ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2014. Том 21, № 5. С. 76–94

УДК 519.714.7

МИНИМАЛЬНЫЕ КОМПЛЕКСЫ ГРАНЕЙ СЛУЧАЙНОЙ БУЛЕВОЙ ФУНКЦИИ *)

И. П. Чухров

Аннотация. Для почти всех булевых функций n переменных доказано, что число минимальных относительно меры сложности комплексов граней не превосходит $2^{2^{n-1}(1+o(1))}$, если максимальная длина минимальных и длина кратчайших комплексов граней асимптотически равны. Для аддитивных мер сложности доказаны эффективно проверяемые достаточные условия, при которых асимптотически равны максимальная длина минимальных и длина кратчайших комплексов граней для почти всех булевых функций.

Ключевые слова: единичный куб, грань, комплекс граней, случайная булева функция, мера сложности, минимальный комплекс граней.

Введение

Исследование метрических параметров при минимизации булевых функций обычно рассматривается в двух постановках задач — оценка экстремальных или типичных значений, при этом для представления булевых функций применяются две эквивалентные модели — аналитическая и геометрическая. В аналитической модели используются понятия булевой функции, импликанты, дизъюнктивной нормальной формы (ДНФ) и т. д., зависящие от n переменных. В геометрической модели эквивалентными понятиями являются подмножество вершин, грань, комплекс граней и т. п. в n-мерном единичном кубе.

Оценкам сложности и числа минимальных ДНФ посвящены работы С. В. Яблонского, Ю. И. Журавлёва, Ю. Л. Васильева, В. В. Глаголева, А. А. Сапоженко, А. Д. Коршунова, Р. Г. Нигматуллина и др. Подробные обзоры полученных результатов представлены в [2, 12].

Верхние мощностные оценки для максимальных и типичных значений числа минимальных ДНФ булевой функции считались тривиальными, и ставилась задача получения нетривиальных верхних оценок

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 13–01–00958–а).

[2, с. 102]. Однако для максимальных значений числа кратчайших и минимальных ДНФ верхние оценки оказались достижимы по порядку логарифма [13, 14]. Для числа минимальных ДНФ у почти всех функций известна только верхняя оценка, которая превосходит число булевых функций n переменных. Нетривиальные нижние оценки числа минимальных ДНФ, т. е. хотя бы две минимальные ДНФ, для почти всех функций неизвестны.

При изложении будем использовать следующие понятия и обозначения для граней и множеств вершин единичного куба B^n.

Гранью единичного куба B^n называется множество вершин $\widetilde{x} = (x_1, \ldots, x_n) \in B^n$ таких, что $x_{i_1} = \sigma_1, \ldots, x_{i_k} = \sigma_k$, где $1 \leqslant i_s \leqslant n$ и $\sigma_s \in \{0, 1\}$ при $s = 1, \ldots, k$. *Рангом* и *размерностью* такой грани называются числа k и $n - k$ соответственно. Множество граней единичного куба B^n будем обозначать через $\mathcal{I}^n$.

Комплекс граней $M = \{I_r \in \mathcal{I}^n,\ r = 1, \ldots, l\}$ содержит множество вершин $N_M = \bigcup\limits_{r=1}^{l} I_r \subseteq B^n$ и называется *комплексом граней функции* $f \in P_n$, если множество N_M совпадает с множеством N_f, т. е. с *множеством единичных вершин функции* f в кубе B^n. Любая грань, содержащаяся в множестве N_f, называется *допустимой* гранью функции f.

Два комплекса граней называются *эквивалентными*, если они являются комплексами граней одной функции.

Комплекс граней называется *неприводимым*, если после удаления из него любой грани получается не эквивалентный комплекс граней, т. е. соответствующий другой функции.

Функционал, определённый на множестве всех комплексов граней (ДНФ), является мерой сложности, если он удовлетворяет аксиомам неотрицательности, монотонности относительно умножения, выпуклости относительно сложения и инвариантности относительно изоморфизма [15; 16, с. 298].

В дальнейшем рассматриваются меры сложности $\mathcal{L} \not\equiv 0$, т. е. отличные от тождественно нулевой меры сложности.

Комплекс граней называется *$\mathcal{L}$-минимальным*, если он имеет наименьшую меру сложности $\mathcal{L}$ среди всех эквивалентных комплексов граней.

Мера сложности, равная числу граней в комплексе M, называется *длиной* и обозначается через $l(M)$. Мера сложности, равная сумме рангов граней в комплексе M, называется *сложностью* и обозначается через $L(M)$. Комплекс граней, который имеет минимальное число граней или минимальную сумму рангов граней среди всех эквивалентных комплексов, называется *кратчайшим* или *минимальным* соответственно.

Примерами мер сложности могут быть функционалы: L_0 — число переменных с отрицанием и L_1 — число переменных без отрицания в ДНФ, т. е. число координат, равных 0 и 1 в гранях комплекса.

Мера сложности $\mathcal{L}$ называется *аддитивной*, если аксиома выпуклости выполняется в следующем виде: $\mathcal{L}(M) = \mathcal{L}(M_1) + \mathcal{L}(M_2)$ для любого представления комплекса граней M в виде объединения комплексов M_1 и M_2, не имеющих общих граней.

Для аддитивной меры сложности $\mathcal{L}$ и комплекса граней M имеет место равенство $\mathcal{L}(M) = \sum\limits_{I \in M} \mathcal{L}(I)$, т. е. сложность комплекса равна сумме сложностей граней комплекса.

При изучении свойств случайных булевых функций все функции n переменных из множества P_n считаются равновероятными, т. е. вероятность любой функции равна $|P_n|^{-1} = 2^{-2^n}$. Это эквивалентно вероятностной модели, в которой для любого набора значений переменных функция независимо с вероятностью $\frac{1}{2}$ может быть равна 0 или 1.

Для получения асимптотических утверждений рассматривается последовательность случайных булевых функций $\{f_n\}_{n=1}^{\infty}$, где $f_n \in P_n$. Говорят, что утверждение справедливо *для почти всех булевых функций*, если вероятность справедливости утверждения для функции f_n стремится к 1 при $n \to \infty$. Соответственно число функций n переменных, для которых утверждение справедливо, асимптотически равно 2^{2^n}, а число функций, для которых утверждение не справедливо, равно $o(2^{2^n})$.

Используемые, но не определяемые в этой статье понятия и определения можно найти в [2, 14]. Целую часть и верхнюю целую часть числа x будем обозначать через $\lfloor x \rfloor$ и $\lceil x \rceil$ соответственно. Под $\log$ всюду понимается логарифм по основанию 2. Под $H(x)$ понимается функция $H(x) = -x \log x - (1-x) \log (1-x)$ при $0 < x < 1$.

Далее всюду $o(1)$ означает величину, при $n \to \infty$ стремящуюся к нулю, а $\Theta(\varphi(n))$ для функции $\varphi(n) > 0$ — функцию $\psi(n) > 0$, для которой существуют $c_1 > 0$ и $c_2 > 0$ такие, что $c_1 \varphi(n) \leqslant \psi(n) \leqslant c_2 \varphi(n)$ при $n \to \infty$.

Для единичного куба B^n и целых i, k, удовлетворяющих условию $0 \leqslant i \leqslant i + k \leqslant n$, введём обозначения:

B_i^n — слой с номером i, т. е. вершины $\widetilde{x} \in B^n$, для которых $\|\widetilde{x}\| = i$;

$S_{i,i+k}^n$ — пояс, т. е. вершины слоёв B_j^n с номерами $j = i, \ldots, i+k$;

$\mathcal{I}_{i,i+k}^n$ — множество граней размерности k, которые содержатся в поясе $S_{i,i+k}^n$ единичного куба B^n; для граней такого множества минимальная вершина содержится в слое B_i^n, а максимальная — в слое B_{i+k}^n;

$\mathcal{L}^n(i, i+k)$ — $\mathcal{L}$-сложность грани из множества $\mathcal{I}_{i,i+k}^n$. Грани из множества $\mathcal{I}_{i,i+k}^n$ изоморфны. Следовательно, в силу аксиомы инвариантности относительно изоморфизма для любой меры сложности они имеют одинаковую сложность.

Очевидно, что меры сложности l, L, L_0, L_1 аддитивны и выполняются следующие соотношения: $l^n(i, i+k) = 1$, $L^n(i, i+k) = n-k$, $L_0^n(i, i+k) = n-k-i$, $L_1^n(i, i+k) = i$.

Множество и число комплексов из не более чем m различных граней размерности не более k в единичном кубе B^n обозначим через $\mathcal{G}^{n,k}(m)$ и $g_{n,k}(m)$ соответственно, где $0 \leqslant m$ и $0 \leqslant k \leqslant n$.

Множества допустимых и максимальных граней булевой функции f обозначим через G_f и S_f, а их мощности — через $g(f)$ и $s(f)$ соответственно.

Множество и число $\mathcal{L}$-минимальных комплексов граней булевой функции f обозначим через $\mathcal{M}_{\mathcal{L}}(f)$ и $\mu_{\mathcal{L}}(f)$. Максимальную длину для всех $\mathcal{L}$-минимальных комплексов граней булевой функции f обозначим через $l_{\mathcal{L}}(f) = \max\limits_{M \in \mathcal{M}_{\mathcal{L}}(f)} l(M)$. Очевидно, что для любой меры сложности $\mathcal{L}$ справедливо соотношение $l(f) = l_l(f) \leqslant l_{\mathcal{L}}(f)$.

Для функций из подмножества $\mathcal{P} \subseteq P_n$ максимальную длину $\mathcal{L}$-минимальных комплексов граней и множество $\mathcal{L}$-минимальных комплексов граней обозначим через $l_{\mathcal{L}}(\mathcal{P}) = \max\limits_{f \in \mathcal{P}} l_{\mathcal{L}}(f)$ и $\mathcal{M}_{\mathcal{L}}(\mathcal{P}) = \bigcup\limits_{f \in \mathcal{P}} \mathcal{M}_{\mathcal{L}}(f)$ соответственно.

Верхняя оценка числа $\mathcal{L}$-минимальных комплексов граней функции f может быть получена из очевидного соотношения

$$\mu_{\mathcal{L}}(f) \leqslant \sum_{i=l(f)}^{l_{\mathcal{L}}(f)} \binom{g(f)}{i}.$$

Так как $H(x) < x \log(e/x)$ для $0 < x < 1$, при $0 < q < p/2$ имеем

$$\log \binom{p}{q} < \log \sum_{i=0}^{q} \binom{p}{i} < pH(p/q) < q \log(ep/q).$$

Тогда при выполнении неравенства $l_{\mathcal{L}}(f) < g(f)/2$ приходим к оценке

$$\log \mu_{\mathcal{L}}(f) < l_{\mathcal{L}}(f) \log \frac{eg(f)}{l_{\mathcal{L}}(f)}.$$

Отметим, что при использовании свойств конкретной меры сложности, например, для кратчайших и минимальных комплексов граней, верхняя оценка может быть уточнена:

$$\mu_l(f) \leqslant \binom{g(f)}{l(f)}, \quad \mu_L(f) \leqslant \sum_{i=l(f)}^{l_L(f)} \binom{s(f)}{i}.$$

Через $\widetilde{\mathcal{P}}_n$ будем обозначать подмножество функций n переменных, содержащее почти все функции, которые обладают следующими свойствами.

1. Нет допустимых граней размерности более $k_0 = \lceil \log n \rceil$ [4].

2. Для числа допустимых граней при $k_2 = \lfloor \log\log n \rfloor$ и $k \leqslant k_0$ справедливы оценки [3]:

$$g_k(f) \sim \overline{g}_k(n) = \binom{n}{k} 2^{n-k-2^k},$$

$$g(f) \sim \overline{g}_{k_2}(n) + \overline{g}_{k_2+1}(n) = 2^n n^{\log\log n(1+o(1))}.$$

Поэтому $|N_f| \sim \overline{g}_0(n) = 2^{n-1}$ и число вершин множества N_f, которые содержатся в допустимых гранях функции размерности больше $k_1 = \lceil \log\log n + \log\log\log n \rceil$, не превосходит $2^n n^{-\log\log n(1-o(1))}$.

3. Для числа максимальных граней функций при $k \leqslant k_0$ справедливы оценки [11]:

$$s_k(f) \sim \overline{s}_k(n) = \binom{n}{k} 2^{n-k-2^k} \left(1 - 2^{-2^k}\right)^{n-k},$$

$$s(f) \sim \overline{s}_{k_2}(n) + \overline{s}_{k_2+1}(n) = 2^n n^{\log\log n(1+o(1))}.$$

Тем самым почти все максимальные грани функции имеют размерность либо k_2, либо $k_2 + 1$ и $g_k(f) \sim s_k(f)$ при $k > k_2$, т. е. почти все k-мерные допустимые грани функции максимальны.

4. $l_L(f) \sim l(f)$ и $L_l(f) \sim L(f) \sim nl(f)$, т. е. длина минимальных и кратчайших комплексов граней, а также сложность минимальных и кратчайших комплексов граней асимптотически равны [6].

5. $l(f) \sim \overline{l}(n)$, где $\overline{l}(n)$ — среднее значение длины кратчайшего комплекса граней функции [10, с. 94].

Оценкам длины кратчайших ДНФ для почти всех функций посвящены работы В. В. Глаголева [3], Р. Г. Нигматуллина [10], А. А. Сапоженко [11, 12], А. Д. Коршунова [7], С. Е. Кузнецова [8], А. Е. Андреева [1], Н. Пиппенгер [17]. Наилучшие известные результаты следующие:

$$l(f) \sim \overline{l}(n) = \overline{c}_n 2^n / \log n \log\log n,$$

где $1 \leqslant \bar{c}_n$ [8] и $\bar{c}_n \leqslant 1.5$ [1] или $\bar{c}_n \leqslant \omega(n)$ [17], при этом функция $\omega(n)$ зависит от *дробной части* $\log\log n + \log\log\log n$ и колеблется между $1.38826\ldots$ и $1.54169\ldots$ в зависимости от n.

Отметим, что для почти всех булевых функций уточнённые верхние оценки числа кратчайших и минимальных ДНФ с точностью до асимптотики логарифма совпадают и имеют вид

$$\log \mu_l(f) \lesssim \bar{c}_n 2^n \quad \text{и} \quad \log \mu_L(f) \lesssim \bar{c}_n 2^n,$$

так как

$$l(f) \log \frac{eg(f)}{l(f)} \sim l_L(f) \log \frac{es(f)}{l_L(f)} \sim \bar{c}_n 2^n \quad \text{при } n \to \infty.$$

Идея улучшения верхней оценки числа кратчайших комплексов граней для почти всех булевых функций основана на сравнении этой оценки с оценками:

(i) числа кратчайших комплексов граней типичных булевых функций из множества $\widetilde{\mathcal{P}}_n$, т. е. мощности множества $\mathcal{M}_l(\widetilde{\mathcal{P}}_n)$;

(ii) числа комплексов граней в единичном кубе B^n, в которых размерности и количество граней соответствуют значениям типичных булевых функций множества $\widetilde{\mathcal{P}}_n$.

Множество $\mathcal{M}_l(\widetilde{\mathcal{P}}_n)$ содержит различные комплексы граней, «близкие» к комплексам граней из множества $\mathcal{G}^{n,k}(m)$, где $m \sim \bar{l}(n)$ и $k \sim \log\log n$. Отличие может быть только за счёт граней большей размерности, но не более $k_0 = \lceil \log n \rceil$, и число таких граней равно $o\left(\frac{2^n}{n}\right)$. Оказывается, что эти оценки совпадают с точностью до асимптотики логарифма и превосходят в $\bar{c}_n$ раз логарифм числа всех функций. Тогда в силу неравенства Маркова число кратчайших комплексов граней типичных функций не может по порядку логарифма превосходить $2^{-2^n}|\mathcal{M}_l(\widetilde{\mathcal{P}}_n)|$ — среднего значения числа кратчайших комплексов граней для почти всех булевых функций. Поэтому с точностью до асимптотики логарифма возможно улучшение верхней оценки до величины

$$\log |\mathcal{M}_l(\widetilde{\mathcal{P}}_n)| - 2^n \lesssim (\bar{c}_n - 1)\, 2^n,$$

что существенно меньше числа всех функций n переменных.

Замечание. В единичном кубе B^n существует множество кратчайших комплексов граней с характерными для типичных функций размерностями граней $k \sim \log\log n$ и числом граней $m \sim c2^n/\log n \log\log n$, для которого асимптотика логарифма числа комплексов граней равна $c2^n$.

В [13, лемма 7] для $M_l(n,k,m)$ — числа кратчайших комплексов k-мерных граней длины m в единичном кубе B^n, где $k < \overline{k} = o(n)$ и $m \lesssim 2^{n-1}/e$ при $n \to \infty$, — получена нижняя оценка

$$\log M_l(n,k,m) \gtrsim m \log \binom{\overline{k}}{k}.$$

Поэтому при $\overline{k} = n/\log\frac{n}{k}$ имеем

$$\log M_l(n,k,m) \gtrsim mk \log \frac{n}{k} \sim mk\log n \sim c2^n.$$

Для аддитивных мер сложности представляется естественным, что при некоторых предположениях о свойствах функционала сложности $\mathcal{L}$, характеризующих максимальную и типичную $\mathcal{L}$-сложность граней, число граней в любом $\mathcal{L}$–минимальном комплексе асимптотически совпадает с длиной кратчайшего комплекса граней для почти всех функций. В таком случае верхние оценки числа $\mathcal{L}$–минимальных комплексов и числа кратчайших комплексов граней для почти всех функций совпадают с точностью до асимптотики логарифма.

Если сложность грани может иметь экспоненциальный рост, т. е. быть величиной порядка c^n в единичном кубе B^n, то основной вклад в значение сложности комплекса граней для случайной функции может определяться отдельными гранями. Например, рассмотрим аддитивную меру сложности $\mathcal{L}$ такую, что $\mathcal{L}(I) = c^{L_1(I)}$ для любой грани I. Для случайной функции почти всегда найдётся единичная вершина, «близкая» к вершине $\widetilde{1}$. Любая грань функции, содержащая такую вершину, имеет L_1-сложность, асимптотически равную n. При этом почти все единичные вершины расположены в средних слоях куба B^n и содержатся в гранях, для которых L_1-сложность асимптотически равна $n/2$. Тогда почти всегда для любого неприводимого комплекса граней M случайной функции, так как $l(M) < 2^n$, при $c > 4$ и $n \to \infty$ выполняется соотношение

$$\mathcal{L}(M) \gtrsim l(M)(1-o(1))\,c^{n/2(1-o(1))} + c^{n(1-o(1))} \sim c^{n(1-o(1))}.$$

1. Основные результаты

Теорема 1. *Если $l_{\mathcal{L}}(f) \sim l(f)$ для почти всех функций, то*

$$\log \mu_{\mathcal{L}}(f) \lesssim (\overline{c}_n - 1)\,2^n$$

при $n \to \infty$, где $\overline{c}_n$ определяется из соотношения для среднего значения длины кратчайшего комплекса граней булевой функции в n-мерном кубе:

$$\overline{l}(n) = \overline{c}_n 2^n/\log n \log\log n.$$

Из теоремы 1 следует, что для почти всех функций

$$\log \mu_l (f) \lesssim 2^{n-1} \quad \text{и} \quad \log \mu_{\mathcal{L}} (f) \lesssim 2^{n-1},$$

если $l_{\mathcal{L}} (f) \sim l (f)$, так как $\bar{c}_n \leqslant 1.5$ [1].

Теорема 2. *Для меры сложности $\mathcal{L} \not\equiv 0$ и любой грани I выполняется*

(i) *если $\mathcal{L} (I) = 0$, то $\min \{L_0 (I), L_1 (I)\} \leqslant R_{\mathcal{L}}^{\min}$,*

(ii) *если $\mathcal{L} (I) > 0$, то $\mathcal{L} (I) \geqslant C_{\mathcal{L}}^{\min} > 0$, где $R_{\mathcal{L}}^{\min}$ — минимальный ранг грани, которая имеет положительную $\mathcal{L}$-сложность, $C_{\mathcal{L}}^{\min}$ — положительная константа, зависящая только от меры сложности.*

Для меры сложности $\mathcal{L} \not\equiv 0$ это означает, во-первых, что нулевую сложность могут иметь только грани, в которых число координат, либо равных 0, либо равных 1, является конечным числом, не превосходящим $R_{\mathcal{L}}^{\min}$. Во-вторых, для граней ненулевой сложности существует минимальное положительное значение.

Следствие 1. *В единичном кубе B^n для меры сложности $\mathcal{L} \not\equiv 0$ все грани сложности нуль и размерности не более $k_0 = \lceil \log n \rceil$ содержатся в множестве $S_{0,p}^n \cup S_{n-p,n}^n$, где $p = R_{\mathcal{L}}^{\min} + k_0 = \Theta (1) + \log n$, и их число не превосходит $2^{\log^2 n (1+o(1))}$ при $n \to \infty$.*

Для аддитивных мер сложности в следующей теореме сформулированы достаточные условия для асимптотического равенства максимальной длины минимальных и длины кратчайших комплексов граней почти всех булевых функций.

Теорема 3. *Пусть для аддитивной меры сложности $\mathcal{L} \not\equiv 0$ в единичном кубе B^n при $n \to \infty$ выполняются условия*

(i) *максимальная $\mathcal{L}$-сложность граней ограничена полиномом от n,*

(ii) *грани размерности не более $k_0 = \lceil \log n \rceil$ и содержащиеся в средних слоях куба ширины $\Theta (\sqrt{n} \log n)$ имеют асимптотически одинаковую $\mathcal{L}$-сложность.*

Тогда для почти всех функций $l_{\mathcal{L}} (f) \sim l (f)$ при $n \to \infty$.

В силу аксиомы монотонности для мер сложности среди граней, которые имеют размерность не более k_0 и расположены в поясе куба $S_{r,n-r}^n$ ширины, большей k_0, минимальная сложность достигается на гранях размерности k_0, а максимальная — на гранях размерности 0. Поэтому условие (ii) теоремы 3 выполняется, если

$$\min_{i=r,\ldots,n-r-k_0} \mathcal{L}^n (i, i+k_0) \sim \max_{i=r,\ldots,n-r} \mathcal{L}^n (i, i)$$

для $r = n/2 - \Theta\left(\sqrt{n}\log n\right)$ и $k_0 = \lceil \log n \rceil$ при $n \to \infty$.

Следствие 2. *Пусть для аддитивной меры сложности функционал имеет вид* $L_Q(I) = Q(L_0(I), L_1(I))$, *где* $Q(x,y)$ — *произвольный полином двух переменных и* I — *грань куба. Тогда для почти всех функций* $l_{L_Q}(f) \sim l(f)$ *и для числа* L_Q*-минимальных комплексов граней почти всех функций справедлива оценка теоремы* 1.

2. Доказательства

Лемма 1. *Если* $0 \leqslant k \leqslant n$, $m < 2^{n-1}$ *и* $n \geqslant 2$, *то*

$$\log g_{n,k}(m) < mk\log n + m\log\frac{e2^n}{m}.$$

Доказательство. Очевидно, что $g_{n,k}(m) = \sum\limits_{s=0}^{m}\binom{I_{n,k}}{s}$, где $I_{n,k} = \sum\limits_{s=0}^{k} i_{n,s}$ — число граней размерности не более k и $i_{n,k} = \binom{n}{k}2^{n-k}$ — число k-мерных граней в единичном кубе B^n.

Тогда при $m < 2^{n-1} = \frac{1}{2}I_{n,0} \leqslant \frac{1}{2}I_{n,k}$ справедлива оценка

$$\begin{aligned} g_{n,k}(m) < I_{n,k}H\left(m/I_{n,k}\right) < m\log\frac{eI_{n,k}}{m} \\ = mk\log n + m\log\frac{e2^n}{m} + m\log\frac{I_{n,k}}{2^n n^k}. \end{aligned}$$

Покажем, что $\log\frac{I_{n,k}}{2^n n^k} \leqslant 0$ при $0 \leqslant k \leqslant n$ и $n \geqslant 2$, т. е.

$$a_{n,k} = \frac{I_{n,k}}{2^n n^k} = \frac{1}{n^k}\sum_{s=0}^{k}\binom{n}{s}2^{-s} \leqslant 1.$$

Действительно, имеем

$$a_{n,0} = 1,$$

$$a_{n,1} = \frac{1}{n}\left(1 + \frac{n}{2}\right) = \frac{1}{n} + \frac{1}{2} \leqslant 1,$$

$$a_{n,2} = \frac{1}{n^2} + \frac{1}{2n} + \frac{1 - 1/n}{2^3} < \frac{1}{4} + \frac{1}{4} + \frac{1}{8} = \frac{5}{8},$$

$$a_{n,k} < \frac{a_{n,2}}{n^{k-2}} + \frac{1}{n^k}\sum_{s=3}^{k}\left(\frac{en}{s}\right)^s 2^{-s} < \frac{5}{8n} + \sum_{s=3}^{k}2^{-s} < \frac{5}{8n} + \frac{1}{4} < 1,$$

$3 \leqslant s \leqslant k \leqslant n$, так как $\frac{1}{n^k}\left(\frac{en}{s}\right)^s \leqslant \left(\frac{e}{s}\right)^s \leqslant 1$. Лемма 1 доказана.

В единичном кубе B^n комплекс граней M булевой функции f для параметра d при условии $0 < d < n$ однозначно представляется в виде объединения двух комплексов $M = M_d^- \cup M_d^+$, которые не имеют общих граней, где

$$M_d^- = \left\{I \in M \mid \text{если } I' \in G_f \text{ и } I' \cap I \neq \varnothing, \text{ то } \dim I' \leqslant d\right\},$$
$$M_d^+ = M \setminus M_d^- = \left\{I \in M \mid \exists I' \in G_f \colon I' \cap I \neq \varnothing \text{ и } \dim I' > d\right\}$$

и $\dim I'$ — размерность грани I'.

Из определения множества M_d^- следует, что грань $I' \in G_f$ может совпадать с гранью I, т. е. все грани множества M_d^- имеют размерность не более d и эти грани не пересекаются с гранями размерности больше d, допустимыми для функции f. В множестве M_d^+ грани могут иметь любую размерность и пересекаются с гранями размерности больше d, допустимыми для функции f. Отметим, что $M_d^+ = \varnothing$, если $d > d_{\max}(f)$, где $d_{\max}(f)$ — максимальная размерность допустимых граней функции f.

Лемма 2. *Для любого подмножества булевых функций $\mathcal{P} \subset P_n$ и параметра d при условии $0 < d < n$ справедливо неравенство*

$$|\mathcal{M}_{\mathcal{L}}(\mathcal{P})| \leqslant \max\{|\mathcal{G}_d^-(\mathcal{P},\mathcal{L})|,\ 1\} \max\{|\mathcal{G}_d^+(\mathcal{P},\mathcal{L})|,\ 1\},$$

где

$$\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) = \{M_d^- \mid \exists M = M_d^- \cup M_d^+ \in \mathcal{M}_{\mathcal{L}}(f) \text{ и } f \in \mathcal{P}\},$$
$$\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) = \left\{M_d^+ \mid \exists M = M_d^- \cup M_d^+ \in \mathcal{M}_{\mathcal{L}}(f) \text{ и } f \in \mathcal{P}\right\}.$$

Доказательство. Для любого подмножества булевых функций $\mathcal{P} \subset P_n$ справедливо представление

$$\mathcal{M}_{\mathcal{L}}(\mathcal{P}) = \bigcup_{f\in\mathcal{P}} \mathcal{M}_{\mathcal{L}}(f) = \bigcup_{f\in\mathcal{P}} \bigcup_{M\in\mathcal{M}_{\mathcal{L}}(f)} M = \bigcup_{f\in\mathcal{P}} \bigcup_{M\in\mathcal{M}_{\mathcal{L}}(f)} \left(M_d^- \cup M_d^+\right).$$

Если $\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) = \varnothing$, т. е. все комплексы множества $\mathcal{M}_{\mathcal{L}}(\mathcal{P})$ состоят из граней, которые пересекаются с гранями размерности более d, то $\mathcal{M}_{\mathcal{L}}(\mathcal{P}) = \mathcal{G}_d^+(\mathcal{P},\mathcal{L})$ и $|\mathcal{M}_{\mathcal{L}}(\mathcal{P})| = \left|\mathcal{G}_d^+(\mathcal{P},\mathcal{L})\right|$.

Если $\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) = \varnothing$, т. е. все комплексы множества $\mathcal{M}_{\mathcal{L}}(\mathcal{P})$ состоят из граней и пересекаются только с гранями размерности не более d, то $\mathcal{M}_{\mathcal{L}}(\mathcal{P}) = \mathcal{G}_d^-(\mathcal{P},\mathcal{L})$ и $|\mathcal{M}_{\mathcal{L}}(\mathcal{P})| = \left|\mathcal{G}_d^-(\mathcal{P},\mathcal{L})\right|$.

Если $\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) \neq \varnothing$ и $\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \neq \varnothing$, то

$$\mathcal{M}_{\mathcal{L}}(\mathcal{P}) \subseteq \left\{M_1 \cup M_2 \mid M_1 \in \mathcal{G}_d^-(\mathcal{P},\mathcal{L}),\ M_2 \in \mathcal{G}_d^+(\mathcal{P},\mathcal{L})\right\}$$

и, следовательно, $|\mathcal{M}_{\mathcal{L}}(\mathcal{P})| \leqslant \left|\mathcal{G}_d^-(\mathcal{P},\mathcal{L})\right| \left|\mathcal{G}_d^+(\mathcal{P},\mathcal{L})\right|$. Лемма 2 доказана.

Лемма 3. *Для любого подмножества булевых функций* $\mathcal{P} \subseteq \widetilde{\mathcal{P}}_n \subset P_n$ *справедливы соотношения*

$$\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) \subseteq \mathcal{G}^{n,k_1}(m_1), \quad \mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \subseteq \mathcal{G}^{n,k_0}(m_0),$$

где $d = k_1 = \lceil \log\log n + \log\log\log n \rceil$, $l_{\mathcal{L}}(\mathcal{P}) \leqslant m_1$, $k_0 = \lceil \log n \rceil$ *и* $m_0 = \left\lceil \frac{2^n}{n} \right\rceil$ *при достаточно больших* n.

Доказательство. Очевидно, что $\mathcal{G}^{n,k}(m) \subseteq \mathcal{G}^{n,k'}(m')$, если $k \leqslant k'$ и $m \leqslant m'$.

(i) Если $\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) \neq \varnothing$, то $\mathcal{G}_d^-(\mathcal{P},\mathcal{L}) \subseteq \mathcal{G}^{n,d}(l_{\mathcal{L}}(\mathcal{P})) \subseteq \mathcal{G}^{n,k_1}(m_1)$, так как $d = k_1$ и $l_{\mathcal{L}}(\mathcal{P}) \leqslant m_1$.

(ii) Если $\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \neq \varnothing$, то $\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \subseteq \mathcal{G}^{n,d_{\max}(\mathcal{P},d)}(N_{\max}(\mathcal{P},d))$, где $d_{\max}(\mathcal{P},d)$ — максимальная размерность допустимых граней размерности более d для булевых функций из множества $\mathcal{P}$; $N_{\max}(\mathcal{P},d)$ — максимальное число единичных вершин функции из множества $\mathcal{P}$, которые содержатся в допустимых гранях функции размерности более d.

При условии $\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \neq \varnothing$ значения $d_{\max}(\mathcal{P},d)$ и $N_{\max}(\mathcal{P},d)$ определены, так как существует хотя бы одна функция в множестве $\mathcal{P}$, имеющая допустимую грань размерности более d.

Из свойств 1 и 2 определения множества функций $\widetilde{\mathcal{P}}_n$, следует, что при $d = k_1$ выполняются неравенства

$$d_{\max}(\mathcal{P},d) \leqslant d_{\max}(\widetilde{\mathcal{P}}_n,k_1) \leqslant k_0,$$
$$N_{\max}(\mathcal{P},d) \leqslant N_{\max}(\widetilde{\mathcal{P}}_n,k_1) \leqslant 2^n n^{-\log\log n(1+o(1))} = o(m_0).$$

Тогда

$$\mathcal{G}_d^+(\mathcal{P},\mathcal{L}) \subseteq \mathcal{G}_d^+(\widetilde{\mathcal{P}}_n,\mathcal{L}) \subseteq \mathcal{G}^{n,d_{\max}(\widetilde{\mathcal{P}}_n,k_1)}(N_{\max}(\widetilde{\mathcal{P}}_n,k_1)) \subseteq \mathcal{G}^{n,k_0}(m_0).$$

Лемма 3 доказана.

Доказательство теоремы 1. Используем лемму 1 для оценки значений $g_{n,k_0}(m_0)$ и $g_{n,k_1}(m_1)$ при $k_0 = \lceil \log n \rceil$, $m_0 = \left\lceil \frac{2^n}{n} \right\rceil = o(2^n)$, $k_1 = \lceil \log\log n + \log\log\log n \rceil$ и $m_1 \sim \bar{l}(n) = o(2^n)$. Отметим, что $m \log \frac{e2^n}{m} = o(2^n)$, если $m = o(2^n)$ при $n \to \infty$. Тогда

$$\log g_{n,k_0}(m_0) < m_0 k_0 \log n + m_0 \log \frac{e2^n}{m_0} \lesssim \frac{2^n \log^2 n}{n} + o(2^n) = o(2^n),$$

$$\log g_{n,k_1}(m_1) < m_1 k_1 \log n + m_1 \log \frac{e2^n}{m_1} \lesssim \bar{c}_n 2^n + o(2^n) \sim \bar{c}_n 2^n.$$

Пусть $\widetilde{\mathcal{Q}}_n \subseteq P_n$ — подмножество функций такое, что $l_{\mathcal{L}}(\widetilde{\mathcal{Q}}_n) \sim \bar{l}(n)$ и $|\widetilde{\mathcal{Q}}_n| \sim |P_n| = 2^{2^n}$. Тогда множество $\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n$ также содержит почти все функции и для $m_1 = l_{\mathcal{L}}(\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n) \leqslant l_{\mathcal{L}}(\widetilde{\mathcal{Q}}_n) \sim \bar{l}(n)$ при $n \to \infty$ выполняется неравенство

$$|\mathcal{M}_{\mathcal{L}}(\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n)| \leqslant g_{n,k_0}(m_0) g_{n,k_1}(m_1) \leqslant 2^{\overline{c}_n 2^n (1+o(1))}.$$

Поскольку $\mathcal{M}_{\mathcal{L}}(f_1) \cap \mathcal{M}_{\mathcal{L}}(f_2) = \varnothing$ для любых функций $f_1 \neq f_2$ из P_n, для среднего числа $\mathcal{L}$-минимальных комплексов граней подмножества функций $\mathcal{P} \subset P_n$ выполняется равенство

$$\overline{\mu}_{\mathcal{L}}(\mathcal{P}) = |\mathcal{P}|^{-1} \sum_{f \in \mathcal{P}} |\mathcal{M}_{\mathcal{L}(f)|} = |\mathcal{P}|^{-1} |\mathcal{M}_{\mathcal{L}}(\mathcal{P})|.$$

Следовательно, для функций из множества $\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n$ в силу неравенства Маркова при $\varepsilon_n = 1/n$ имеем

$$P\{f \in \widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n \mid \mu_{\mathcal{L}}(f) > \varepsilon_n^{-1} \overline{\mu}_{\mathcal{L}}(\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n)\} < \varepsilon_n.$$

Тогда с вероятностью не меньше $1 - \varepsilon_n \sim 1$ при $n \to \infty$ выполняется

$$\mu_{\mathcal{L}}(f) < n \overline{\mu}_{\mathcal{L}}(\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n) \lesssim n 2^{-2^n} |\mathcal{M}_{\mathcal{L}}(\widetilde{\mathcal{P}}_n \cap \widetilde{\mathcal{Q}}_n)| = 2^{(\overline{c}_n - 1) 2^n (1+o(1))}.$$

Теорема 1 доказана.

Замечание. Нижняя оценка $\overline{c}_n \geqslant 1$ [8, 17] при $n \to \infty$ следует из того факта, что предположение $\overline{c}_n < 1$ приводит к противоречию:

$$2^{2^n} \sim |\widetilde{\mathcal{P}}_n| \leqslant |\mathcal{M}_l(\widetilde{\mathcal{P}}_n)| \leqslant 2^{\overline{c}_n 2^n (1+o(1))} = o(2^{2^n}), \quad \text{если } \overline{c}_n < 1.$$

Для доказательства теоремы 2 рассмотрим множество $\mathcal{K} = \bigcup\limits_{r=1}^{\infty} \mathcal{K}^r$, где $\mathcal{K}^r = \{K_{r,0}, K_{r-1,1}, \ldots, K_{1,r-1}, K_{0,r}\}$ — элементарные конъюнкции (ЭК) ранга r и вида $K_{r-s,s} = x_1 \ldots x_{r-s} \overline{x}_{r-s+1} \ldots \overline{x}_r$ для $s = 0, \ldots, r$ и $r = 1, 2, \ldots$. Например, $\mathcal{K}^1 = \{K_{1,0}, K_{0,1}\} = \{x_1, \overline{x}_1\}$, $\mathcal{K}^2 = \{K_{2,0}, K_{1,1}, K_{0,2}\} = \{x_1 x_2, x_1 \overline{x}_2, \overline{x}_1 \overline{x}_2\}$ и т. д.

Очевидно, что в множестве $\mathcal{K}^r$ нет изоморфных ЭК и любая ЭК ранга r изоморфна некоторой ЭК из множества $\mathcal{K}^r$, при этом ЭК различного ранга не могут быть изоморфными. На множестве $\mathcal{K}$ определим отношение строгого частичного порядка $\succ$ следующим образом: $K' \succ K$ тогда и только тогда, когда ЭК K может быть получена из ЭК K' удалением одной или нескольких переменных. Из определения отношения $\succ$ следует, что непосредственно предшествующими ЭК в множестве $\mathcal{K}$ являются

$K_{r,0} \succ K_{r-1,0}$, $K_{0,r} \succ K_{0,r-1}$ — для ЭК, которая содержит все переменные либо без отрицания, либо с отрицанием, где $r = 2, 3, \ldots$;

$K_{r-s,s} \succ K_{r-s,s-1}$ и $K_{r-s,s} \succ K_{r-s-1,s}$ — для ЭК, которая содержит переменные и без отрицания, и с отрицанием, где $r = 2, 3, \ldots$ и $s = 1, \ldots, r-1$.

Пусть

$\overline{\mathcal{K}} = \{K \in \mathcal{K} \mid \mathcal{L}(K) = 0$ и если $K' \succ K$, то $\mathcal{L}(K') > 0\}$ — множество «верхних» ЭК нулевой сложности;

$\underline{\mathcal{K}} = \{K \in \mathcal{K} \mid \mathcal{L}(K) > 0$ и если $K \succ K'$, то $\mathcal{L}(K') = 0\}$ — множество «нижних» ЭК положительной сложности.

Из определения множеств $\overline{\mathcal{K}}$ и $\underline{\mathcal{K}}$ следует, что в каждом из них нет сравнимых элементов, т. е. они являются антицепями.

Лемма 4. *Для произвольной меры сложности $\mathcal{L} \not\equiv 0$ справедливы утверждения*

(i) $\left|\overline{\mathcal{K}}\right| \leqslant R_{\mathcal{L}}^{\min}$ *и* $\min\{L_0(K'), L_1(K')\} \leqslant R_{\mathcal{L}}^{\min} - 1$ *для* $K' \in \overline{\mathcal{K}}$,

(ii) $|\underline{\mathcal{K}}| \leqslant R_{\mathcal{L}}^{\min} + 1$ *и* $\min\{L_0(K'), L_1(K')\} \leqslant R_{\mathcal{L}}^{\min}$ *для* $K' \in \underline{\mathcal{K}}$,

где $R_{\mathcal{L}}^{\min}$ — минимальный ранг ЭК, которая имеет положительную $\mathcal{L}$-сложность.

Доказательство. Пусть ЭК $K = K_{r-s,s} \in \mathcal{K}^r$, $0 \leqslant s \leqslant r$, $r \geqslant 1$, имеет минимальный ранг с положительной сложностью, т. е. $\mathcal{L}(K) > 0$ и $r = R_{\mathcal{L}}^{\min}$.

Пусть $M_K = \{K' \in \mathcal{K} \mid K' \succ K\} \cup \{K\}$. Тогда $\mathcal{L}(K') \geqslant \mathcal{L}(K) > 0$ для любой ЭК $K' \in M_K$ в силу определения отношения $\succ$. Это означает, что $\overline{\mathcal{K}} \cap M_K = \varnothing$ и $\underline{\mathcal{K}} \cap M_K = K$, т. е. $\overline{\mathcal{K}} \subseteq \mathcal{K} \setminus M_K$ и $\underline{\mathcal{K}} \subseteq (\mathcal{K} \setminus M_K) \cup \{K\}$.

Отметим, что для любой ЭК $K' \in \mathcal{K}$, если $\min L_0(K')$, $L_1(K') \geqslant r$, то $K' \succ K_{r-s,s} = K$ при любом $s = 0, \ldots, r$, следовательно, $K' \in M_K$. Поэтому $\min\{L_0(K'), L_1(K')\} \leqslant r-1$ для любой ЭК $K' \in \mathcal{K} \setminus M_K$. Тогда

из $\overline{\mathcal{K}} \subseteq \mathcal{K} \setminus M_K$ следует, что $\min\{L_0(K'), L_1(K')\} \leqslant r-1$ для любой ЭК $K' \in \overline{\mathcal{K}}$;

из $\underline{\mathcal{K}} \subseteq (\mathcal{K} \setminus M_K) \cup \{K\}$ следует, что $\min\{L_0(K'), L_1(K')\} \leqslant r$ для любой ЭК $K' \in \underline{\mathcal{K}}$, при этом равенство r достигается, если $K_{r,0} \in \underline{\mathcal{K}}$ или $K_{0,r} \in \underline{\mathcal{K}}$.

Для доказательства неравенств $\left|\overline{\mathcal{K}}\right| \leqslant R_{\mathcal{L}}^{\min}$ и $|\underline{\mathcal{K}}| \leqslant R_{\mathcal{L}}^{\min} + 1$ рассмотрим два случая.

Случай 1: $r = 1$, т. е. $\mathcal{L}(K) > 0$ для $K = K_{1-s,s} \in \mathcal{K}^1 = \{K_{1,0}, K_{0,1}\} = \{x_1, \overline{x}_1\}$, где $s \in \{0, 1\}$.

Если $\mathcal{L}(K_{s,1-s}) > 0$, то $\overline{\mathcal{K}} = \varnothing$ и $\underline{\mathcal{K}} = \mathcal{K}^1$. Следовательно, $\left|\overline{\mathcal{K}}\right| = 0 \leqslant 1 = R_{\mathcal{L}}^{\min}$ и $|\underline{\mathcal{K}}| = 2 = R_{\mathcal{L}}^{\min} + 1$.

Если $\mathcal{L}(K_{s,1-s}) = 0$, то положим $C = \mathcal{K} \setminus M_K = \{K_{s,1-s+t}\}_{t=0}^{\infty}$. Множество $C \subset \mathcal{K}$ является бесконечной цепью из непосредственно предшествующих ЭК, так как $K_{s,1-s+t+1} \succ K_{s,1-s+t}$ для $t = 0, 1, \ldots$.

Поскольку в множествах $\overline{\mathcal{K}}$ и $\underline{\mathcal{K}}$ нет сравнимых элементов, $\left|\overline{\mathcal{K}} \cap C\right| \leqslant 1$ и $|\underline{\mathcal{K}} \cap C| \leqslant 1$, при этом $\overline{\mathcal{K}} \cap M_K = \varnothing$ и $\underline{\mathcal{K}} \cap M_K = K$. Стало быть, $\left|\overline{\mathcal{K}}\right| \leqslant 1 = R_{\mathcal{L}}^{\min}$ и $|\underline{\mathcal{K}}| \leqslant 2 = R_{\mathcal{L}}^{\min} + 1$.

Случай 2: $r \geqslant 2$, т. е. $\mathcal{L}(K) > 0$ для $K = K_{r-s,s} \in \mathcal{K}^r$, где $0 \leqslant s \leqslant r$. Представим множество ЭК ранга не менее $r-1$ в виде

$$\bigcup_{t=r-1}^{\infty} \mathcal{K}^t = M_K^- \cup M_K \cup M_K^+,$$

где

$$M_K^- = \begin{cases} \varnothing, & \text{если } s = r, \text{ т. е. для } K = K_{0,r}, \\ \left\{C_i^-\right\}_{i=1}^{r-s}, & \text{если } s = 0, \ldots, r-1, \text{ где } C_i^- = \{K_{r-s-i,s+i+t-1}\}_{t=0}^{\infty}, \end{cases}$$

$$M_K^+ = \begin{cases} \varnothing, & \text{если } s = 0, \text{ т. е. для } K = K_{r,0}, \\ \left\{C_j^+\right\}_{j=1}^{s}, & \text{если } s = 1, \ldots, r, \text{ где } C_j^+ = \{K_{r-s+j+t-1,s-j}\}_{t=0}^{\infty}. \end{cases}$$

Очевидно, что множества M_K^-, M_K, M_K^+ попарно не пересекаются и непустые множества M_K^- и M_K^+ представляются в виде объединения бесконечных цепей из непосредственно предшествующих ЭК.

В множестве $\overline{\mathcal{K}}$ могут содержаться только ЭК ранга не менее $r-1$, так как любая ЭК ранга $r-1$ и меньше имеет $\mathcal{L}$-сложность, равную 0. Тогда $\overline{\mathcal{K}} \subset M_K^- \cup M_K^+$. Поскольку в множестве $\overline{\mathcal{K}}$ нет сравнимых элементов, $|\overline{\mathcal{K}} \cap C_i^-| \leqslant 1$ и $|\overline{\mathcal{K}} \cap C_j^+| \leqslant 1$, где $i = 1, \ldots, r-s$, $j = 1, \ldots, s$, следовательно, $|\overline{\mathcal{K}}| = |\overline{\mathcal{K}} \cap (M_K^- \cup M_K^+)| \leqslant r = R_{\mathcal{L}}^{\min}$.

В множестве $\underline{\mathcal{K}}$ могут содержаться только ЭК ранга не менее r. Тогда $\underline{\mathcal{K}} \subset M_K^- \cup \{K\} \cup M_K^+$. Так как в множестве $\underline{\mathcal{K}}$ нет сравнимых элементов, $|\underline{\mathcal{K}} \cap C_i^-| \leqslant 1$ и $|\underline{\mathcal{K}} \cap C_j^+| \leqslant 1$, где $i = 1, \ldots, r-s$, $j = 1, \ldots, s$, следовательно, $|\underline{\mathcal{K}}| \leqslant r + 1 = R_{\mathcal{L}}^{\min} + 1$. Лемма 4 доказана.

Доказательство теоремы 2. Любой грани единичного куба взаимно однозначно соответствует ЭК, для которой есть изоморфная ЭК из множества $\mathcal{K}$, имеющая тем самым такую же сложность в силу аксиомы инвариантности относительно изоморфизма. Поэтому достаточно доказать утверждение теоремы для ЭК из множества $\mathcal{K}$.

Для любой меры сложности $\mathcal{L} \not\equiv 0$ число $R_{\mathcal{L}}^{\min}$ является константой, зависящей только от меры сложности, следовательно, множества $\underline{\mathcal{K}}$ и $\overline{\mathcal{K}}$ конечны. Поэтому для $K' \in \mathcal{K}$ имеем

(i) Если $\mathcal{L}(K') = 0$ и $K' \notin \overline{\mathcal{K}}$, то найдётся $K \in \overline{\mathcal{K}}$ и $K \succ K'$. Тогда $\min\{L_0(K'), L_1(K')\} \leqslant \min\{L_0(K), L_1(K)\} \leqslant R_{\mathcal{L}}^{\min}$.

(ii) Если $\mathcal{L}(K') > 0$ и $K' \notin \underline{\mathcal{K}}$, то найдётся $K \in \underline{\mathcal{K}}$ и $K' \succ K$. Тогда

$$\mathcal{L}(K') \geqslant \mathcal{L}(K) \geqslant C_{\mathcal{L}}^{\min} = \min_{K \in \underline{\mathcal{K}}} \mathcal{L}(K) > 0.$$

Теорема 2 доказана.

Доказательство следствия 1. Из теоремы 2 вытекает, что любая грань I в единичном кубе B^n, имеющая $\mathcal{L}$-сложность, равную 0, и размерность не более k_0, может содержать только вершины $\widetilde{x} \in B^n$, для которых $\min\{n - \|\widetilde{x}\|, \|\widetilde{x}\|\} + k_0 \leqslant p = R_{\mathcal{L}}^{\min} + k_0$. Следовательно, $I \subset S_{0,p}^n \cup S_{n-p,n}^n$ и число таких граней при $n \to \infty$ не превосходит

$$\left(\left|S_{0,p-k_0}^n\right| + \left|S_{n-p+k_0,n}^n\right|\right)\left|S_{0,k_0}^n\right| \sim 2\binom{n}{p-k_0}\binom{n}{k_0} < 2n^{p+k_0} = 2^{\log^2 n(1+o(1))}.$$

Доказательство теоремы 3. В силу справедливости неравенства $l(f) \leqslant l_{\mathcal{L}}(f)$ достаточно доказать, что $l_{\mathcal{L}}(f) \lesssim l(f)$.

Пусть M_1 — $\mathcal{L}$-минимальный комплекс граней максимальной длины и M_2 — кратчайший комплекс граней для функции $f \in \widetilde{P}_n$, т. е. $l(M_1) = l_{\mathcal{L}}(f) \geqslant l(f) = l(M_2)$ и $\mathcal{L}(f) = \mathcal{L}(M_1) \leqslant \mathcal{L}(M_2)$.

Докажем, что если $\mathcal{L}_{\max}^n = \max\limits_{I \subset B^n} \mathcal{L}(I) \leqslant n^{\Theta(1)}$ и $r = \frac{n}{2} - \Theta(\sqrt{n}\log n)$ при $n \to \infty$, то

$$l_{\mathcal{L}}(f)\,\widetilde{\mathcal{L}}_{\min}^n(r, n-r) \lesssim \mathcal{L}(M_1) \leqslant \mathcal{L}(M_2) \lesssim l(f)\,\widetilde{\mathcal{L}}_{\max}^n(r, n-r),$$

где $\widetilde{\mathcal{L}}_{\min}^n(r, n-r)$ и $\widetilde{\mathcal{L}}_{\max}^n(r, n-r)$ — минимальная и максимальная сложности граней размерности не более k_0, которые содержатся в поясе $S_{r,n-r}^n$.

Комплекс граней $M_1 \in \mathcal{M}_{\mathcal{L}}(f)$ может не быть неприводимым, если есть грани $\mathcal{L}$-сложности, равной 0. Грани функций из множества $\widetilde{P}_n$ имеют размерность не более $k_0 = \lceil \log n \rceil$ и в силу следствия 1 такие грани содержатся в $S_{0,p}^n \cup S_{n-p,n}^n$, где $p = \Theta(1) + \log n$. Число таких граней не превосходит $2^{\log^2 n(1+o(1))}$, а сложность любой грани $I \not\subset S_{0,p}^n \cup S_{n-p,n}^n$ не меньше положительной константы $C_{\mathcal{L}}^{\min}$. Поэтому комплекс граней $\widehat{M}_1 = \{I \in M_1 \in \mathcal{M}_{\mathcal{L}}(f) \mid I \not\subset S_{0,p}^n \cup S_{n-p,n}^n\}$ для аддитивной меры сложности $\mathcal{L}$ является неприводимым и каждая грань имеет собственную вершину, которая не содержится ни в одной другой грани $\mathcal{L}$-минимального комплекса M_1.

Для $t = \left\lfloor \frac{n}{2} + \frac{\sqrt{n}}{2} x \right\rfloor$, где $x = o(n^{1/6})$ и $x \to \infty$ при $n \to \infty$, справедливо асимптотическое равенство

$$\left|S^n_{t,n}\right| = \sum_{i \geqslant t} \binom{n}{i} \sim 2^n \frac{e^{-x^2/2}}{x\sqrt{2\pi}}.$$

Тогда для $x = \sqrt{2a}\ln n$, где $a > 0$, имеем

$$\left|S^n_{t,n}\right| \sim \frac{2^n}{n^{a\ln n} 2\sqrt{\pi a}\ln n} = o\left(\frac{2^n}{n^{a\ln n}}\right),$$

значит, $\left|B^n \setminus S^n_{t,n-t}\right| = o\left(2^n / n^{\Theta(\log n)}\right)$ для $t = \frac{n}{2} - \Theta\left(\sqrt{n}\log n\right)$.

Для любого неприводимого комплекса граней размерности не более k_0, которые содержатся или пересекаются с $B^n \setminus S^n_{r,n-r}$, где $r = \frac{n}{2} - \Theta\left(\sqrt{n}\log n\right)$, собственные вершины таких граней содержатся в $B^n \setminus S^n_{r+k_0,n-r-k_0}$. Поскольку $\frac{n}{2} - r - k_0 = \Theta\left(\sqrt{n}\log n\right)$, число граней в таком неприводимом комплексе есть $o\left(\frac{2^n}{n^{\Theta(\log n)}}\right)$. Тогда в комплексе $M_1 \in \mathcal{M}_{\mathcal{L}}(f)$ не менее $l_{\mathcal{L}}(f) - \frac{2^n}{n^{\Theta(\log n)}} - 2^{\log^2 n(1+o(1))}$ граней содержатся в $S^n_{r,n-r}$ и имеют сложность не менее $\widetilde{\mathcal{L}}^n_{\min}(r, n-r)$. Следовательно, справедлива оценка

$$\left(l_{\mathcal{L}}(f) - \frac{2^n}{n^{\Theta(\log n)}} - 2^{\log^2 n(1+o(1))}\right)\widetilde{\mathcal{L}}^n_{\min}(r, n-r) \leqslant \mathcal{L}(M_1).$$

Учитывая, что $l_{\mathcal{L}}(f) \geqslant l(f) \sim \bar{l}(n)$, $\frac{2^n}{n^{\Theta(\log n)}} = o(\bar{l}(n))$, $2^{\log^2 n(1+o(1))} = o(\bar{l}(n))$, так как $\bar{l}(n) = \Theta\left(\frac{2^n}{\log n \log\log n}\right)$, получаем

$$l_{\mathcal{L}}(f)\,\widetilde{\mathcal{L}}^n_{\min}(r, n-r) \lesssim \mathcal{L}(M_1).$$

Кратчайший комплекс граней $M_2 \in \mathcal{M}_l(f)$ неприводим и состоит из граней размерности не более k_0. Поэтому для граней комплекса M_2, которые содержатся или пересекаются с $B^n \setminus S^n_{r,n-r}$, где $r = \frac{n}{2} - \Theta\left(\sqrt{n}\log n\right)$, собственные вершины граней содержатся в $B^n \setminus S^n_{r+k_0,n-r-k_0}$. Следовательно, число таких граней в комплексе M_2 есть $o\left(\frac{2^n}{n^{\Theta(\log n)}}\right)$ и сложность любой такой грани не более $\mathcal{L}^n_{\max}$. Остальные грани содержатся в $S^n_{r,n-r}$ и имеют сложность не более $\widetilde{\mathcal{L}}^n_{\max}(r, n-r)$. Учитывая, что $l(f) \sim \bar{l}(n)$, $\frac{2^n}{n^{\Theta(\log n)}} = o(\bar{l}(n))$, $\frac{2^n}{n^{\Theta(\log n)}}\mathcal{L}^n_{\max} \leqslant \frac{2^n}{n^{\Theta(\log n)}} n^{\Theta(1)} = o(\bar{l}(n))$ и $\widetilde{\mathcal{L}}^n_{\max}(r, n-r) \geqslant C^{\min}_{\mathcal{L}}$ получаем

$$\mathcal{L}(M_2) \leqslant \left(l(f) - \frac{2^n}{n^{\Theta(\log n)}} \right) \widetilde{\mathcal{L}}^n_{\max}(r, n-r) + \frac{2^n}{n^{\Theta(\log n)}} \mathcal{L}^n_{\max}$$
$$\lesssim l(f) \widetilde{\mathcal{L}}^n_{\max}(r, n-r) + o\left(\bar{l}(n)\right) \sim l(f) \widetilde{\mathcal{L}}^n_{\max}(r, n-r).$$

Тем самым доказано неравенство

$$l_{\mathcal{L}}(f) \widetilde{\mathcal{L}}^n_{\min}(r, n-r) \lesssim l(f) \widetilde{\mathcal{L}}^n_{\max}(r, n-r).$$

Так как $\widetilde{\mathcal{L}}^n_{\min}(r, n-r) \geqslant C^{\min}_{\mathcal{L}} > 0$, в силу условия (ii) теоремы 3 из этого неравенства следует, что $l_{\mathcal{L}}(f) \lesssim l(f)$. Теорема 3 доказана.

Доказательство следствия 2. Условие (i) теоремы 3 выполняется, поскольку $\max\{L_0(I), L_1(I)\} \leqslant n$ для любой грани и функционал сложности $Q(x, y)$ является полиномом.

Условие (ii) теоремы 3 выполняется, так как $L_0(I) \sim L_1(I) = \frac{n}{2} + o(n)$ для любой грани I, содержащейся в средних слоях куба ширины $\Theta(\sqrt{n}\log n)$, и $Q\left(\frac{n}{2} + o(n), \frac{n}{2} + o(n)\right) \sim Q\left(\frac{n}{2}, \frac{n}{2}\right)$ для полинома $Q(x, y)$ при $n \to \infty$. Следствие 2 доказано.

3. Открытые проблемы

Известные примеры булевых функций [5, 9, 15], которые имеют минимальные комплексы граней, не являющиеся кратчайшими, основаны на следующем свойстве. У функции есть несколько единичных вершин, которые содержатся либо в одной или нескольких гранях большого ранга кратчайшего комплекса, либо в большем числе граней меньшего ранга минимального комплекса. При этом сумма рангов таких граней в минимальном комплексе должна быть меньше суммы рангов соответствующих граней в кратчайшем комплексе. Выполнение этого условия достигается за счёт граней минимального комплекса, которые имеют размерность, сравнимую с размерностью единичного n-мерного куба, и тем самым малый ранг. Но у почти всех функций в единичном n-мерном кубе максимальные грани имеют ранг, асимптотически равный n. Представляется естественным, что доля функций, имеющих минимальные и не кратчайшие комплексы граней, «мала». Поэтому возникает вопрос о справедливости следующего утверждения.

Гипотеза. *Минимальные комплексы граней являются кратчайшими для почти всех функций, т. е.* $l_L(f) = l(f)$.

Также представляется интересным для исследования вопрос о существовании меры сложности $\mathcal{L}$, которая удовлетворяет одному из следующих условий.

(a) Для почти всех функций верно неравенство $l_{\mathcal{L}}(f) > l(f)$, т. е. существует $\mathcal{L}$-минимальный и не кратчайший комплекс граней.

(b) В единичном кубе B^n рост $\mathcal{L}$-сложности граней ограничен полиномом от n, но грани размерности не более $k_0 = \lceil \log n \rceil$, содержащиеся в средних слоях куба ширины $\Theta(\sqrt{n} \log n)$, могут иметь не асимптотически одинаковую $\mathcal{L}$-сложность. Это означает, что выполнения только условия (i) не достаточно для справедливости теоремы 3.

ЛИТЕРАТУРА

1. **Андреев А. Е.** Об одной модификации градиентного алгоритма // Вестн. МГУ. Математика. Механика. — 1985. — № 3. — С. 29–35.
2. **Васильев Ю. Л., Глаголев В. В.** Метрические свойства дизъюнктивных нормальных форм // Дискретная математика и математические вопросы кибернетики. Т. 1. — М.: Наука, 1974. — С. 99–148.
3. **Глаголев В. В.** Некоторые оценки ДНФ булевых функций алгебры логики // Пробл. кибернетики. — 1967. — № 19. — С. 75–94.
4. **Журавлёв Ю. И.** Оценка для числа тупиковых д.н.ф. функций алгебры логики // Сиб. мат. журн. — 1962. — Т. 3, № 5. — С. 802–804.
5. **Журавлёв Ю. И.** Алгоритмы построения минимальных ДНФ // Дискретная математика и математические вопросы кибернетики. Т. 1. — М.: Наука, 1974. — С. 67–98.
6. **Коршунов А. Д.** Сравнение сложности длиннейших и кратчайших ДНФ и нижняя оценка числа тупиковых ДНФ для почти всех булевых функций // Кибернетика. — 1969. — № 4. — С. 1–11.
7. **Коршунов А. Д.** О сложности кратчайших дизъюнктивных нормальных форм случайных булевых функций // Методы дискретного анализа в оптимизации управляющих систем. — Новосибирск: Ин-т математики СО АН СССР, 1983. — № 40. — С. 25–53.
8. **Кузнецов С. Е.** О нижней оценке длины кратчайшей ДНФ почти всех булевых функций // Вероятностные методы и кибернетика. — Казань: Изд-во Казан. ун-та, 1983. — № 19. — С. 44–47.
9. **Лин Син-Лян.** О сравнении сложностей минимальных и кратчайших дизъюнктивных нормальных форм для функций алгебры логики // Пробл. кибернетики. — 1967. — № 18. — С. 11–44.
10. **Нигматуллин Р. Г.** Сложность булевых функций. — М.: Наука, 1991. — 240 с.
11. **Сапоженко А. А.** Введение в дискретную математику. — М.: Изд-во МГУ, 1975. — 90 с.
12. **Сапоженко А. А., Чухров И. П.** Минимизация булевых функций в классе дизъюнктивных нормальных форм // Итоги науки и техники. Сер. Теория вероятности. Мат. статистика. Теор. кибернетика. — 1987. — Т. 25. — С. 68–116.

13. **Чухров И. П.** О ядровых и кратчайших комплексах граней в единичном кубе // Дискрет. анализ и исслед. операций. — 2011. — Т. 18, № 2. — С. 75–94.
14. **Чухров И. П.** О минимальных комплексах граней в единичном кубе // Дискрет. анализ и исслед. операций. — 2012. — Т. 19, № 3. — С. 79–99.
15. **Чухров И. П.** О мерах сложности комплексов граней в единичном кубе // Дискрет. анализ и исслед. операций. — 2013. — Т. 20, № 6. — С. 77–94.
16. **Яблонский С. В.** Введение в дискретную математику. — М.: Высш. шк., 2003. — 384 с.
17. **Pippenger N.** The shortest disjunctive normal form of a random Boolean function // Random Struct. Algorithms. — 2003. — Vol. 22, N 2. — P. 161–186.

Чухров Игорь Петрович,
e-mail: chip@icad.org.ru

Статья поступила
19 декабря 2013 г.