилучшему приближению $\dfrac{p}{q}$. Для этого найдем рациональные величины

$$\begin{aligned} \frac{p_0}{q_0} &= \min \left\{ \frac{u}{v} : \ (u, v) \in T_0(f, \mathscr{A}_2) \right\}; \\ \frac{p_1}{q_1} &= \max \left\{ \frac{u}{v} : \ (u, v) \in T_1(f, \mathscr{A}_2) \right\} \end{aligned} \tag{4.11}$$

и зададим вопрос оракулу $\alpha$, верно ли, что

$$\alpha \le \frac{1}{2} \left( \frac{p_0}{q_0} + \frac{p_1}{q_1} \right). \tag{4.12}$$

Если неравенство (4.12) выполняется, то $p/q = p_0/q_0$, в противном случае $p/q = p_1/q_1$. Для завершения доказательства теоремы напомним, что $\tau(\mathscr{A}_2) = O(\log k)$ и, следовательно, min и max в (4.11) можно найти за полиномиальное от $\log k$ время. ∎

Заметим, что после того, как наилучшее приближение $\frac{p}{q}$ к числу $\alpha$ найдено, можно найти все подходящие дроби числа $\alpha$ со знаменателями, не превосходящими $Q$. Для этого алгоритмом Евклида разложим $\frac{p}{q}$ в цепную дробь и найдем все ее подходящие дроби $p_0/q_0, p_1/q_1, \ldots, p_i/q_i$. Очевидно, что все они будут являться подходящими дробями числа $\alpha$, кроме, быть может, самой последней $p_i/q_i = p/q$, НОД$(p_i/q_i) = 1$. Чтобы

определить, является ли дробь $p_i/q_i$ подходящей к $\alpha$, найдем

$$\frac{p_i + p_{i-1}}{q_i + q_{i-1}}.$$

$p_i/q_i$ является подходящей дробью числа $\alpha$ тогда и только тогда, когда выражения

$$\alpha - \frac{p_i + p_{i-1}}{q_i + q_{i-1}} \quad \text{и} \quad \alpha - \frac{p_i}{q_i} \tag{4.13}$$

имеют разный знак.

Действительно, из свойства 7

$$\frac{p_i}{q_i} = \frac{p_{i-2} + jp_{i-1}}{q_{i-2} + jq_{i-1}},$$

тогда

$$\frac{p_i + p_{i-1}}{q_i + q_{i-1}} = \frac{p_{i-1} + (j+1)p_i}{q_{i-1} + (j+1)q_i}.$$

Если (4.13) имеют одинаковый знак, тогда

$$(q_i, p_i) = \frac{j}{j+1}\{(q_{i-2}, p_{i-2}) + (j+1)(q_{i-1}, p_{i-1})\} + \frac{1}{j+1}(q_{i-2}, p_{i-2}),$$

т. е. $(q_i, p_i)$ является выпуклой комбинацией точек $(q_i + q_{i-1}, p_i + p_{i-1})$ и $(q_{i-2}, p_{i-2})$, следовательно, по свойству 5, $p_i/q_i$ не является подходящей дробью. Если (4.13) имеют разный знак, то ввиду взаимной простоты $p_{i-1}$ и $q_{i-1}$, получаем, что отрезок с концами $(q_i, p_i)$ и $(q_i + q_{i-1}, p_i + p_{i-1})$ не содержит внутренних целочисленных точек, следовательно, $(q_i, p_i)$ является вершиной множества $L$ или множества $G$ и, по свойству 5, $p_i/q_i$ — подходящая дробь числа $\alpha$.

## 4.3. Диофантовы приближения алгебраических чисел

Отдельно рассмотрим задачу наилучшего приближения алгебраических вещественных чисел, заданных минимальным многочленом. Алгебраическое число $\alpha$ будет кодироваться тройкой $(h, a, b)$ такой, что $\alpha$

является единственным корнем минимального многочлена $h(x) = h_0x^n + h_1x^{n-1} + \cdots + h_n$ на отрезке с концами $a$, $b$, $(a, b \in \mathbb{Q})$. В этом случае размером входа задачи наилучшего приближения является величина

$$\sum_{i=0}^{n} \langle h_i \rangle + \langle a \rangle + \langle b \rangle,$$

Как отмечено в [148], $a$ и $b$ можно подобрать так, чтобы $\langle a \rangle$ и $\langle b \rangle$ были бы ограничены полиномом от $\langle h \rangle = \sum_{i=0}^{n} \langle h_i \rangle$.

Имея в наличии тройку $(h, a, b)$ за полиномиальное от размера входа время можно определить, выполняется ли равенство $\alpha \leq r$ для произвольного $r \in \mathbb{Q}$. Ответ очевиден, если $r$ не принадлежит отрезку $[a, b]$. Если же $r \in [a, b]$, то, выполнив $n$ сложений и $n$ умножений рациональных чисел, схемой Горнера определим $h(r)$. Если $h(r) \cdot h(b) \geq 0$, то $\alpha \leq r$, в противном случае $\alpha > r$. Для доказательства этого предложения заметим, что, т. к. $h$ — минимальный и, следовательно, неприводимый многочлен и на отрезке $[a, b]$ содержится лишь один корень, то для любого $x \in (\alpha, b]$ $h(x)$ совпадает по знаку с $h(b)$, а для любого $x \in [a, \alpha)$ $h(x)$ совпадает по знаку с $h(a)$. Учитывая вышесказанное, получаем

**Следствие 4.4.** *Для любого $Q$ и для любого алгебраического вещественного $\alpha$, заданного тройкой $(h, a, b)$, существует полиномиальный от длины входа алгоритм решения задачи наилучшего приближения числа $\alpha$.*

# Заключение

Перечислим основные результаты диссертации.

1) Разработан алгоритм $\mathscr{A}_0$ расшифровки в классе $\mathfrak{F}_0(M) \cap \mathfrak{F}_1(M)$. В классе $\mathfrak{F}(M,h)$, где $M \in \mathfrak{M}(n,l,\gamma)$, при любом фиксированном $n$ алгоритм имеет полиномиальную от $h$, $l$ и $\log\gamma$ вычислительную трудоемкость $\rho(\mathscr{A}_0)$ и оракульную сложность

$$\tau(\mathscr{A}_0) = O\Big((l+h)^{\lfloor\frac{n}{2}\rfloor^2} l^{\lfloor\frac{n}{2}\rfloor} \log^{(n-1)\lfloor\frac{n}{2}\rfloor+n}(\gamma+1)\Big)$$

(асимптотика при фиксированном $n$). В классе $\mathfrak{F}_0(E_k^n) \cap \mathfrak{F}_1(E_k^n)$ алгоритм при фиксированном $n$ имеет оракульную сложность

$$\tau(\mathscr{A}_0) = O\Big(\log^{(n-1)\lfloor\frac{n}{2}\rfloor+n} k\Big).$$

2) Разработан алгоритм $\mathscr{A}_1$ расшифровки в классе $\mathfrak{T}(M)$, где $M \in \mathfrak{M}(n,l,\gamma)$, для которого при фиксированном $n$ величина $\rho(\mathscr{A}_1)$ ограничена полиномом от $l$ и $\log\gamma$ и

$$\tau(\mathscr{A}_1) = O\Big(l^{\lfloor\frac{n}{2}\rfloor} \log^n(\gamma+1)\Big).$$

Установлена нижняя оценка сложности этой задачи, а именно, доказано, что для любых $n \geq 2$ и $l > n$ найдется такое $\gamma_0$, что для всех $\gamma \geq \gamma_0$ существует политоп $P \in \mathfrak{P}(n,l,\gamma)$ такой, что при фиксированном $n \geq 2$

$$\tau(M) \geq \sigma(M) = \Omega\Big(l^{\lfloor n/2\rfloor} \log^{n-1}\gamma\Big),$$

где $M = P \cap \mathbb{Z}^n$. Таким образом оракульная сложность предложенного алгоритма $\mathscr{A}_1$ при фиксированном $n$ близка по порядку к нижней оценке сложности.

3) Предложен полиномиальный при фиксированном $n$ алгоритм $\mathscr{A}_1^{\mathrm{o}}$ расшифровки в классе $\mathfrak{T}(M)$. Его оракульная сложность $\tau(\mathscr{A}_1^{\mathrm{o}})$ отличается от сложности оптимального (по числу обращений к оракулу в худшем случае) алгоритма расшифровки не более, чем в $O\bigl(n^3 \log(n\gamma)\bigr)$ раз. Для класса $\mathfrak{T}(E_k^n)$ сложность алгоритма $\mathscr{A}_1^{\mathrm{o}}$ отличается от сложности оптимального алгоритма не более, чем в $O\bigl(n^2 \log(nk)\bigr)$ раз и при фиксированном $n \geq 2$

$$\tau(E_k^n) \leq \tau(\mathscr{A}_1^{\mathrm{o}}) = O(\log^{n-1} k).$$

Оракульная сложность алгоритма $\mathscr{A}_1^{\mathrm{o}}$ при фиксированном $n$ близка по порядку к нижней оценке сложности $\tau(E_k^n) = \Omega(\log^{n-2} k)$.

4) Описано строение минимального разрешающего множества $T(f)$ пороговой функции $f$ из класса $\mathfrak{T}(M)$. Установлены оценки длины обучения в классе $\mathfrak{T}(E_k^n)$: при фиксированном $n \geq 3$

$$\sigma(E_k^n) = \Theta(\log^{n-2} k).$$

5) Разработан полиномиальный алгоритм $\mathscr{A}_2$ расшифровки в классе $E_k^2$, для которого

$$\tau(\mathscr{A}_2) = 6 \log(k-1) + 4.$$

Таким образом,

$$4 \log k \leq \tau(E_k^2) \leq 6 \log(k-1) + 4.$$

Также установлено, что

$$\sigma(E_k^2) = 4, \qquad \overline{\sigma}(E_k^2) = \frac{7}{2} + O\left(\frac{1}{k}\right).$$

6) Установлена связь задачи расшифровки пороговой функции двух переменных с проблемой нахождения диофантовых приближений

вещественных чисел. На основе алгоритма $\mathscr{A}_2$ предложен полиномиальный алгоритм приближения вещественного числа, заданного оракулом, и полиномиальный алгоритм приближения алгебраического числа, заданного минимальным многочленом.

7) Предлагается новая модификация («графовый» тест проверки смежности экстремальных лучей) метода двойного описания построения вершинного описания полиэдра. Теоретическая оценка сложности построенной модификации и результаты экспериментов показали преимущество алгоритма по сравнению с классическим его вариантом.

В частности, при фиксированном $n$ удалось решить задачу об асимптотическом поведении длины обучения $\sigma(E_k^n) = \Theta(\log^{n-2} k)$. Однако на настоящий момент не известно (даже при фиксированном $n \geq 3$) поведение величины $\tau(E_k^n)$:

$$\tau(E_k^n) = O(\log^{n-1} k), \qquad \tau(E_k^n) = \Omega(\log^{n-2} k).$$

По-видимому, при $n \geq 3$ показатель степени в верхней оценке для $\tau(E_k^n)$ можно понизить до $n - 2$.

Указанные верхние и нижние оценки близки друг к другу только при фиксированном $n$. Задача о сближении верхних и нижних оценок при $n \to \infty$ представляется весьма сложной.

Остается открытым вопрос о среднем значении $\overline{\sigma}(n, k)$ мощности минимального разрешающего множества. Ивестна лишь верхняя оценка $\overline{\sigma}(E_k^n) \leq n^2 \log k$ [117], а также установлено асимптотическое значение при $n = 2$, равное $\frac{7}{2}$.

Относительно других открытых проблем, касающихся пороговых и близких к ним функций, отсылаю к списку из обзора Ю. А. Зуева [39].

Многие из приведенных там задач естественным образом обобщаются на случай пороговых функций $k$-значной логики. Как уже отмечалось, среди задач, представляющих наибольший интерес, Ю. А. Зуев указывает исследование свойств графа пороговых функций. Результаты, касающиеся $\sigma(M)$ и $\overline{\sigma}(M)$ можно интерпретировать в этих терминах: $\sigma(M)$ есть максимальная, а $\overline{\sigma}(M)$ — средняя степень вершины графа.

# Литература


1. *Алексеев В. Б.* О числе монотонных $k$-значных функций // Проблемы кибернетики. Вып. 28. — М.: Наука, 1974. — С. 5–24.

2. *Алексеев В. Б.* О расшифровке некоторых классов монотонных многозначных функций // Журнал вычислительной математики и математической физики. — 1976. — Т. 16, № 1. — С. 189–198.

3. *Архангельский С. В.* Энтропия классов цифровых сигналов // Комбинаторно–алгебраические и вероятностные методы в прикладной математике. — Горький: Издательство Горьковского государственного университета, 1988. — С. 5–9.

4. *Архангельский С. В.* Информационный анализ цифровых сигналов. — Самара: Издательство Саратовского университета, Самарский филиал, 1991.

5. *Бастраков С. И., Золотых Н. Ю.* Использование идей алгоритма Quickhull в методе двойного описания // Вычислительные методы и программирование. — 2011. — Т. 12, № 1. — С. 232–237.

6. *Болтянский В. Г., Яглом И. М.* Выпуклые фигуры и тела // Энциклопедия элементарной математики. Кн. 4. Геометрия. — М.: Наука, 1966. — С. 181–269.

7. *Брянстед А.* Введение в теорию выпуклых многогранников. — М.: Мир, 1988.

8. *Веселов С. И.* Нижняя оценка среднего числа неприводимых и крайних точек в двух задачах дискретного программирования / Горь-

ковский гос. университет. — Горький, 1984. — Деп. в ВИНИТИ № 619–84.

9. *Веселов С. И., Парубочий И. Е., Шевченко В. Н.* Программа нахождения остова конуса неотрицательных решений системы линейных неравенств // Системные и прикладные программы. Часть 2. — Горький: Издательство Горьковского государственного университета, 1984. — С. 83–92.

10. *Веселов С. И., Чирков А. Ю.* Оценки числа вершин целых полиэдров // Дискретный анализ и исследование операций. Серия 2. — 2007. — Т. 14, № 2. — С. 14–31.

11. *Веселов С. И., Шевченко В. Н.* О числе экстремальных точек квадратной системы линейных неравенств / Горьковский гос. университет. — Горький, 1978. — Деп. в ВИНИТИ 22.12.1978, № 450–79.

12. *Вировлянская М. А., Золотых Н. Ю.* Верхняя оценка средней мощности минимального разрешающего множества пороговой функции многозначной логики // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 2003. — № 1. — С. 238–247.

13. *Вороненко А. А., Чистиков Д. В.* Индивидуальное тестирование бесповторных функций // Ученые записки Казанского гос. университета. Серия Физико-математические науки. — 2009. — Т. 151, № 2. — С. 36–44.

14. *Горяинов М. В., Сапоженко А. А.* О расшифровке монотонных функций на частично упорядоченных множествах // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 79–80.

15. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

16. *Деза М. М., Лоран М.* Геометрия разрезов и метрик. — М.: МЦНМО, 2001.

17. *Емеличев В. А., Ковалев М. М., Кравцов М. К.* Многогранники, графы, оптимизация. — М.: Наука, 1981.

18. *Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И.* Лекции по теории графов. — М.: Наука, 1990.

19. *Журавлев Ю. И.* Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. Вып. 33. — М.: Наука, 1978. — С. 5–68.

20. *Загоруйко Н. Г.* Прикладные методы анализа данных и знаний. — Новосибирск: ИМ СО РАН, 1999.

21. *Золотых Н. Ю.* Алгоритм расшифровки пороговой функции $k$-значной логики на плоскости с числом обращений к оракулу $O(\log k)$ // Труды Первой Международной конференции «Математические алгоритмы». — Н. Новгород: Издательство Нижегород. гос. ун-та, 1995. — С. 21–26.

22. *Золотых Н. Ю.* О пороговых и близких к ним функциях, определенных в целочисленных точках политопа // Дискретный анализ и исследование операций. Серия 1. — 1998. — Т. 5, № 2. — С. 40–54.

23. *Золотых Н. Ю.* Расшифровка пороговых и близких к ним функций многозначной логики: Дис. . . . канд. физ.-матем. наук / Нижегородский гос. университет им. Н. И. Лобачевского. — Нижний Новгород, 1998.

24. *Золотых Н. Ю.* Оракульная сложность задачи о рюкзаке // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 2000. — № 1. — С. 84–87.

25. *Золотых Н. Ю.* Пороговые функции, зависящие от двух переменных: сложность расшифровки и мощность разрешающего множества // Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям. — М.: Издательство механико-матем. факультета МГУ, 2000. — С. 48–54.

26. *Золотых Н. Ю.* О сложности расшифровки пороговых функций, зависящих от двух переменных // Материалы XI Межгосударственной школы-семинара «Синтез и сложность управляющих систем». Часть I. — М.: Издательство Центра прикладных исследований при механико-математическом ф-те МГУ, 2001. — С. 74–79.

27. *Золотых Н. Ю.* О сложности решения одного класса задач целочисленного линейного программирования // Дискретный анализ и исследование операций. Серия 2. — 2003. — Т. 10, № 1. — С. 3–10.

28. *Золотых Н. Ю.* Оценки мощности минимального разрешающего множества пороговой функции многозначной логики // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 159–168.

29. *Золотых Н. Ю.* Новая модификация метода двойного описания для построения остова многогранного конуса // Журнал вычислительной математики и математической физики. — 2012. — Т. 52, № 1. — С. 153–163.

30. *Золотых Н. Ю.* Расшифровка пороговой функции, заданной расширенным оракулом // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2012. — № 3. — С. 175–178.

31. *Золотых Н. Ю., Лялин С. С.* Параллельный алгоритм нахождения общего решения системы линейных неравенств // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2009. — № 5. — С. 193–199.

32. *Золотых Н. Ю., Чирков А. Ю.* О верхней оценке мощности минимального разрешающего множества пороговой функции // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 5. — С. 35–46.

33. *Золотых Н. Ю., Чирков А. Ю.* Сложность расшифровки пороговых функций многозначной логики // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (18—23 июня 2012 г.). — М.: Издательство механико-матем. факультета МГУ, 2012. — С. 63–77.

34. *Золотых Н. Ю., Шевченко В. Н.* Расшифровка пороговых функций $k$-значной логики // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 3. — С. 18–23.

35. *Золотых Н. Ю., Шевченко В. Н.* Расшифровка пороговых функций и диофантовы приближения // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Математическое моделирование и оптимальное управление. — 1998. — № 1. — С. 199–207.

36. *Золотых Н. Ю., Шевченко В. Н.* Об оценке сложности расшифров-

ки пороговых функций $k$-значной логики // Журнал вычислительной математики и математической физики. — 1999. — Т. 39, № 2. — С. 346–352.

37. *Зуев Ю. А.* Асимптотика логарифма числа пороговых функций алгебры логики // Доклады АН СССР. — 1989. — Т. 306, № 3. — С. 528–530.

38. *Зуев Ю. А.* Комбинаторно-вероятностные и геометрические методы в пороговой логике // Дискретная математика. — 1991. — Т. 3, № 2. — С. 47–57.

39. *Зуев Ю. А.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. Вып. 5. — М.: Физматлит, 1994. — С. 5–61.

40. *Ирматов А. А.* О числе пороговых функций // Дискретная математика. — 1993. — Т. 5, № 3. — С. 40–43.

41. *Ирматов А. А.* Оценки числа пороговых функций // Дискретная математика. — 1996. — Т. 8, № 4. — С. 92–107.

42. *Ирматов А. А., Ковиянич Ж. Д.* Об асимптотике логарифма числа пороговых функций $k$-значной логики // Дискретная математика. — 1998. — Т. 10, № 3. — С. 35–56.

43. *Катериночкина Н. Н.* Поиск максимального верхнего нуля монотонной функции алгебры логики // Доклады АН СССР. — 1975. — Т. 224, № 3. — С. 557–560.

44. *Катериночкина Н. Н.* Поиск максимального нуля для некоторых классов монотонных функций из классификации поста // Журнал

вычислительной математики и математической физики. — 1988. — Т. 28, № 9. — С. 1397–1406.

45. *Китаев А. Ю.* О приближенном вычислении высоты максимального верхнего нуля монотонной булевой фукнции // Математические заметки. — 1991. — Т. 50, № 1. — С. 41–45.

46. *Клейн Ф.* Элементарная математика с точки зрения высшей. Т. 1. — М.: Наука, 1987.

47. *Коробков В. К.* Оценка числа монотонных функций алгебры логики и сложности алгоритма отыскания разрешающего множества для произвольной монотонной функции алгебры логики // Доклады Академии Наук СССР. — 1963. — Т. 150, № 4. — С. 744–747.

48. *Коробков В. К.* Некоторые обобщения задачи «расшифровки» монотонных функций алгебры логики // Дискретный анализ. Сб. тр. Вып. 5. — Новосибирск: Издательство Института матем. СО АН СССР, 1965. — С. 19–25.

49. *Коробков В. К.* О монотонных функциях алгебры логики // Проблемы кибернетики. Вып. 13. — М.: Наука, 1965. — С. 5–28.

50. *Коробков В. К.* О некоторых целочисленных задачах линейного программирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 297–299.

51. *Коробков В. К., Резник Т. Л.* О некоторых алгоритмах вычисления монотонных функций алгебры логики // Доклады Академии Наук СССР. — 1962. — Т. 147, № 5. — С. 1022–1025.

52. *Коршунов А. Д.* Решение проблемы Дедекинда о числе монотонных

булевых функций // Доклады АН СССР. — 1977. — Т. 223, № 4. — С. 543–546.

53. *Коршунов А. Д.* О числе монотонных булевых функций // Проблемы кибернетики. Вып. 38. — М.: Наука, 1981. — С. 5–108.

54. *Коршунов А. Д.* Монотонные булевы функции // Успехи математических наук. — 2003. — Т. 58, № 5. — С. 5–108.

55. *Кудрявцев В. Б.* Теория тестового распознавания // Дискретная математика. — 2006. — Т. 18, № 3. — С. 3–34.

56. *Леонтьев В. К.* Дискретная оптимизация // Журнал вычислительной математики и математической физики. — 2007. — Т. 47, № 2. — С. 338–352.

57. *Лупанов О. Б.* О возможности синтеза схем из произвольных элементов // Труды математического института им. В. А. Стеклова. Т. 51. — М.: АН СССР, 1958. — С. 158–173.

58. *Лупанов О. Б.* О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26. — М.: Наука, 1973. — С. 109–140.

59. *Митягин Б. С.* Два неравенства для объемов выпуклых тел // Математические заметки. — 1969. — Т. 5, № 1. — С. 99–106.

60. *Мишина А. П., Проскуряков И. В.* Высшая алгебра. Линейная алгебра, многочлены, общая алгебра. — М.: Наука, 1965.

61. *Мошков М. Ю.* Об условных тестах // Доклады Академии Наук СССР. — 1982. — Т. 265, № 3. — С. 550–552.

62. *Мошков М. Ю.* Условные тесты // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 131–170.

63. *Немировский А. С., Юдин Д. Б.* Сложность задачи и эффективность методов оптимизации. — М.: Наука, 1979.

64. *Нечипорук Э. И.* О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 11. — М.: Наука, 1964. — С. 49–62.

65. *Осокин В. В.* О сложности расшифровки разбиения булева куба на подкубы // Дискретная математика. — 2008. — Т. 20, № 2. — С. 46–62.

66. *Осокин В. В.* О расшифровке монотонных булевых функций с несущественными переменными // Дискретная математика. — 2010. — Т. 22, № 3. — С. 134–145.

67. *Прасолов В. В.* Задачи по планиметрии. — 5 изд. — М.: Издательство МЦНМО: ОАО «Московские учебники», 2006.

68. *Препарата Ф., Шеймос М.* Вычислительная геометрия: Введение. — М.: Мир, 1989.

69. *Рокафеллар Р.* Выпуклый анализ. — М.: Мир, 1973.

70. *Сапоженко А. А.* О поиске максимального верхнего нуля монотонных функций на ранжированных множествах // Журнал вычислительной математики и математической физики. — 1991. — Т. 31, № 12. — С. 1871–1884.

71. *Сапоженко А. А.* Проблема Дедекинда и метод граничных функционалов // Математические вопросы кибернетики. Вып. 9. — М.: Наука, 2000. — С. 161–220.

72. *Сапоженко А. А.* Проблема Дедекинда и метод граничных функционалов. — М.: Физматлит, 2009.

73. *Сержантов А. В.* Оптимальный алгоритм расшифровки некоторых классов монотонных функций // Журнал вычислительной математики и математической физики. — 1983. — Т. 23, № 1. — С. 206–212.

74. *Сержантов А. В.* Об оптимальном алгоритме расшифровки некоторых монотонных функций конечнозначной логики // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 223–233.

75. *Смирнов А. Н.* О сложности одного класса задач булева программирования // Сообщения ВЦ АН. Вып. 10. — М.: ВЦ АН СССР, 1978.

76. *Соколов Н. А.* Поиск максимального верхнего нуля для одного класса монотонных дискретных функций // Доклады АН СССР. — 1980. — Т. 251, № 5. — С. 1077–1080.

77. *Соколов Н. А.* О поиске максимального верхнего нуля для одного класса монотонных функций конечнозначной логики // Журнал вычислительной математики и математической физики. — 1981. — Т. 21, № 6. — С. 1552–1565.

78. *Соколов Н. А.* Частичная расшифровка монотонных булевых функций // Журнал вычислительной математики и математической физики. — 1983. — Т. 23, № 5. — С. 1267–1271.

79. *Соколов Н. А.* Оптимальная расшифровка монотонных булевых функций // Журнал вычислительной математики и математической физики. — 1987. — Т. 27, № 12. — С. 1878–1887.

80. *Соколов Н. А.* Оракульная сложность порядковой оптимизации на булевом кубе // Комбинаторные модели и методы. Вып. 2. — М.: ВЦ РАН, 1997. — С. 85–90.

81. *Схрейвер А.* Теория линейного и целочисленного программирования. В 2-х тт. — М.: Мир, 1991.

82. *Трауб Д., Васильковский Г., Вожьняковский Х.* Информация, неопределенность, сложность. — М.: Мир, 1988.

83. *Хайкин С.* Нейронные сети. — М.: Вильямс, 2006.

84. *Хачиян Л. Г.* Полиномиальные алгоритмы в линейном программировании // Журнал вычислительной математики и математической физики. — 1980. — Т. 20, № 1. — С. 51–68.

85. *Хачиян Л. Г.* Полиномиальный алгоритм в линейном программировании // Доклады АН СССР. — 1980. — Т. 244, № 5. — С. 1093–1096.

86. *Хинчин А. Я.* Цепные дроби. — М.: Наука, 1978.

87. *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды Матем. Института АН СССР. — 1958. — Т. 51. — С. 270–360.

88. *Черников С. Н.* Линейные неравенства. — М.: Наука, 1968.

89. *Черникова Н. В.* Алгоритм для нахождения общей формулы неотрицательных решений системы линейных уравнений // Журнал вычислительной математики и математической физики. — 1964. — Т. 4, № 4. — С. 733–738.

90. *Черникова Н. В.* Алгоритм для нахождения общей формулы неотрицательных решений системы линейных неравенств // Журнал вычислительной математики и математической физики. — 1965. — Т. 5, № 2. — С. 334–337.

91. *Черных О. Л.* Построение выпуклой оболочки конечного множества точек на основе триангуляции // Ж. вычисл. матем. и матем. физ. — 1991. — Т. 31, № 8. — С. 1231–409.

92. *Чирков А. Ю.* Теорема Каратеодори и покрытие многогранника симплексами / Нижегородский государственный университет им. Н. И. Лобачевского. — Н. Новгород, 1993. — Деп. в ВИНИТИ 19.03.93, № 668-В93.

93. *Чирков А. Ю.* О нижней оценке числа вершин выпуклой оболочки целочисленных и частично целочисленных точек полиэдра // Труды Первой Международной конференции «Математические алгоритмы» (15–19 августа 1994 г., Нижний Новгород) / Под ред. В. Е. Алексеев, М. А. Антонец, В. Н. Шевченко. — Н. Новгород: Издательство Нижегородского университета, 1995. — С. 128–134.

94. *Чирков А. Ю.* О нижней оценке числа вершин выпуклой оболочки целочисленных и частично целочисленных точек полиэдра // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 2. — С. 80–89.

95. *Чирков А. Ю.* О связи верхних оценок числа вершин выпуклой оболочки целочисленных точек полиэдра с его метрическими характеристиками // Труды Второй международной конференции «Математические алгоритмы». — Н. Новгород: Издательство Нижегородского университета, 1997. — С. 169–174.

96. *Чирков А. Ю., Федотова А. А.* О покрытии полиэдра параллелепипедами / Нижегородский государственный университет им. Н. И. Лобачевского. — 1993. — Деп. в ВИНИТИ 03.06.94, № 1361-В94.

97. *Чирков А. Ю., Шевченко В. Н.* О числе вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой / Нижегородский государственный университет им. Н. И. Лобачевского. — Н. Новгород, 1993. — Деп. в ВИНИТИ 29.07.93, № 2165-В93.

98. *Чистиков Д. В.* О связи задач диагностического и проверяющего тестирования бесповторных функций // Дискретная математика. — 2011. — Т. 23, № 1. — С. 46–50.

99. *Чистиков Д. В.* Использование запросов существенности для расшифровки бесповторных функций // Записки научных семинаров ПОМИ РАН. — 2012. — Т. 402. — С. 183–217.

100. *Шевченко В. Н.* О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. — № 2. — С. 133–134.

101. *Шевченко В. Н.* Задача о размене задача фробениуса и задача групповой минимизации // Комбинаторно–алгебраические методы в прикладной математике. — Горький: Издательство Горьковского государственного университета, 1982. — С. 166–179.

102. *Шевченко В. Н.* Алгебраический подход в целочисленном программировании // Кибернетика. — 1984. — № 4. — С. 36–41.

103. *Шевченко В. Н.* О некоторых функциях многозначной логики, связанных с целочисленным программированием // Методы дискретного анализа в теории графов и схем. Вып. 42. — Новосибирск: Институт матем. СО АН СССР, 1985. — С. 99–108.

104. *Шевченко В. Н.* О расшифровке пороговых функции многозначной логики // Комбинаторно–алгебраические методы в прикладной

математике. — Горький: Издательство Горьковского университета, 1987. — С. 155–163.

105. *Шевченко В. Н.* Качественные вопросы целочисленного программирования. — М.: Физматлит, 1995.

106. *Шевченко В. Н.* Триангуляции выпуклых многогранников и их булевы функции // Математические вопросы кибернетики. Вып. 16. — М.: Физматлит, 2007. — С. 43–56.

107. *Шевченко В. Н., Веселов С. И.* Расшифровка функций многозначной логики // Теория и программная реализация методов дискретной оптимизации. Сб. науч. тр. — Киев: Институт кибернетики АН УССР, науч. совет по пробл. «Кибернетика», 1989. — С. 30–34.

108. *Шевченко В. Н., Груздев Д. В.* Модификация алгоритма Фурье–Моцкина для построения триангуляций // Дискретный анализ и исследование операций. Серия 2. — 2003. — Т. 10, № 10. — С. 53–64.

109. *Шевченко В. Н., Золотых Н. Ю.* О сложности расшифровки пороговых функций $k$-значной логики // Доклады РАН. — 1998. — Т. 362, № 5. — С. 606–608.

110. *Шевченко В. Н., Чирков А. Ю.* О сложности построения остова конуса // X Всероссийская конференция «Математическое программирование и приложения». — Екатеринбург: Уральское отделение РАН, 1997. — С. 237.

111. *Шор Н. З.* Методы минимизации недифференцируемых функций. — Киев: Наукова Думка, 1979.

112. *Acketa D. M., Žunić J. D.* On the number of linear partitions of

the $(m, n)$-grid // Information Processing Letters. — 1991. — V. 38. — P. 163–168.

113. *Aizenstein H., Hegedüs T., Hellerstein L., Pitt L.* Complexity theoretic hardness results for query learning // Journal Computational Complexity. — 1998. — V. 7, N. 1. — P. 19–53.

114. *Alekseyev M. A.* On the number of two-dimensional threshold functions // SIAM Journal on Discrete Mathematics. — 2010. — V. 24, N. 4. — P. 1617–1631.

115. *Angluin D.* Queries and concept learning // Machine Learning. — 1988. — V. 2, N. 4. — P. 319–342.

116. *Anthony M., Bartlett P. L.* Neural network learning: theoretical foundations. — Cambridge: Cambridge Univesity Press, 1999.

117. *Anthony M., Brightwell G., Shawe-Taylor J.* On specifying boolean functions by labelled examples // Discrete Applied Mathematics. — 1995. — V. 61, N. 1. — P. 1–25.

118. *Avis D., Bremner D., Seidel R.* How good are convex hull algorithms? // Computational Geometry: Theory and Apllications. — 1997. — V. 7, N. 5–6. — P. 265–301.

119. *Bárány I., Howe R., Lovász L.* On integer points in polyhedra: A lower bound // Combinatorica. — 1992. — V. 12, N. 2. — P. 135–142.

120. *Bloch M., Moravek J.* Bounds of the number of threshold functions // Information Processing Machines. — 1967. — N. 13. — P. 67–73. — [Рус. пер.: *Блох М., Моравек Я.* Оценка числа пороговых функций // Кибернетический сборник. Новая серия. Вып. 6. — М.: Мир, 1969. — С. 82–88].

121. *Bshouty N. H., Goldberg P. W., Goldman S. A., Mathias H. D.* Exact learning of discretized geometric concepts // SIAM Journal of Computations. — 1998. — V. 28, N. 2. — P. 674–699.

122. *Bultman W. J., Maass W.* Fast identification of geometric objects with membership queries // Information and Computation. — 1995. — V. 118, N. 1. — P. 48–64.

123. *Burger E.* Über homogene lineare Ungleichungssysteme // Zeitschrift für Angewandte Mathematik und Mechanik. — 1956. — V. 36, N. 3/4. — P. 135–139.

124. *Cameron S. H.* An estimate of the complexity requisite in a universal decision network / Wright Air Development Division. — Dayton, Ohio, 1960. — P. 197–212. — Technical Report 60–600.

125. *Carbonell J. G., Michalski R. S., Mitchell T. M.* An overview of machine learning // Machine learning. An artificial intelligence approach / Ed. by J. G. Carbonell, R. S. Michalski, T. M. Mitchell. — Berlin: Springer–Verlag, 1984. — P. 3–23.

126. *Chaselle B.* An optimal convex hull algorithm in any fixed dimension // Discrete Comput. Geom. — 1993. — N. 10. — P. 377–409.

127. *Cook W., Hartmann M., Kannan R., McDiarmid C.* On integer points in polyhedra // Combinatorica. — 1992. — V. 12, N. 1. — P. 27–37.

128. *Duda R. O., Fossum H.* Pattern classification by iteratively determined linear and piecewise linear discriminant functions // IEEE Transactions on Electronic Computers, EC-15. — 1966. — [Рус. пер.: *Дуда Р. О., Фоссум Х.* Классификация образов посредством последовательно определяемых линейных и кусочно-линейных

разделительных функций // Техническая кибернетика за рубежом. — М.: Машиностроение, 1968. — С. 34–58].

129. *Fernandez F., Quinton P.* Extension of Chernikova's Algorithm for Solving General Mixed Linear Programming Problems / INRIA. — Rennes, 1988. — Research Report RR-0943.

130. *Fukuda K., Prodon A.* Double description method revisited // Combinatorics and Computer Science / Ed. by M. Deza, R. Euler, I. Manoussakis. — Springer-Verlag, 1996. — P. 91–111.

131. *Goldberg P. W.* Learning fixed-dimension linear thresholds from fragmented data // Information and Computation. — 2001. — V. 171, N. 1. — P. 98–122.

132. *Goldman S. A., Kearns M. J.* On the complexity of teaching // Journal of Computer and System Sciences. — 1995. — V. 50. — P. 20–31.

133. *Grötschel M., Lovász L., Schrijver A.* Geometric algorithms and combinatorial optimization. — Berlin, Heidelberg: Springer–Verlag, 1988.

134. *Hansel G.* Sur le nombre des fonctions booléennes monotones de $n$ variables // C. R. Acad. Sci. Paris. — 1966. — V. 262, N. 20. — P. 1088–1090. — [Рус. пер.: *Ансель Ж.* О числе монотонных булевых функций $n$ переменных // Кибернетический сборник. Новая серия. Вып. 5. — М. Мир, 1968. — С. 53–57].

135. *Haukkanen P., Merikoski J. K.* Some formulas for numbers of line segments and lines in a rectangular grid // Ars Combinatoria. — 2012. — V. 104. — P. 353–361.

136. *Haukkanen P., Merikoski J. K.* Asymptotics of the number of threshold

functions on a two-dimensional rectangular grid // Discrete Applied Mathematics. — 2013. — V. 161, N. 1–2. — P. 13–18.

137. *Hausmann D., Korte B.* Lower bounds on the worst-case complexity of some oracle algorithms // Discrete Mathematics. — 1978. — V. 24, N. 3. — P. 261–272.

138. *Hegedüs T.* Geometrical concept learning and convex polytopes // Proc. 7 annual conf. on Computational learning theory (COLT'94). — New York: ACM Press, 1994. — P. 228–236.

139. *Hegedüs T.* Generalized teaching dimensions and the query complexity of learning // Proc. 8 annual conf. on Computational learning theory (COLT'95). — New York: ACM Press, 1995. — P. 108–117.

140. *Hellerstein L., Pillaipakkamnatt K., Wilkins D., Raghavan V.* How many queries are needed to learn // Journal of ACM. — 1996. — V. 43, N. 5. — P. 840–862.

141. *Håstad J.* On the size of weights for threshold gates // SIAM Journal on Discrete Mathematics. — 1994. — V. 7, N. 3. — P. 484–492.

142. *Irmatov A. A.* Arrangements of hyperplanes and the number of threshold functions // Acta Applicandae Mathematicae. — 2001. — V. 68, N. 1–3. — P. 211–226.

143. *Kleitman D.* On Dedekind's problem: the number of monotone boolean functions // Proc. Amer. Math. Soc. — 1969. — V. 21, N. 3. — P. 677–682. — [Рус. пер.: *Клейтмен Д.* О проблеме Дедекинда: число монотонных булевых функций // Кибернетический сборник. Новая серия. Вып. 7. — М.: Мир, 1970. — С. 43–52].

144. *Koplowitz J., Lindenbaum M., Bruckstein A. M.* The number of digital straight lines on an $n \times n$ grid // IEEE Trans. Inform. Theory. — 1990. — V. 36. — P. 192–197.

145. *Kwek S. S.* Geometric concept learning and related topics: Phd thesis / Graduate College of the University of Illinois. — Urbana-Champaign, 1997.

146. *Le Verge H.* A note on Chernikova's algorithm / INRIA. — Rennes, 1992. — Research Report RR-1662.

147. *Lenstra H. W.* Integer programming with a fixed number of variables // Mathematics of Operations Research. — 1983. — V. 8, N. 4. — P. 538–548.

148. *Lovász L.* An algorithmic theory of numbers, graphs and convexity. — Philadelphia, PA: Society for Industrial and Applied Mathematics, 1986.

149. *Maass W.* Lower bound methods and separation results for on-line learning models // Machine Learning. — 1992. — N. 9. — P. 107–145.

150. *Maass W., Turán G.* How fast can a threshold gate learn? // Computational Learning Theory and Natural Learning Systems: Constraints and Prospects. — MIT Press, 1994. — P. 381–414.

151. *McMullen P.* The maximum number of faces of a convex polytope // Mathematika. — 1970. — V. 17. — P. 179–184.

152. *Mitchell T.* Machine Learning. — McGraw-Hill Science/Engineering/Math, 1997.

153. *Motzkin T., Raiffa H., Thompson G., Thrall R.* The double description method // Contributions to Theory of Games / Ed. by H. Kuhn,

A.W.Tucker. — Princeton, RI: Princeton University Press, 1953. — V. 2. — P. 51–73. — [Рус. пер.: *Моцкин Т. С., Райфа Х., Томпсон Дж. Л., Тролл Р. М.* Метод двойного описания // Матричные игры / Под ред. Н. Н. Воробьева. — М.: Физматгиз, 1961].

154. *Muroga S.* Threshold logic and its applications. — N. Y.: Wiley, 1971.

155. *Mustonen S.* On lines and their intersection points in a rectangular grid of points. — 2009. — `www.survo.fi/papers/PointsInGrid.pdf`.

156. *Ngom A., Stojmenović I., Žunić J. D.* On the number of multilinear partitions and computing capacity of multiple-valued multiple threshold perceptrons // IEEE Transactions on Neural Networks. — 2003. — V. 14. — P. 469–477.

157. *Odlyzko A. M.* On subspaces spanned by random selections of $\pm 1$ vectors // Journal of Combinatorial Theory, A. — 1988. — V. 17, N. 1. — P. 124–133.

158. *Perkins D. T., Willis D. G., Whitmore E. A.* Division of space by concurrent hyperplanes / Lockheed Aircraft Corp. Missiles and Space Division. — Sunnyvale, Calif., 1959. — Internal Report.

159. *Schläfli L.* Gesammelte mathematisce Abhanglugen. Band 1. — Basel: Verlag Birkhäuzer, 1850.

160. *Shevchenko V. N., Zolotykh N. Y.* Decoding of threshold functions defined on the integer points of a polytope // Pattern recognition and image analysis. — 1997. — V. 7, N. 2. — P. 235–240.

161. *Shevchenko V. N., Zolotykh N. Y.* Lower bounds for the complexity

of learning half-spaces with membership queries // Lecture Notes in Computer Science. V. 1501. — Springer-Verlag, 1998. — P. 61–71.

162. *Žunić J. D.* Note on the number of two-dimensional threshold functions // SIAM Journal on Discrete Mathematics. — 2011. — V. 25, N. 3. — P. 1266–1268.

163. *Widrow B., Lehr M. A.* Adaptive signal processing. — Englewood-Cliffs, N. J.: Prentice-Hall, 1985.

164. *Winder R. O.* Single stage threshold logic // Minimization of Boolean Functions and Logic Design. Switching Circuit Theory and Logical Design. — AIEE Special Publication, 1961. — P. 321–332.

165. *Winder R. O.* The status of threshold logic // RCA Review. — 1969. — V. 30, N. 1. — P. 62–84.

166. *Yajima S., Ibaraki T.* A lower bound of the number of threshold functions // IEEE Trans. on Electronic Comput. — 1965. — V. 14, N. 6. — P. 929–929. — [Рус. пер.: *Яджима С., Ибараки Т.* Нижняя оценка числа пороговых функций // Кибернетический сборник. Новая серия. Вып. 6. — М.: Мир, 1969. — С. 72–81].

167. *Ziegler G. M.* Lectures on Polytopes. — Berlin, New York: Springer–Verlag, 1995.