ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 1997. Том 4, № 2, 75–111

УДК 519.7

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ СУЖЕНИЙ БУЛЕВЫХ ФУНКЦИЙ*)

А. В. Чашкин

Изучается сложность сужений булевых функций при их реализации различными управляющими системами. Установлены нижние оценки для сложности самых сложных сужений на области фиксированной мощности. Показано, что в случае схем из функциональных элементов полученные оценки оптимальны по порядку. Установлено, что для каждой булевой функции от n переменных, сложность реализации которой схемами из функциональных элементов превышает величину $n^{2+\epsilon}$, ϵ — произвольная положительная константа, найдется область в $\{0,1\}^n$, сужение на которую имеет нелинейную сложность, и эта сложность не более чем в постоянное число раз отличается от сложности самой сложной частичной функции, определенной в данной области. Доказано, что любая булева функция от n переменных однозначно определяется по своим значениям не более чем в n областях, мощности которых не более чем в полиномиальное (относительно n) число раз превосходят сложность функции.

Введение

Пусть $f(x_1,\ldots,x_n)$ — произвольная булева функция. Сложностью $L(f)$ функции f называется число элементов в минимальной схеме из функциональных элементов в базисе $\{\vee,\&,\bar{}\}$, реализующей функцию f. Сложностью $L_k(f)$ функции f называется число контактов в минимальной контактной схеме, реализующей f. Пусть B — произвольный базис, состоящий из двухместных функций и содержащий дизъюнкцию и конъюнкцию. Сложностью $L_\phi(f)$ функции f называется число вхождений переменных в минимальную формулу в базисе B, реализующую эту функцию. Пусть $D' \subseteq D \subseteq \{0,1\}^n$. Сужением функции $h : D \to \{0,1\}$ на область D' называется функция $g : D' \to \{0,1\}$ такая, что при всех $x \in D'$ справедливо равенство $g(x) = h(x)$. Сужение функции f на область D будем обозначать через f_D.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-01068).

В настоящей работе рассматриваются две задачи. Первая заключается в следующем: для конкретной управляющей системы (схемы из функциональных элементов, контактной схемы, формулы), произвольной булевой функции f и множества M, состоящего из всех областей из $\{0,1\}^n$ фиксированной мощности d, требуется установить нижнюю оценку для сложности самого сложного сужения f на области из M. Вторая задача является в некотором смысле предельным случаем первой и для схем из функциональных элементов формулируется следующим образом: для произвольной булевой функции f требуется установить нижнюю оценку для сложности самого сложного сужения f_D, удовлетворяющего с точностью до постоянного множителя равенству $L(f_D)\log L(f_D) = |D|$. (Всюду в этой статье log обозначает логарифм по основанию 2.) Сложность сужения в первом случае оценивается через сложность рассматриваемой функции и мощность области сужения, во втором случае — через сложность функции и число ее аргументов. Эти задачи, а также некоторые другие, подобные им, рассматривались в [5, 6].

Кратко перечислим основные результаты, полученные в настоящей работе, и укажем их возможные применения. Результаты, относящиеся к решению первой задачи, содержатся в теоремах 4, 7 и 9. Нижние оценки для сложности сужений в случае реализации булевых функций схемами из функциональных элементов представлены в теореме 4. Из этой теоремы следует, что у любой функции f от n переменных, сложность которой $L(f)$ по крайней мере квадратична, существует область полиномиальной относительно $L(f)$ мощности, сложность сужения на которую функции f по порядку не более чем в $n/\log n$ раз отличается от $L(f)$.

Установленные в теореме 6 верхние оценки для сложности сужений функций полиномиального веса показывают, что нижняя оценка из теоремы 4 оптимальна по порядку, т. е. существуют функции, для которых сложность любого сужения на область фиксированной мощности по порядку не превосходит нижней оценки из этой теоремы.

Чуть менее точные результаты получены в теореме 7 при реализации функций контактными схемами и в теореме 9 для формул.

Решение второй задачи содержится в теоремах 5, 8 и 10. Наибольший интерес представляет теорема 5. Согласно этой теореме для любой булевой функции от n переменных, сложность реализации которой схемами из функциональных элементов превышает величину $n^{2+\epsilon}$, ϵ — сколь угодно малая положительная константа, можно найти такую область D, что сужение функции на D имеет нелинейную сложность, которая лишь в фиксированное число раз отличается от сложности

самой сложной определенной на D функции. Теорема 5 позволяет перенести на произвольные булевы функции ряд «плохих» свойств, которыми обладают функции, имеющие максимальную по порядку сложность (результаты будут опубликованы позднее). Среди этих «плохих» свойств наибольший интерес представляют два.

Первое свойство заключается в том, что при вычислении любой максимально сложной по порядку функции использование датчиков случайных чисел позволяет не более чем в фиксированное число раз уменьшить время вычисления (утверждение верно и в том случае, когда правильное значение функции вычисляется с вероятностью, отличной от единицы). Это свойство легко установить, используя результат О. Б. Лупанова [3] о сложности реализаций булевых функций малого веса. Второе свойство состоит в том, что среднее время вычисления любой максимально сложной по порядку функции не более чем в постоянное число раз отличается от ее обычной схемной сложности. Это свойство легко извлекается из упомянутого результата О. Б. Лупанова и из доказательства теоремы 1 из [7]. Доказательства всех упомянутых теорем основаны на важном результате, приведенном в теореме 1. Неформально этот результат может быть сформулирован в виде следующего предложения.

Каждая булева функция f от n переменных может быть представлена в виде пороговой суммы своих сужений f_{D_i} на некоторые области D_i, т. е. $f = M(f_{D_1}, \ldots, f_{D_s})$, где M — функция голосования, причем мощности этих областей не более чем в n^3 раз превышают сложность функции, а число областей не превосходит n. Используя теорему 1, можно получить аналоги теорем 4 и 5 как для других управляющих систем (плоские схемы, схемы ограниченной глубины и т. д.), так и для мер сложности, отличных от рассматриваемых в настоящей работе (например, для глубины схем). Теорема 1 имеет интересное следствие: для любой булевой функции от n переменных можно указать не более n областей таких, что их мощности не более чем в n^3 раз превышают сложность функции f, а функция f однозначно определяется по своим значениям в этих областях, т. е. вся информация о функции содержится в этих областях.

Далее, как правило, без специального упоминания будем полагать, что n — число переменных всех рассматриваемых ниже функций не меньше некоторого n_0. Через c_i, $i = 0, 1, \ldots$, обозначаются подходящие константы.

1. Сужения булевых функций

Во введении сужение булевой функции было определено как частичная функция. В настоящем пункте это определение уточняется.

Пусть $D_1 \subseteq D_2 \subseteq \{0,1\}^n$, P_2^n — множество всех полностью определенных булевых функций от n переменных, $P_2^n(D_1)$ — множество всех частичных булевых функций от n переменных, определенных в области D_1; $F : P_2^n(D_1) \to P_2^n$ такая функция, что для любой $f \in P_2^n(D_1)$ справедливо равенство $(F(f))_{D_1} = f$. Функцию $F(f)$ назовем *продолжением* функции f на область D_2 относительно функции F. Введенное понятие позволяет для каждой $f \in P_2^n(D_1)$ и $x \in D_2$ однозначно определить значение $f(x)$. Поэтому рассматривая далее сужение произвольной функции f на некоторую область D, будем считать это сужение полностью определенной функцией, т. е. значения $f_D(x)$ определены не только для $x \in D$, но и для $x \notin D$.

Рассмотрим важный частный случай, указав конкретную функцию F. Пусть $\mu : g \to R^+$ — произвольная вычислимая положительная функция, определенная на множестве всех полностью определенных булевых функций. Распространим μ на частичные булевы функции. Пусть $D \subseteq \{0,1\}^n$ и $f : D \to \{0,1\}$. Значение μ на f определим следующим образом:

$$\mu(f) = \min_{h:h_D=f} \mu(h).$$

Линейно упорядочим все полностью определенные булевы функции от n переменных. Сделать это можно разными способами, например сравнивая векторы значений функций как целые числа, записанные в двоичной системе счисления. Пусть $D_1 \subseteq D_2 \subseteq \{0,1\}^n$. Каждой частичной булевой функции $f : D_1 \to \{0,1\}$ поставим в соответствие полностью определенную булеву функцию h', являющуюся минимальной (относительно указанного выше линейного порядка) среди таких функций h, что $f = h_{D_1}$ и $\mu(f) = \mu(h)$. Положим $F(f) = h'$. Построенное продолжение (функцию $F(f)$) будем называть *минимальным продолжением* функции f относительно функции μ на область D_2.

Продолжения функций будем обозначать далее так же, как и сами продолжаемые функции, т. е. $F(f)$ будем обозначать символом f.

2. Пороговые суммы

Будем говорить, что функция f *представима* в виде пороговой суммы функций $h_1, \ldots, h_s$, если имеет место равенство $f = M(h_1, \ldots, h_s)$, где M — функция голосования.

Пусть, как и ранее, $\mu : g \to R^+$ — произвольная вычислимая положительная функция, определенная на множестве всех полностью определенных булевых функций. Обозначим через $N_\mu(L, n)$ число полностью определенных булевых функций от n переменных, на которых значение μ не превосходит L. Справедлива следующая

Теорема 1. *Пусть L, d — положительные, $p \geqslant 2$ — натуральное*[*], $D \subset \{0,1\}^n$, $|D| \geqslant n$, $|D| \geqslant d$, $|D| \geqslant 2d\log(4|D|/d)$, $d \geqslant 16p\ln(N_\mu(L,n)|D|)$ и $f : D \to \{0,1\}$. Далее, пусть для любой области D' такой, что $D' \subset D$ и $|D'| \leqslant pd(\log(4|D|/d))^2$, справедливо неравенство $\mu(f_{D'}) \leqslant L$. Тогда среди областей D' имеются области $D_1, \ldots, D_s$ такие, что*

$$\sum_{j=1}^{s}(f(x) \oplus f_{D_j}(x)) < l, \quad f = M(f_{D_1}, \ldots, f_{D_s}),$$

где

$$l = \left\lceil \frac{\log(|D|/(d\log(|D|/d)))}{\log(d/3p\ln(N_\mu(L,n)|D|))} \right\rceil + 1, \quad s = pl - 1.$$

В основе доказательства теоремы лежит следующая конструкция. В области D, в которой определена исследуемая функция f, рассматриваются выбранные по определенному правилу A области D' и продолжения сужений функции f на эти области. Параметры теоремы подобраны так, что число областей значительно превосходит число продолжений, которое оценивается через значение μ. Поэтому на очень большой доле областей сужения продолжаются одной и той же функцией. Отношение этих двух чисел — числа областей и числа продолжений — так велико, что объединение областей D', на которых продолжения совпадают, покрывает почти всю область D. Следовательно, существует некоторая функция g, являющаяся продолжением функции $f_{D'}$ на D и совпадающая с f на почти всех наборах из D. Повторив подобные рассуждения s раз, каждый раз используя новое правило выбора областей, можно показать, что существует s таких функций. Правила выбора областей таковы, что на каждом наборе из D значения лишь ограниченного числа функций g отличаются от соответствующего значения f.

Прежде чем доказывать теорему, убедимся в справедливости нескольких вспомогательных утверждений (леммы 1–4).

Рассмотрим произвольное положительное число b и последовательности $d^0, d^1, \ldots, d^s$, где $d^k = \{d_0^k, d_1^k, \ldots, d_k^k\}$, d_i^j — натуральные. Если при каждом $k \in \{1, 2, \ldots, s-1\}$ справедливы неравенства

$$d_0^{k+1} \leqslant d_0^k, \quad d_i^{k+1} \leqslant d_i^k + d_{i-1}^k b^{-1}, \tag{1}$$

то последовательность d^k назовем k-м *потомком* последовательности d^0 и числа b.

[*] Для доказательства всех приводимых ниже утверждений, являющихся следствием теоремы 1, достаточно положить $p = 2$. Бóльшие значения этого параметра необходимы для доказательства результатов, не вошедших в настоящую работу.

Лемма 1. *Пусть последовательность* $d^k = \{d_0^k, d_1^k, \ldots, d_k^k\}$ *является* k*-м потомком последовательности* $d^0 = \{d_0^0\}$ *и числа* b. *Тогда*

$$d_i^k \leqslant \binom{k}{i} b^{-i} d_0^0.$$

Доказательство. Воспользуемся индукцией по k. При $k = 1$ утверждение леммы следует из (1). Предположим, что утверждение верно при $k = n - 1$. Тогда имеем

$$d_i^n \leqslant d_i^{n-1} + d_{i-1}^{n-1} b^{-1} \leqslant \binom{n-1}{i} b^{-i} d_0^0 + \binom{n-1}{i-1} b^{-(i-1)} d_0^0 b^{-1}$$
$$= b^{-1} d_0^0 \left(\binom{n-1}{i-1} + \binom{n-1}{i} \right) = b^{-i} d_0^0 \binom{n}{i}.$$

Лемма 1 доказана.

Лемма 2. *Пусть* a, b *и* d *— натуральные числа такие, что* $a \geqslant b \geqslant d$, *а* $c = \binom{a}{d} / \binom{b}{d}$. *Тогда справедливо неравенство*

$$b \geqslant a - ad^{-1} \ln c.$$

Доказательство. Так как $a \geqslant b \geqslant d \geqslant 0$, то из определения величины c непосредственно следует, что

$$\ln c = \ln \frac{a(a-1)\ldots(a-d+1)}{b(b-1)\ldots(b-d+1)} \geqslant d \ln \frac{a}{b}.$$

В силу неравенства $\ln t \geqslant 1 - 1/t$, справедливого при любом $t \geqslant 1$, имеем

$$\ln(a/b) \geqslant 1 - b/a.$$

Следовательно,

$$\ln c \geqslant d(1 - b/a),$$

т. е.

$$b \geqslant a - ad^{-1} \ln c.$$

Лемма 2 доказана.

Последовательность натуральных чисел $k_0, \ldots, k_{s-1}$ назовем *согласованной* относительно последовательности натуральных чисел $l_0, \ldots, l_{s-1}$, если при каждом i, $0 \leqslant i \leqslant s-1$, справедливы неравенства

$$k_i \leqslant l_i/2, \quad \binom{l_i}{k_i} \geqslant \binom{l_j}{k_j},$$

где $l_j = \max\limits_{0 \leqslant i \leqslant s-1} l_i$. Отметим, что при любой фиксированной последовательности $l_0, \ldots, l_{s-1}$ и любом фиксированном числе k_j последовательность $k_0, \ldots, k_{s-1}$ определяется однозначно.

Пусть $D = \{D_0, \ldots, D_{k-1}\}$ — система непересекающихся множеств, j — минимальный индекс такой, что $|D_j| = \max\limits_{0 \leqslant i \leqslant k-1} |D_i|$. Систему множеств $D' = \{D'_0, \ldots, D'_{k-1}\}$ назовем (d,k)-*подсистемой* системы D, если $D'_i \subset D_i$ при $0 \leqslant i \leqslant k-1$, последовательность $|D'_0|, \ldots, |D'_{k-1}|$ согласована относительно последовательности $|D_0|, \ldots, |D_{k-1}|$ и $|D'_j| = d$.

Заметим, что при конкретных d и k не всякая система множеств $\{D_0, \ldots, D_{k-1}\}$ имеет (d,k)-подсистему. В следующей лемме устанавливается достаточное условие существования такой подсистемы и доказывается верхняя оценка для ее мощности.

Лемма 3. *Пусть* $D \subset \{0,1\}^n$, $|D| \geqslant n$, $\{D_0, \ldots, D_{k-1}\}$ — *разбиение области* D, $n \geqslant \log|D|$ — *натуральное и* $\min\limits_{0 \leqslant i \leqslant k-1} |D_i| \geqslant d\log(4|D|/d)$. *Тогда в* $\{D_0, \ldots, D_{k-1}\}$ *имеются* (d,k)-*подсистемы и для любой такой подсистемы* $\{D'_0, \ldots, D'_{k-1}\}$ *справедливы соотношения*:

(a) $|D'_i| \geqslant d$,

(b) $\sum\limits_{i=0}^{k-1} |D'_i| \leqslant \frac{1}{2} dk \log(4|D|/d)$.

Доказательство. Без ограничения общности будем считать, что $|D_0| = \max\limits_i |D_i|$, $|D_{k-1}| = \min\limits_i |D_i|$. Сначала убедимся в том, что система множеств $\{D_0, \ldots, D_{k-1}\}$ содержит хотя бы одну (d,k)-подсистему $\{D'_0, \ldots, D'_{k-1}\}$, далее докажем неравенство (b), а затем оценим мощность множества $|D'_i|$. Положим $|D'_i| = d_i$ и $d_0 = d$. Легко видеть, что для существования (d,k)-подсистемы достаточно, чтобы при некотором p, $p \leqslant |D_{k-1}|/2$, было справедливо неравенство $\binom{|D_{k-1}|}{p} \geqslant \binom{|D_0|}{d}$. Действительно, так как $\binom{m}{n}$ возрастает по m, то $\binom{|D_i|}{p} \geqslant \binom{|D_{k-1}|}{p} \geqslant \binom{|D_0|}{d}$, а уменьшая p можно найти такое d_i, что $\binom{|D_i|}{d_i} \geqslant \binom{|D_0|}{d}$ и $\binom{|D_i|}{d_i - 1} < \binom{|D_0|}{d}$. Покажем, что если $|D_{k-1}| \geqslant d\log(4|D|/d)$, то при $|D|$, большем некоторой константы, такое p найдется. Положим $p = \lfloor (d\log(4|D|/d))/2 \rfloor$. Так как при любом $n \geqslant 10$ справедливы неравенства $(n/3)^n < n! < (n/2)^n$ и $\binom{2n}{n} \geqslant 2^{2n+2}/2n$, то в силу условий леммы имеем

$$\binom{|D_{k-1}|}{p} \geqslant \binom{2p}{p} \geqslant \frac{2^{2p+2}}{2p} \geqslant 2^{d\log(4|D|/d) - \log(d\log(4|D|/d))}$$

$$= \left(\frac{4|D|}{d}\right)^d \Big/ \left(d\log\left(\frac{4|D|}{d}\right)\right) \geqslant \frac{|D|^d}{d!} \geqslant \binom{|D|}{d} \geqslant \binom{|D_0|}{d}.$$

Следовательно, в разбиении $\{D_0, \ldots, D_{k-1}\}$ обязательно существуют (d,k)-подсистемы и $d_i \leqslant \lfloor (d\log(4|D|/d))/2 \rfloor$. Поэтому

$$\sum_{i=0}^{k-1} d_i \leqslant \frac{1}{2} dk \log(4|D|/d).$$

Утверждение (b) леммы доказано. Предположим, что при некотором i справедливо неравенство $d_i < d_0$. Тогда имеем

$$\binom{|D_i|}{d_i} \leqslant \binom{|D_0|}{d_i} < \binom{|D_0|}{d_0}.$$

Однако по определению (d,k)-подсистемы неравенство $\binom{|D_i|}{d_i} \geqslant \binom{|D_0|}{d_0}$ справедливо при всех i. Таким образом, справедливо утверждение (a) леммы. Лемма 3 доказана.

Пусть D — произвольное n-элементное множество. При любом $m \in \{1,\dots,n\}$ перенумеруем все m-элементные подмножества множества D, присвоив каждому подмножеству D' его номер $N_D(D')$ такой, что $1 \leqslant N_D(D') \leqslant \binom{n}{m}$ и $N_D(D') \neq N_D(D'')$, если $D' \neq D''$.

Пусть $D = \{D_0,\dots,D_{k-1}\}$ — система непересекающихся множеств, $D' = \{D'_0,\dots,D'_{k-1}\}$ есть (d,k)-подсистема системы D, $|D_j| = \max\limits_{0\leqslant i\leqslant k-1} |D_i|$. Систему множеств D' назовем *регулярной* (d,k)-подсистемой системы D, если $N_{D_i}(D'_i) = N_{D_j}(D'_j)$. Легко видеть, что если у системы $\{D_0,\dots,D_{k-1}\}$ существует (d,k)-подсистема, то у нее также существует и регулярная (d,k)-подсистема. Отметим одно простое, но важное свойство регулярных подсистем, лежащее в основе доказательства приводимой ниже леммы 4. Если $D' = \{D'_0,\dots,D'_{k-1}\}$ и $D'' = \{D''_0,\dots,D''_{k-1}\}$ две регулярные (d,k)-подсистемы системы D и при некотором i множества D'_i и D''_i различны, то при любом s, $0 \leqslant s \leqslant k-1$, различны множества D'_s и D''_s. Для регулярной подсистемы $D' = \{D'_0,\dots,D'_{k-1}\}$ через $\widetilde{D}'$ обозначим множество, являющееся объединением всех множеств D'_i из D', т. е. $\widetilde{D}' = \bigcup\limits_{i=0}^{k-1} D'_i$.

Пусть $f : D \to \{0,1\}$. Величина $w(f) = \sum_{x\in D} f(x)$ называется *весом* частичной булевой функции f. Справедлива следующая

Лемма 4. *Пусть L — положительное, $D \subset \{0,1\}^n$, $|D| \geqslant n$, $d \geqslant \log|D|$ — натуральное, $f : D \to \{0,1\}$ и $\{C, D_0,\dots,D_{k-1}\}$ — такое разбиение области D, что $\min\limits_{0\leqslant i\leqslant k-1} |D_i| \geqslant d\log(4|D|/d)$. Далее, пусть для любой области D' такой, что*

$$C \subset D' \subset D, \quad |D'| \leqslant |C| + \frac{1}{2}dk\log(4|D|/d),$$

справедливо неравенство $\mu(f_{D'}) \leqslant L$. Тогда среди областей D' имеются область D'' и функция $g : D'' \to \{0,1\}$, продолжение которой на D обладает следующими свойствами:

(a) $\mu(g) \leqslant L$;

(b) $w(f_{D_i} \oplus g_{D_i}) \leqslant |D_i|\ln(N_\mu(L,n)|D_i|)d^{-1}$ *при* $0 \leqslant i \leqslant k-1$,

(c) $f_C = g_C$.

Доказательство. Кратко поясним основную идею доказательства леммы. Она заключается в следующем. В области D рассматриваются различные подмножества, являющиеся объединением области C и множества некоторой регулярной (d,k)-подсистемы разбиения $\{D_0,\dots,D_{k-1}\}$ области $D\setminus C$. По условию леммы для каждого такого подмножества D' справедливо неравенство $\mu(f_{D'})\leqslant L$, т. е. существует некоторая полностью определенная функция h такая, что $\mu(h)\leqslant L$ и h на D' совпадает с f. Другими словами, каждой частичной функции $f_{D'}$ соответствует ее продолжение h и $\mu(h)\leqslant L$. Если число регулярных подсистем, а следовательно, и число рассматриваемых подмножеств существенно больше числа различных функций, на которых μ не превосходит L, то на значительной доле этих подмножеств функции f соответствует одно и то же продолжение h. Значит, f совпадает с h на объединении этих подмножеств. Поэтому для доказательства леммы достаточно найти такие множества $W_0,\dots,W_{k-1}$, где $W_i\subseteq D_i$, минимально возможной мощности, которые будут гарантировать существование в разбиении $\{W_0,\dots,W_{k-1}\}$ необходимого числа регулярных (d,k)-подсистем, равного отношению числа всех регулярных (d,k)-подсистем разбиения $\{D_0,\dots,D_{k-1}\}$ к числу различных функций, на которых μ не превосходит L.

Как и при доказательстве предыдущей леммы, без ограничения общности будем считать, что $|D_0|=\max\limits_i|D_i|$ и $|D_{k-1}|=\min\limits_i|D_i|$. Пусть R — произвольная регулярная (d,k)-подсистема разбиения $\{D_0,\dots,D_{k-1}\}$. Существование такой подсистемы следует из леммы 3. Через $\widetilde{R}$ обозначим множество этой подсистемы. Положив $d_i=|\widetilde{R}\cap D_i|$, имеем $d_0=d$.

Рассмотрим множество $M=\{M_i=C\cup\widetilde{R}_i\}$, состоящее из множеств всех регулярных (d,k)-подсистем R_i разбиения $\{D_0,\dots,D_{k-1}\}$ области $D\setminus C$, объединенных с C, и частичные функции $f_i:M_i\to\{0,1\}$ такие, что $f_i(x)=f(x)$ при $x\in M_i$. В силу леммы 3 при каждом i имеем $|M_i|\leqslant|C|+\frac{1}{2}dk\log(4|D|/d)$. Поэтому из условий леммы следует, что при любом i справедливо неравенство

$$\mu(f_i)\leqslant L.$$

Так как число различных регулярных (d,k)-подсистем R_i равно $\binom{|D_0|}{d}$, то число различных множеств M_i также равно $\binom{|D_0|}{d}$. Поэтому в силу последнего неравенства среди этих множеств найдется не менее $\binom{|D_0|}{d}N_\mu(L,n)^{-1}$ таких, на которых сужения функции f имеют одно и то же продолжение g. Пусть $\widetilde{W}$ — объединение всех этих множеств, $W=D\setminus\widetilde{W}$, $\widetilde{W}_i=\widetilde{W}\cap D_i$ и $W_i=W\cap D_i$. Очевидно, что $\mu(g)\leqslant L$, $f_C=g_C$ и значения функций g и f совпадают в области $\widetilde{W}$ и, возможно, различны в W.

Поэтому $w(f_{D_i} \oplus g_{D_i}) = |W_i|$ и для доказательства леммы достаточно установить справедливость неравенства $|W_i| \leqslant |D_i| \ln(N_\mu(L,n)|D_i|)d^{-1}$. Оценим сверху мощность области W_i. Сначала отметим, что область $\widetilde{W}_i$ должна быть достаточно велика для того, чтобы в ней нашлось не менее $\binom{|D_0|}{d} N_\mu(L,n)^{-1}$ областей мощности d_i. Поэтому должно быть справедливым следующее неравенство:

$$\binom{|D_0|}{d} N_\mu(L,n)^{-1} \leqslant \binom{|\widetilde{W}_i|}{d_i}.$$

Так как

$$\binom{|D_i|}{d_i} = \binom{|D_i|}{d_i - 1} \frac{|D_i| - d_i + 1}{d_i}, \quad \binom{|D_i|}{d_i - 1} < \binom{D_0|}{d},$$

то

$$\begin{aligned}\binom{|D_i|}{d_i} &< \binom{|D_0|}{d} \frac{|D_i| - d_i + 1}{d_i} \\ &\leqslant \binom{|\widetilde{W}_i|}{d_i} \frac{|D_i| - d_i + 1}{d_i} N_\mu(L,n) \leqslant \binom{|\widetilde{W}_i|}{d_i} N_\mu(L,n)|D|.\end{aligned}$$

Следовательно,

$$\binom{|D_i|}{d_i} \Big/ \binom{|\widetilde{W}_i|}{d_i} \leqslant N_\mu(L,n)|D_i|.$$

Далее в силу леммы 2 имеем

$$|\widetilde{W}_i| \geqslant |D_i| - |D_i| \ln(N_\mu(L,n)|D_i|)d_i^{-1}.$$

Так как $D_i = W_i \cup \widetilde{W}_i$, то, используя утверждение (а) леммы 3, из последнего неравенства получаем

$$|W_i| < |D_i| \ln(N_\mu(L,n)|D_i|)d_i^{-1} \leqslant |D_i| \ln(N_\mu(L,n)|D_i|)d^{-1}.$$

Лемма 4 доказана.

Доказательство теоремы 1 разобьем на пять этапов. На первом этапе построим относительно небольшие области $D_1, \ldots, D_s$ и определим в этих областях такие функции $g^1, \ldots, g^s$, что $g^i = f_{D_i}$, $\mu(g^i) \leqslant L$ и каждая g^i на значительной доле наборов из D совпадает с f. Требуемые области и функции будем определять последовательно. На каждом шаге будем использовать лемму 4, применяя ее к функции f и к некоторому разбиению $\{C^i, D_0^i, \ldots, D_i^i\}$ области D, полученному на предыдущем шаге. (Здесь верхний индекс указывает на то, что множества построены на i-м шаге.) В доказательстве будут использованы вспомогательные множества W_j^i и B_j^i, причем при каждом $i \geqslant 1$ множества $D_j^i \cup B_j^i$,

$j \in \{0, \ldots, i\}$, образуют разбиение области D, т. е. $D = \bigcup_{j=0}^{i} (D_j^i \cup B_j^i)$. Так как в условиях леммы 4 параметр d натуральный, то использовать эту лемму будем с новым параметром $d' = \lfloor d \rfloor$. На втором этапе установим важное свойство, которое для каждого $x \in D$ позволяет определить функции g^i такие, что $g^i(x) \neq f(x)$. Будет показано, что если $x \in D_j^k \cup B_j^k$, то число таких функций равно j. На третьем этапе доказательства оценим мощности множеств, построенных на первом этапе, в том числе и множеств $D_j^i \cup B_j^i$. Покажем, что, начиная с некоторых i и j, все множества $D_j^i \cup B_j^i$ будут пустыми. На четвертом этапе определим условия, при которых на первом этапе возможно применение леммы 4. Наконец, на пятом этапе установим, что области и функции, построенные на первом этапе, удовлетворяют условию теоремы.

1. Определим области $D_1, \ldots, D_s$ и функции $g^1, \ldots, g^s$. Сделаем это индуктивно. Базой индукции являются область D_1 и функция g^1. Сначала опишем два первых шага, т. е. определим области D_1, D_2, разбиения $\{C^0, D_0^0\}$, $\{C^1, D_0^1, D_1^1\}$ и функции g^1, g^2. Положим $D_0^0 = D$, $C^0 = \varnothing$. К функции f и областям $\{C^0, D_0^0\}$ применим лемму 4. Легко видеть, что сделать это можно: справедливость условий леммы 4 следует из справедливости условий теоремы 1. В силу леммы 4 найдется область $D_1 \subseteq D$, $|D_1| \leqslant \frac{1}{2} d' \log(4|D|/d')$, и функция $g^1 : D_1 \to \{0, 1\}$, продолжение которой на D обладает следующими свойствами:

(a) $\mu(g^1) \leqslant L$,

(b) $w(f \oplus g^1) \leqslant |D_0^0| \ln(N_\mu(L, n)|D_0^0|)/d'$.

Положим

$$W_1^1 = \{x | x \in D,\ f(x) \neq g^1(x)\}.$$

Очевидно, что

$$|W_1^1| \leqslant |D_0^0| \ln(N_\mu(L, n)|D_0^0|)/d'.$$

Теперь определим множества D_0^1, D_1^1, B_0^1, B_1^1, C^1. Положим

$$D_0^1 = D_0^0 \setminus W_1^1, \quad B_0^1 = \varnothing.$$

Так как по условию теоремы $d \geqslant 16p \ln(N_\mu(L, n)|D|)$, $N_\mu(L, n) \geqslant 1$ и $|D| \geqslant 2d \log(4|D|/d)$, то из полученной выше оценки для $|W_1^1|$ следует, что $|W_1^1| \leqslant \frac{1}{30}|D|$. Поэтому

$$|D_0^1| = |D| - |W_1^1| \geqslant \frac{29}{30}|D| \geqslant \frac{29}{30} d' \log(4|D|/d') > d' \log(4|D|/d').$$

Далее, положим

$$D_1^1 = W_1^1, \quad B_1^1 = \varnothing,$$

если $|W_1^1| \geqslant d' \log(4|D|/d')$;

$$D_1^1 = \varnothing, \quad B_1^1 = W_1^1,$$

если $|W_1^1| < d' \log(4|D|/d')$, и, наконец,

$$C^1 = B_0^1 \cup B_1^1.$$

Очевидно, что $D = (D_0^1 \cup B_0^1) \cup (D_1^1 \cup B_1^1)$. Поэтому $C^1 = D \setminus (D_0^1 \cup D_1^1)$ и $\{C^1, D_0^1, D_1^1\}$ является разбиением области D. Легко видеть, что справедливы неравенства

$$|D_0^1| \leqslant |D_0^0|, \quad |D_1^1| \leqslant |W_1^1| \leqslant |D_0^0| \ln(N_\mu(L,n)|D_0^0|)/d'.$$

Область D_1, функция g^1, множества W_1^1, B_0^1, B_1^1 и разбиение $\{C^1, D_0^1, D_1^1\}$ области D определены. Очевидно, что

$$\begin{aligned} &\text{если} \quad x \in D_0^1 \cup B_0^1, \quad \text{то} \quad f(x) = g^1(x), \\ &\text{если} \quad x \in D_1^1 \cup B_1^1, \quad \text{то} \quad f(x) \neq g^1(x). \end{aligned} \tag{2}$$

Перейдем к определению области D_2, функции g^2 и нового разбиения области D. Заметим, что если D_1^1 непусто, то по построению $|D_1^1| \geqslant d' \log(4|D|/d')$. Поэтому снова можно воспользоваться леммой 4. Применим ее к функции f и либо к разбиению $\{C^1, D_0^1, D_1^1\}$, если D_1^1 непусто, либо к разбиению $\{C^1, D_0^1\}$, если D_1^1 пусто. В результате получим новую область $D_2 \subseteq D$, $|D_2| \leqslant |C^1| + d' \log(4|D|/d')$, и функцию $g^2 : D_2 \to \{0,1\}$, продолжение которой на D обладает следующими свойствами:

$$\begin{gathered} \mu(g^2) \leqslant L, \\ w(f_{D_i^1} \oplus g^2_{D_i^1}) \leqslant |D_i^1| \ln(N_\mu(L,n)|D_i^1|)/d', \quad i \in \{0,1\} \\ f_{C^1} = g^2_{C^1}. \end{gathered} \tag{3}$$

Положим*)

$$W_1^2 = \{x | x \in D_0^1, f(x) \neq g^2(x)\}, \quad W_2^2 = \{x | x \in D_1^1, f(x) \neq g^2(x)\};$$

$$D_0^2 = B_0^1 \cup D_0^1 \setminus W_1^2 \text{ и } B_0^2 = \varnothing,$$

если $|B_0^1 \cup D_0^1 \setminus W_1^2| \geqslant d' \log(4|D|/d')$;

$$D_0^2 = \varnothing \text{ и } B_0^2 = B_0^1 \cup D_0^1 \setminus W_1^2,$$

если $|B_0^1 \cup D_0^1 \setminus W_1^2| < d' \log(4|D|/d')$;

$$D_1^2 = B_1^1 \cup W_1^2 \cup D_1^1 \setminus W_2^2 \text{ и } B_1^2 = \varnothing,$$

если $|B_1^1 \cup W_1^2 \cup D_1^1 \setminus W_2^2| \geqslant d' \log(4|D|/d')$;

$$D_1^2 = \varnothing \text{ и } B_1^2 = B_1^1 \cup W_1^2 \cup D_1^1 \setminus W_2^2,$$

*) Далее полагаем, что операция взятия разности двух множеств выполняется раньше других теоретико-множественных операций.

если $|B_1^1 \cup W_1^2 \cup D_1^1 \setminus W_2^2| < d' \log(4|D|/d')$;

$$D_2^2 = W_2^2 \text{ и } B_2^2 = \varnothing,$$

если $|W_2^2| \geqslant d' \log(4|D|/d')$;

$$D_2^2 = \varnothing \text{ и } B_2^2 = W_2^2,$$

если $|W_2^2| < d' \log(4|D|/d')$, и, наконец,

$$C^2 = B_0^2 \cup B_1^2 \cup B_2^2.$$

Легко видеть, что $D = (D_0^2 \cup B_0^2) \cup (D_1^2 \cup B_1^2) \cup (D_2^2 \cup B_2^2)$. Так как все 6 множеств B_i^2, D_i^2 попарно не пересекаются, то $C^2 = D \setminus (D_0^2 \cup D_1^2 \cup D_2^2)$. Поэтому $\{C^2, D_0^2, D_1^2, D_2^2\}$ является разбиением области D. Оценим сверху мощности перечисленных областей. В силу (3) имеем

$$|W_1^2| \leqslant |D_0^1| \ln(N_\mu(L,n)|D_0^1|)/d', \quad |W_2^2| \leqslant |D_1^1| \ln(N_\mu(L,n)|D_1^1|)/d'.$$

Очевидно также, что

$$|D_0^2| \leqslant |D_0^1|,$$
$$|D_1^2| + |B_1^2| \leqslant |D_1^1| + |B_1^1| + |D_0^1| \ln(N_\mu(L,n)|D_0^1|)/d',$$
$$|D_2^2| \leqslant |D_1^1| \ln(N_\mu(L,n)|D_1^1|)/d'.$$

Область D_2, функция g^2 и новое разбиение $\{C^2, D_0^2, D_1^2, D_2^2\}$ области D определены. Определены также множества W_1^2, W_2^2, B_0^2, B_1^2, B_2^2. Отметим одно важное свойство множеств $B_i^2 \cup D_i^2$, $i \in \{0,1,2\}$, являющееся аналогом свойства (2). Если $x \in B_0^2 \cup D_0^2$, то $g^1(x) = g^2(x) = f(x)$. Если $x \in B_1^2 \cup D_1^2$, то $g^1(x) \neq g^2(x)$, т. е. значение только одной из построенных функций на наборе x совпадает со значением $f(x)$. Если $x \in B_2^2 \cup D_2^2$, то $g^1(x) = g^2(x) \neq f(x)$.

Предположим, что уже найдены область D_{m-1}, функция g^{m-1}, разбиение $\{C^{m-1}, D_0^{m-1}, \ldots, D_{m-1}^{m-1}\}$ и такие множества $B_0^{m-1}, \ldots, B_{m-1}^{m-1}$, что $\{B_i^{m-1} \cup D_i^{m-1}\}_{i=0}^{m-1}$ также является разбиением области D. Определим функцию g^m, разбиение $\{C^m, D_0^m, \ldots, D_m^m\}$ и новые множества $B_0^m, \ldots, B_m^m$ такие, что $\{B_i^m \cup D_i^m\}_{i=0}^m$ — разбиение области D. Пусть q_{m-1} — число непустых множеств среди $D_0^{m-1}, \ldots, D_{m-1}^{m-1}$. К функции f и непустым множествам разбиения $\{C^{m-1}, D_0^{m-1}, \ldots, D_{m-1}^{m-1}\}$ применим лемму 4. Для того чтобы это можно было сделать, достаточно выполнения следующих двух условий:

(a) $\min\limits_{\substack{0 \leqslant i \leqslant m-1 \\ |D_i^{m-1}|>0}} |D_i^{m-1}| \geqslant d' \log(4|D|/d)$,

(b) для любой области D' такой, что

$$C^{m-1} \subset D' \subset D, \quad |D'| \leqslant |C^{m-1}| + \frac{1}{2} d' q_{m-1} \log(4|D|/d'),$$

справедливо неравенство

$$\mu(f_{D'}) \leqslant L.$$

Потребуем выполнения этих условий. Их справедливость докажем ниже, в п. 4 доказательства настоящей теоремы. Итак, воспользуемся леммой 4. В результате получим область $D_m \subseteq D$ такую, что

$$|D_m| \leqslant |C^{m-1}| + d' q_{m-1} \log(4|D|/d'), \tag{4}$$

и функцию $g^m : D_m \to \{0,1\}$, продолжение которой на D обладает следующими свойствами:

$$\mu(g^m) \leqslant L, \tag{5}$$

$$w(f_{D_i^{m-1}} \oplus g^m_{D_i^{m-1}}) \leqslant |D_i^{m-1}| \ln(N_\mu(L,n)|D_i^{m-1}|)/d', \tag{6}$$

$$f_{C^{m-1}} = g^m_{C^{m-1}}. \tag{7}$$

Положим

$$W_i^m = \{x | x \in D_{i-1}^{m-1},\ f(x) \neq g^m(x)\}, \quad 1 \leqslant i \leqslant m;$$

$$D_0^m = B_0^{m-1} \cup D_0^{m-1} \setminus W_1^m \text{ и } B_0^m = \varnothing,$$

если $|B_0^{m-1} \cup D_0^{m-1} \setminus W_1^m| \geqslant d' \log(4|D|/d')$;

$$D_0^m = \varnothing, \quad B_0^m = B_0^{m-1} \cup D_0^{m-1} \setminus W_1^m,$$

если $|B_0^{m-1} \cup D_0^{m-1} \setminus W_1^m| < d' \log(4|D|/d')$.

Пусть $1 \leqslant i \leqslant m-1$. Положим

$$D_i^m = B_i^{m-1} \cup W_i^m \cup D_i^{m-1} \setminus W_{i+1}^m \text{ и } B_i^m = \varnothing,$$

если $|B_i^{m-1} \cup D_i^{m-1} \setminus W_{i+1}^m| \geqslant d' \log(4|D|/d')$;

$$D_i^m = \varnothing, \quad B_i^m = B_i^{m-1} \cup W_i^m \cup D_i^{m-1} \setminus W_{i+1}^m,$$

если $|B_i^{m-1} \cup D_i^{m-1} \setminus W_{i+1}^m| < d' \log(4|D|/d')$;

$$D_m^m = W_m^m \text{ и } B_m^m = \varnothing,$$

если $|W_m^m| \geqslant d' \log(4|D|/d')$;

$$D_m^m = \varnothing \text{ и } B_m^m = W_m^m,$$

если $|W_m^m| < d' \log(4|D|/d')$, и, наконец,

$$C^m = \bigcup_{0 \leqslant i \leqslant m} B_i^m.$$

Так как $D_0^m \cup B_0^m = B_0^{m-1} \cup (D_0^{m-1} \setminus W_1^m)$, $D_i^m \cup B_i^m = B_i^{m-1} \cup W_i^m \cup D_i^{m-1} \setminus W_{i+1}^m$, $D_m^m \cup B_m^m = W_m^m$, то

$$\bigcup_{0 \leqslant i \leqslant m} (D_i^m \cup B_i^m) = (B_0^{m-1} \cup D_0^{m-1} \setminus W_1^m)$$

$$\cup \left(\bigcup_{0 \leqslant i \leqslant m-1} (B_i^{m-1} \cup W_i^m \cup (D_i^{m-1} \setminus W_{i+1}^m)) \right) \cup W_m^m$$

$$= \bigcup_{0 \leqslant i \leqslant m-1} (B_i^{m-1} \cup D_i^{m-1}) = D.$$

Поскольку все множества B_i^m и D_i^m попарно не пересекаются, имеем

$$C^m = D \setminus \left(\bigcup_{0 \leqslant i \leqslant m} D_i^m \right)$$

и $\{C^m, D_0^m, \ldots, D_m^m\}$ является разбиением области D. Все необходимые множества построены.

2. Индукцией по верхнему индексу покажем, что если $x \in B_i^m \cup D_i^m$, то

$$\sum_{j=1}^{m} (f(x) \oplus g^j(x)) = i, \tag{8}$$

т. е. среди функций $g^1, \ldots, g^m$ найдется ровно i функций, значения которых отличны от $f(x)$. Случай $m = 1$ был рассмотрен выше. Предположим, что доказываемое свойство справедливо при $m = k$. Допустим, что $x \in B_i^k \cup D_i^k$. Тогда по предположению индукции $\sum_{j=1}^{k} (f(x) \oplus g^j(x)) = i$. Пусть $f(x) = g^{k+1}(x)$. Следовательно, $\sum_{j=1}^{k+1} (f(x) \oplus g^j(x)) = i$ и из определения множеств W_i^j, B_i^j и D_i^j следует, что $x \notin W_{i+1}^{k+1}$. Поэтому $x \in B_i^{k+1} \cup D_i^{k+1}$. Если же $f(x) \neq g^{k+1}(x)$, то $\sum_{j=1}^{k+1} (f(x) \oplus g^j(x)) = i + 1$, $x \in W_{i+1}^{k+1}$, и, следовательно, $x \in B_{i+1}^{k+1} \cup D_{i+1}^{k+1}$. Равенство (8) доказано.

3. Оценим сверху мощности множеств C^m, B_i^m, D_i^m, а также множеств $\widetilde{D}_i^m = B_i^m \cup D_i^m$. Пусть k_m — число непустых множеств B_i^m. Из определения множеств B_i^m следует, что $|B_i^m| < d' \log(4|D|/d')$. Поэтому

$$|C^m| < d' k_m \log(4|D|/d'). \tag{9}$$

Оценим сверху мощности множеств $\widetilde{D}_i^m$ и D_i^m. В силу неравенства (6) и определения множества W_i^m при $1 \leqslant i \leqslant m$ имеем

$$|W_i^m| \leqslant |D_{i-1}^{m-1}| \ln(N_\mu(L, n)|D_{i-1}^{m-1}|)/d'.$$

Так как $D_i^m \cup B_i^m = B_i^{m-1} \cup W_i^m \cup D_i^{m-1} \setminus W_{i+1}^m$ и $D_m^m \cup B_m^m = W_m^m$, то

$$|D_i^m \cup B_i^m| \leqslant |D_i^{m-1} \cup B_i^{m-1}| + |W_i^m| = |B_i^{m-1}| + |D_i^{m-1}| + |W_i^m|,$$
$$|D_m^m \cup B_m^m| = |W_m^m|.$$

Отсюда и из неравенства $|D_i^m| \leqslant |\widetilde{D}_i^m| \leqslant |D|$ следует, что

$$|\widetilde{D}_m^m| \leqslant |\widetilde{D}_{m-1}^{m-1}| \ln(N_\mu(L,n)|D|)/d', \tag{10}$$
$$|\widetilde{D}_i^m| \leqslant |\widetilde{D}_{i-1}^{m-1}| + |\widetilde{D}_{i-1}^{m-1}| \ln(N_\mu(L,n)|D|)/d', \quad 1 \leqslant i \leqslant m-1. \tag{11}$$

Так как из определения множеств D_0^m и B_0^m следует вложение $D_0^m \cup B_0^m \subseteq D_0^{m-1} \cup B_0^{m-1}$, то

$$|\widetilde{D}_0^m| \leqslant |\widetilde{D}_0^{m-1}|.$$

Сравнивая последнее неравенство и неравенства (10), (11) с (1), нетрудно видеть, что последовательность $|\widetilde{D}_0^m|, \ldots, |\widetilde{D}_m^m|$ является m-м потомком последовательности, состоящей из одного элемента, равного $|D|$ (напомним, что $D_0^0 = D$), и числа $R = (\ln(N_\mu(L,n)|D|))^{-1} d'$. Поэтому в силу леммы 1 имеем

$$|D_i^m| \leqslant |\widetilde{D}_i^m| \leqslant \binom{m}{i} R^{-1} |D|.$$

Так как по условию теоремы $d \geqslant 16p \ln(N_\mu(L,n)|D|)$ и $d' = \lfloor d \rfloor$, то

$$R > 12p. \tag{12}$$

Теперь покажем, что $|D_{i+t}^{i+j}| = 0$ при любых i, t, j, удовлетворяющих следующим неравенствам:

$$i \geqslant \log_2(|D|/(d \log(4|D|/d))/\log(R/3p), \quad 0 \leqslant t \leqslant j \leqslant i(p-1). \tag{13}$$

Убедимся в этом методом от противного. Предположим, что $|D_{i+t}^{i+j}| > 0$. Тогда в силу определения множеств D_{i+t}^{i+j} имеем

$$2|D_{i+t}^{i+j}| \geqslant 2d' \log(4|D|/d') > d \log(4|D|/d).$$

Поэтому

$$d \log(4|D|/d) < 2|D_{i+t}^{i+j}| \leqslant 2\binom{i+j}{i+t} R^{-i-t} |D|.$$

Так как для всех n справедливо неравенство $n! \geqslant (n/e)^n$, то в силу (13) имеем

$$2\binom{i+j}{i+t} \leqslant 2\frac{(i+j)^{i+t}}{(i+t)!} \leqslant 2\left(\frac{e(i+j)}{i+t}\right)^{i+t} \leqslant (3p)^{i+t}.$$

Объединяя два последних неравенства, после несложных преобразований получаем

$$|D|/(d\log(4|D|/d)) \geqslant (R/3p)^{i+t}.$$

Логарифмируя это неравенство, имеем

$$i + t < \log(|D|/(d\log(4|D|/d))/\log(R/3p).$$

Противоречие с (13). Следовательно, $|D_{i+t}^{i+j}| = 0$ при всех i, j и t, удовлетворяющих (13). Теперь методом от противного покажем, что $|B_{i+t}^{i+j}| = 0$ при любых i, t, j таких, что

$$i \geqslant 1 + \log(|D|/(d\log(4|D|/d))/\log(R/3p) \text{ и } 0 \leqslant t \leqslant j \leqslant i(p-1). \quad (14)$$

Пусть H_i — множество всех таких пар (j, t), которые вместе с i удовлетворяют неравенствам (14) и для которых справедливо неравенство $|B_{i+t}^{i+j}| > 0$. Введем числа t' и j', зависящие от i. Положим

$$t' = \min_{(t,j)\in H_i} t, \quad j' = \min_{(t',j)\in H_i} j.$$

Очевидно, что $i' > 0$ и $j' > 0$. Из определения множеств B_l^m и W_l^m следует, что $B_{i+t'}^{i+j'} = B_{i+t'}^{i+j'-1} \cup W_{i+t'}^{i+j'} \cup D_{i+t'}^{i+j'-1} \setminus W_{i+t'+1}^{i+j'}$ и $W_{i+t'}^{i+j'} = \{x | x \in D_{i+t'-1}^{i+j'-1},\ f(x) \neq g^{i+j'-1}(x)\}$. Пусть $x \in B_{i+t'}^{i+j'}$. Тогда либо $x \in B_{i+t'}^{i+j'-1}$, либо $x \in W_{i+t'}^{i+j'}$, либо $x \in D_{i+t'}^{i+j'-1}$. Первый случай невозможен в силу выбора j' и t'. Во втором случае $x \in W_{i+t'}^{i+j'} \subseteq D_{i+t'-1}^{i+j'-1}$. Однако в силу (13) и (14) множество $D_{i+t'-1}^{i+j'-1}$ пусто. Следовательно, второй случай также невозможен. Невозможен и третий случай, так как в силу (13) и (14) множество $D_{i+t'}^{i+j'-1}$ пусто. Поэтому сделанное предположение неверно. Таким образом, показано, что если тройка (i, j, t) удовлетворяет (14), то

$$|D_{i+t}^{i+j}| = |B_{i+t}^{i+j}| = 0. \quad (15)$$

4. Найдем достаточные условия существования функции g^m. Для этого определим условия применимости леммы 4. Как было отмечено выше, для этого достаточно установить справедливость следующих условий:

(a) $\min\limits_{\substack{0\leqslant i\leqslant m-1 \\ |D_i^{m-1}|>0}} |D_i^{m-1}| \geqslant d'\log(4|D|/d)$;

(b) если область D' является такой, что

$$C^{m-1} \subset D' \subset D \text{ и } |D'| \leqslant |C^{m-1}| + \frac{1}{2}d'q_{m-1}\log(4|D|/d'),$$

где q_{m-1} — число непустых множеств D_j^{m-1}, то

$$\mu(f_{D'}) \leqslant L.$$

Выполнение условия (a) непосредственно следует из определения множеств D_j^i. Покажем, что справедливость условия (b) следует из неравенства

$$m \leqslant p\left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(R/3p)} \right\rceil + 2p.$$

Так как $d' \leqslant d$ и при $d \leqslant |D|$ функция $d(\log(|D|/d))^2$ возрастает по d, то в силу (9) и неравенства $q_{m-1} + k_{m-1} \leqslant m$ для любого рассматриваемого множества D' имеем

$$|D'| \leqslant (m - q_{m-1})d\log(4|D|/d) + \frac{1}{2}dq_{m-1}\log(4|D|/d) \leqslant d\log(4|D|/d)m.$$

Далее, используя (12) и неравенство $|D| > 2d\log(4|D|/d)$, из условий теоремы получаем

$$\left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(R/3p)} \right\rceil < \log(|D|/(d\log(|D|/d)) \leqslant \log(4|D|/d) - 2.$$

Поэтому при

$$m \leqslant m' = p\left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(R/3p)} \right\rceil + 2p$$

справедливо неравенство $m < \log(4|D|/d)$. Следовательно,

$$|D'| \leqslant |C^{m-1}| + \frac{1}{2}d'q_{m-1}\log(4|D|/d') < pd(\log(4|D|/d'))^2. \qquad (16)$$

Таким образом, при $m \leqslant m'$ из условий теоремы и неравенства (16) следует справедливость условия (b). Следовательно, функция $g^{m'}$ существует.

5. Положим

$$l = 1 + \left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(R/3p)} \right\rceil$$

и $s = pl - 1$. В этом случае

$$s = p\left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(R/3p)} \right\rceil + p - 1.$$

Следовательно, как показано в п. 4, существует функция g^s, а вместе с ней и функции $g^1, \ldots, g^{s-1}$. Так как по построению $g^i = f_{D_i}$, а из (4) и (16) следует неравенство $|D_i| < pd(\log(4|D|/d'))^2$, то согласно (5) при всех i имеем

$$\mu(f_{D_i}) \leqslant L.$$

Покажем, что для любого $x \in D$ среди функций $g^1, \ldots, g^s$ найдется менее l функций, значения которых на наборе x отличаются от $f(x)$.

Действительно, в силу (15) при $i \geqslant l$ справедливы равенства $|D_i^\sigma| = 0$ и $|B_i^\sigma| = 0$. А так как $D = \bigcup\limits_{0 \leqslant i \leqslant s} (B_i^\sigma \cup D_i^\sigma)$, то для любого $x \in D$ имеем $x \in \bigcup\limits_{0 \leqslant i \leqslant l-1} (B_i^\sigma \cup D_i^\sigma)$. Наконец, из (8) следует, что для любого $x \in B_i^\sigma \cup D_i^\sigma$ справедливо равенство $\sum\limits_{j=1}^{s} (f(x) \oplus g^j(x)) = i$. Следовательно, для любого $x \in D$ справедливо неравенство

$$\sum_{j=1}^{s} (f(x) \oplus g^j(x)) < l,$$

поэтому

$$f = M(f_{D_1}, \ldots, f_{D_s}).$$

Теорема 1 доказана.

Доказанная теорема имеет интересное следствие (теорема 2). Прежде чем сформулировать эту теорему, дадим одно определение. Пусть $D \subset \{0,1\}^n$, $f : D \to \{0,1\}$, $D_1, \ldots, D_s \subseteq D$. Будем говорить, что функция f однозначно определяется по значениям в областях $D_1, \ldots, D_s$, если существует алгоритм A, не зависящий ни от f, ни от n, ни от областей $D_1, \ldots, D_s$, который, получая на входе эти области (список наборов с указанием каким областям принадлежит каждый набор) и значения функции f на наборах из этих областей, вычисляет значения f на всех наборах из D.

Теорема 2. *Пусть* $D \subset \{0,1\}^n$, $f : D \to \{0,1\}$, $|D| \geqslant n$, $|D| \geqslant d$, $d \geqslant 32 \ln(N_\mu(\mu(f), n)|D|)$ *и* $|D| \geqslant 2d \log(4|D|/d)$. *Тогда имеются такие области* $D_1, \ldots, D_s$, $D_i \subset D$, $|D_i| \leqslant 2d(\log(4|D|/d))^2$,

$$s = 2\left\lceil \frac{\log(|D|/(d\log(|D|/d))}{\log(d/3p\ln(N_\mu(\mu(f), n)|D|))} \right\rceil - 1,$$

что функция f *однозначно определяется по своим значениям в этих областях.*

Доказательство. Рассматривая сужения булевых функций, будем использовать минимальные продолжения этих сужений относительно μ. Очевидно, что в этом случае для любой области $D' \subseteq D$ справедливо неравенство $\mu(f_{D'}) \leqslant \mu(f)$. Полагая $p = 2$ и $L = \mu(f)$, видим, что все условия теоремы 1 выполнены. Следовательно, существуют такие области $D_1, \ldots, D_s$, что $f = M(f_{D_1}, \ldots, f_{D_s})$, где M — функция голосования. Так как при заданной функции μ частичные функции $f_{D_1}, \ldots, f_{D_s}$ рассматриваются как полностью определенные, то значение f на любом наборе из D однозначно определяется значениями функций f_{D_i}. В свою очередь, каждая функция f_{D_i} однозначно определяется по своим значениям

в области D_i. Требуемый алгоритм устроен следующим образом. Для каждой области D_i рассматриваются всевозможные полностью определенные булевы функции, значения которых в области D_i совпадают с соответствующими значениями функции f. Для каждой из этих функций вычисляется значение μ. Среди функций с минимальным значением μ выбирается минимальная относительно введенного в первом пункте порядка функция. Значение функции f на любом наборе из $\{0,1\}^n$ вычисляется голосованием среди значений s выбранных функций. Теорема 2 доказана.

Без доказательства приведем простое следствие теоремы 2.

Следствие. *Пусть* $f : \{0,1\}^n \to \{0,1\}$. *Тогда существуют такие области* $D_1, \ldots, D_s$, *где* $s < 2\lceil n/\log n\rceil$ *и* $|D_i| \leqslant 40n^3L(f)\ln L(f)$, *что функция* f *однозначно определяется по своим значениям в этих областях.*

Пусть функция μ такова, что

$$\prod_{i=1}^{k} N_\mu(L_i, n) \leqslant N_\mu\left(\sum_{i=1}^{k} L_i, n\right). \tag{17}$$

Из (17) легко следует неравенство

$$N_\mu(L, n) \geqslant 2^{\lfloor L/2\rfloor}. \tag{18}$$

Отметим, что условию (17) удовлетворяют многие естественные меры сложности булевых функций и, в частности, сложности реализации функций различными управляющими системами. Доказываемая ниже теорема показывает, что почти все функции имеют сложные сужения. Для схем из функциональных элементов в теореме 4 аналогичный результат будет доказан для всех функций.

Теорема 3. *Пусть* μ *такова, что выполняется неравенство* (17), *а* $q = \log(2^n/\ln(N_\mu(L,n)2^n))$. *Тогда для почти каждой булевой функции* f *от* n *переменных такой, что* $\mu(f) = L$, *и любого целого*

$$M \geqslant 64(\log(2^{n+2}/\ln(N_\mu(L,n)2^n)))^3\ln(N_\mu(L,n)2^n)$$

среди областей мощности M *имеется область* D' *такая, что*

$$\mu(f_{D'}) \geqslant L\frac{c_0\log(Mq/\ln(N_\mu(L,n)))}{\log(2^n/\ln(N_\mu(L,n)))}.$$

Доказательство. Достаточно убедиться в справедливости теоремы только для минимальных продолжений. Сделаем это методом от противного. Положим $d = M/2q^2$. Предположим, что при некоторой

константе $\delta > 0$ найдется не менее $\delta N_\mu(L,n)$ таких функций f, что для любой области D мощности M справедливо неравенство

$$\mu(f_D) < \frac{L\log(d/\ln(N_\mu(L,n)2^n))}{9\log(2^n/6\ln(N_\mu(L,n)2^n))}.$$

Множество таких функций обозначим через $F(L,n)$. Оценим мощность множества $F(L,n)$. Все булевы функции от n переменных перенумеруем так, что для любых двух функций f и h номер функции f больше номера функции h, если $\mu(f) > \mu(h)$. Пусть f — произвольная функция из $F(L,n)$. Легко видеть, что $d \geqslant 32\ln(N_\mu(L,n)2^n))$ и $M \geqslant 2d(\log 2^{n+2}/d)^2$. Так как для любых областей D' и D, $D' \subseteq D$, справедливо неравенство $\mu(f_{D'}) \leqslant \mu(f_D)$, то можно воспользоваться теоремой 1, положив $p = 2$. Из этой теоремы следует, что среди областей D' мощности M', $M' \leqslant 2d(\log 2^{n+2}/d)^2 \leqslant M$, имеются такие области $D_1,\ldots,D_s$, что

$$f = M(f_{D_1},\ldots,f_{D_s}),$$

где

$$s = 2l-1 \text{ и } l = \left\lceil \frac{\log(2^n/(d\log(2^n/d)))}{\log(d/6\ln(N_\mu(L,n)2^n))} \right\rceil + 1 \leqslant \frac{3\log(2^n/(d\log(2^n/d)))}{\log(d/6\ln(N_\mu(L,n)2^n))}.$$

Функция f однозначно определяется своими сужениями $f_{D_1},\ldots,f_{D_s}$, или, что то же самое, номерами этих сужений. Положим

$$R = \frac{3\log(2^n/6\ln(N_\mu(L(f),n)2^n)))}{\log(d/6\ln(N_\mu(L(f),n)2^n))}.$$

Тогда имеем $s < 2R$ и $\mu(f_{D_i}) \leqslant L/3R$. Поскольку

$$|F(L,n)| \leqslant (N_\mu(L/3R,n))^{2R},$$

в силу (17) имеем

$$|F(L,n)| \leqslant (N_\mu(L/3R,n))^{2R} \leqslant N_\mu(2L/3,n).$$

Так как по предположению $|F(L,n)| \geqslant \delta N_\mu(L,n)$, то из (17) и предыдущего неравенства следует, что

$$\delta N_\mu(L/3,n)N_\mu(2L/3,n) \leqslant \delta N_\mu(L,n) \leqslant N_\mu(2L/3,n)$$

или, применяя (18),

$$\delta 2^{\lfloor L/6\rfloor} \leqslant 1.$$

Поскольку δ — константа, приходим к противоречию. Следовательно, сделанное предположение неверно. Поэтому почти у каждой функции f найдется такое сужение f_D, что

$$\mu(f_D) \geqslant \frac{L\log(d/6\ln(N_\mu(L,n)2^n)))}{9\log(2^n/6\ln(N_\mu(L,n)2^n))}.$$

Из условий теоремы легко получаем неравенство

$$\log(Mq/(32\ln(N_\mu(L,n)2^n))) \geqslant 4\log q.$$

Следовательно,

$$\mu(f_D) \geqslant \frac{L\log(Mq/6\ln(N_\mu(L,n)2^n)) - 3\log q}{9\log(2^n/6\ln(N_\mu(L,n)2^n))}$$
$$\geqslant \frac{L\log(Mq/6\ln(N_\mu(L,n)2^n))}{36\log(2^n/6\ln(N_\mu(L,n)2^n))} \geqslant \frac{L\log(Mq/6\ln(N_\mu(L,n)))}{36\log(2^n/6\ln(N_\mu(L,n)))}.$$

Теорема 3 доказана.

3. Нижние оценки для сложности сужений булевых функций. Схемы из функциональных элементов

Все встречающиеся ниже сужения продолжаются при помощи минимальных продолжений относительно соответствующих мер сложности.

Пусть $\widetilde{N}(L,n)$ обозначает число неизоморфных схем из функциональных элементов в базисе $\{\vee, \&, \bar{}\}$, каждая из которых имеет n входов, 1 выход и сложность, не превосходящую L. Из результата О. Б. Лупанова [8] следует, что

$$\widetilde{N}(L,n) \leqslant (c_1(L+n))^{L+n}.$$

Введем функцию $N(L,n) = (c_1(L+n))^{L+n}$. Эту функцию будем использовать вместо функции $\widetilde{N}(L,n)$. Такая замена позволит упростить многие преобразования. Заметим, что все доказываемые ниже утверждения останутся справедливыми при замене функции $N(L,n)$ на любую другую функцию $H(L,n)$ такую, что $H(L,n) > \widetilde{N}(L,n)$ и $\ln H(L,n)$ — вогнутая по L функция. Справедлива следующая

Теорема 4. *Пусть функция $f : \{0,1\}^n \to \{0,1\}$ существенно зависит от всех переменных. Тогда среди областей мощности M, $M \geqslant L(f)\log L(f)$, имеется область D такая, что сложность $L(f_D)$ минимального продолжения функции f_D удовлетворяет неравенству*

$$L(f_D) \geqslant \max\left(n-1, L(f)\frac{c_2\log\dfrac{M\log(2^{n+2}/\log N(L(f),n))}{\log N(L(f),n)}}{\log(2^{n+2}/\log N(L(f),n))}\right).$$

Перед тем как доказывать теорему, сделаем ряд замечаний, касающихся формулировки теоремы. Прежде всего, напомним [1, 8], что частичная булева функция, определенная на множестве мощности M, может быть реализована схемой, содержащей не более $(1+o(1))M/\log M$

элементов. Поэтому можно утверждать, что среди функций сложности L найдутся функция f и область D мощности $L\log L$ такие, что $L(f_D) = O(L)$. Таким образом, ограничение $M \geqslant L(f)\log L(f)$ является достаточно естественным и указывает на размер области сужения, при котором сложность сужаемой функции не обязательно уменьшается. Далее, величина из правой части неравенства теоремы достаточно громоздка. Поэтому имеет смысл привести хотя и более слабое, но более простое неравенство. Легко видеть, что множитель, стоящий после $L(f)$, тем меньше, чем меньше $L(f)$ и M. Следовательно, минимальное значение множителя будет достигаться на функциях полиномиальной сложности и в областях полиномиальной мощности. В этом случае неравенство теоремы принимает следующий вид:

$$L(f_D) \geqslant \max\left(n-1, L(f)\frac{c_2\log n}{n}\right).$$

Доказательство теоремы основано на приводимых ниже леммах 5–8, к формулировке и доказательству которых мы переходим.

Лемма 5. *Пусть* L, d — *положительные,* $L \geqslant n-1$, $D \subset \{0,1\}^n$, $|D| \geqslant d$, $|D| \geqslant 2d\log(4|D|/d)$, $d \geqslant 32\ln(N(L,n)|D|)$ *и* $f : D \to \{0,1\}$. *Далее, пусть для любой области* D' *такой, что* $D' \subset D$ *и* $|D'| \leqslant 2d(\log(4|D|/d))^2$, *справедливо неравенство* $L(f_{D'}) \leqslant L$. *Тогда*

$$L(f) \leqslant L\frac{6\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))} \leqslant L\frac{6\log(|D|/(6\ln(N(L,n)|D|))}{\log(d/6\ln(N(L,n)|D|))}.$$

Доказательство. Положим $p = 2$, $N_\mu(L,n) = N(L,n)$. Легко видеть, что в этом случае из справедливости условий настоящей леммы следует справедливость условий теоремы 1. Согласно этой теореме имеем

$$f = M(f_{D_1}, \ldots, f_{D_s}),$$

где $L(f_{D_i}) \leqslant L$, $l = \left\lceil \dfrac{\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))} \right\rceil + 1$, $s = 2l-1$. Учитывая, что $\dfrac{\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))} > 1$, $L(M) \leqslant 18s$ и $L \geqslant n-1$, после несложных преобразований получаем, что при любом достаточно большом n справедливы неравенства

$$L(f) \leqslant L\left(2\left\lceil\frac{\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))}\right\rceil + 1\right) + 18s$$

$$\leqslant (L+18)\left(2\left\lceil\frac{\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))}\right\rceil + 1\right) \leqslant L\frac{6\log(|D|/(d\log(|D|/d)))}{\log(d/6\ln(N(L,n)|D|))}$$

$$\leqslant L\frac{6\log(|D|/(6\ln(N(L,n)|D|))}{\log(d/6\ln(N(L,n)|D|))}.$$

Лемма 5 доказана.

Лемма 6. *Пусть* $D \subset \{0,1\}^n$, $f : D \to \{0,1\}$,

$$L(f) \geqslant (n-1)\frac{6\log(|D|/6\ln(N(L,n)|D|))}{\log(d/6\ln(N(L,n)|D|))},$$

$$M \geqslant 64(\log(4|D|/(\ln(N(L(f),n)|D|)))^2\ln(N(L(f),n)|D|),$$

$d = M/2\log(4|D|/(\ln(N(L(f),n)|D|)))^2$, $|D| \geqslant 2d(\log(4|D|/d))$ *и* $|D| \geqslant d$. *Тогда среди областей мощности* M *имеется область* D' *такая, что*

$$L(f_{D'}) \geqslant L(f)\frac{\log(d/6\ln(N(L(f),n)|D|)))}{6\log(|D|/\ln(N(L(f),n)|D|))}.$$

Доказательство. Используем метод от противного. Предположим, что для любой области D мощности M справедливо неравенство

$$L(f_{D'}) < L(f)\frac{\log(d/6\ln(N(L(f),n)|D|))}{6\log(|D|/\ln(N(L(f),n)|D|))}.$$

Положим $L = \max_{D,|D|=M} L(f_D)$. Будем считать, что $L < L(f)$. В противном случае утверждение леммы тривиально. Легко видеть, что $d \geqslant 32\ln(N(L(f),\, n|D|))$ и $M \geqslant 2d(\log(4|D|/d))^2$. Поэтому можно воспользоваться леммой 5. Из этой леммы следует, что

$$L(f) \leqslant L\frac{6\log(|D|/(6\ln(N(L,n)|D|)))}{\log(d/6\ln(N(L,n)|D|))}.$$

Но тогда в силу сделанного предположения имеем

$$\begin{aligned} L < L(f)&\frac{\log(d/6\ln(N(L(f),n)|D|))}{6\log(|D|/\ln(N(L(f),n)|D|))} \\ &\leqslant L\frac{\log(d/6\ln(N(L(f),n)|D|))}{6\log(|D|/\ln(N(L(f),n)|D|))}\,\frac{6\log(|D|/6\ln(N(L,n)|D|))}{\log(d/6\ln(N(L,n)|D|))}. \end{aligned} \tag{19}$$

Пусть $x > y > z > t > 0$. Тогда

$$\frac{y-z}{x-z}\cdot\frac{x-t}{y-t} < \frac{y-t}{x-t}\cdot\frac{x-t}{y-t} = 1.$$

Положим $x = \log|D|$, $y = \log d$, $z = \log(6\ln(N(L(f),n)|D|))$ и $t = \log(6\ln(N(L,n)|D|))$. Преобразуя (19) с помощью полученного неравенства, получаем $L < L$. Противоречие. Лемма 6 доказана.

Лемма 7. *Пусть функция* $f : \{0,1\}^n \to \{0,1\}$ *существенно зависит от всех переменных,* $q = \log(2^{n+2}/\ln(N(L(f),n)2^n))$ *и* $M \geqslant 64q^3\ln(N(L(f),n)2^n)$. *Тогда среди областей мощности* M *имеется область* D' *такая, что*

$$L(f_{D'}) \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{24q} \geqslant L(f)\frac{\log q}{6q}.$$

Доказательство. Положим $d = M/2q^2$. Так как

$$M \geqslant 64q^3 \ln(N(L(f),n)2^n),$$

легко видеть, что

$$\log(Mq/\ln(N(L(f),n)2^n)) \geqslant 4\log q - 5.$$

Далее имеем

$$\frac{\log(d/(6\ln(N(L(f),n)2^n)))}{6\log(2^n/\ln(N(L(f),n)2^n))} \geqslant \frac{\log(M/12q\ln(N(L(f),n)2^n))}{6\log(2^n/\ln(N(L(f),n)2^n)}$$
$$\geqslant \frac{\log(Mq/\ln(N(L(f),n)2^n)) - 3\log q - \log 12}{6\log(2^n/\ln(N(L(f),n)2^n)}$$
$$\geqslant \frac{\log(Mq/\ln(N(L(f),n)2^n))}{24\log(2^n/\ln(N(L(f),n)2^n))} \geqslant \frac{\log q}{6q}.$$

Из этих неравенств следует, что если

$$L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{24q} \geqslant L(f)\frac{\log q}{6q} \geqslant n-1,$$

то можно воспользоваться леммой 6.

Пусть эти неравенства выполняются. Тогда найдется область D' такая, что

$$L(f_{D'}) \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{24q} \geqslant L(f)\frac{\log q}{6q}.$$

Если $L(f)\frac{\log q}{6q} < n-1$, то существование требуемой области следует из существенной зависимости f от n переменных. Лемма 7 доказана.

Лемма 8. *Пусть функция* $f : \{0,1\}^n \to \{0,1\}$ *существенно зависит от всех переменных,* $L(f) = o(2^n/n)$, $q = \log(2^{n+2}/\ln(N(L(f),n)2^n))$ *и* $L(f)\ln L(f) \leqslant M \leqslant 64q^3\ln(N(L(f),n)2^n)$. *Тогда среди областей мощности* M *имеется область* D *такая, что*

$$L(f_D) \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{750q}.$$

Доказательство. Доказывая лемму, будем полагать, что сложность всех рассматриваемых сужений не меньше $n-1$. Если это не так, то, как и при доказательстве предыдущей леммы, легко видеть, что существование требуемой области следует из существенной зависимости f от n переменных.

Положим $M_0 = 64q^3\ln(N(L(f),n)2^n)$. В силу леммы 7 найдется такая область D' мощности $\lceil M_0 \rceil$, что

$$L(f_{D'}) \geqslant L(f)\frac{\log q}{6q}.$$

Без ограничения общности можно считать, что $L(f_{D'}) = \lceil L(f)\frac{\log q}{6q}\rceil$. Положим

$$M = \frac{64q}{(\log q)^5}\left(\log\frac{4M_0}{\ln(N(L(f_{D'}),n)M_0)}\right)^2 \ln(N(L(f_{D'}),n)M_0).$$

Тогда при любом достаточно большом n имеем неравенства

$$\lceil M\rceil \leqslant \frac{64q}{(\log q)^5}\left(\log\frac{4\cdot 64q^3\ln(N(L(f),n)2^n)}{\ln(N(L(f)\frac{\log q}{6q},n))}\right)^2 \ln(N(L(f)\frac{\log q}{6q},n)2^n)$$
$$\leqslant \frac{64q}{(\log q)^5}(\log q^4)^2 3L(f)\frac{\log q}{6q}\ln L(f) \leqslant L(f)\ln L(f) \leqslant M_0.$$

Положим $d = M/2(\log(4M_0/\ln(N(L(f_{D'}),n)M_0)))^2$. Для применимости к функции $f_{D'}$ леммы 6 достаточно показать, что $M_0 \geqslant d$ и $M_0 \geqslant 2d\log(4M_0/d)$. Здесь, как и в лемме 6, мощность области сужения обозначим символом M. Положим $x = M_0/d$. Тогда второе неравенство можно переписать в виде $g(x) = x - 2\log x - 4 \geqslant 0$. Поскольку $g(16) = 4$ и $g'(x) > 0$ при $x \geqslant 16$, имеем $g(x) > 0$ при $x \geqslant 16$. Поэтому достаточно убедиться, что $M_0 \geqslant 16d$. Так как

$$M_0/d \geqslant M/d = 2\left(\log\frac{4M_0}{\ln(N(L(f_{D'}),n)M_0)}\right)^2$$
$$\geqslant 2\left(\log\frac{4\cdot 64q^3\ln(N(L(f),n)2^n}{\ln(N(L(f_{D'}),n)M_0)}\right)^2 \geqslant 2(\log 4\cdot 64q^3)^2,$$

$L(f) = o(2^n/n)$ и q растет с ростом n, то $M_0/d \geqslant 128$ и можно применить лемму 6. Эта лемма гарантирует существование такой области $D \subseteq D'$, что $|D| = M$ и

$$L(f_D) \geqslant L(f_{D'})\frac{\log(d/6\ln(N(L(f_{D'}),n)M_0)))}{6\log(M_0/\ln(N(L(f_{D'}),n)M_0))}.$$

Так как $\frac{a+x}{b+x} \geqslant \frac{a}{b}$ при $b \geqslant a$, $N(L(f_{D'}),n) \leqslant N(L(f),n)$, $M \leqslant M_0$, то

$$L(f_D) \geqslant L(f_{D'})\frac{\log q - 5\log\log q}{6\log(64q^3))} \geqslant L(f_{D'})\frac{\log q}{25\log q} \geqslant L(f)\frac{\log q}{150q}.$$

Поскольку $M \leqslant 64q^3\ln(N(L(f),n)2^n)$, легко видеть, что

$$\log q \geqslant \frac{1}{5}\log(Mq/\ln(N(L(f),n)2^n)).$$

Следовательно,

$$L(f_D) \geqslant L(f)\frac{\log q}{150q} \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{750q}.$$

Лемма 8 доказана.

Доказательство теоремы 4. Будем полагать, что сложность каждого рассматриваемого сужения не меньше $n-1$. Если это не так, то существование требуемой области следует из существенной зависимости f от n переменнных.

Если $L(f) = \Theta(2^n/n)$, то утверждение теоремы тривиально. При $L(f) = o(2^n/n)$ утверждение теоремы следует из лемм 7 и 8. При $L(f)\ln L(f) \leqslant M \leqslant 64q^3\ln(N(L(f),n)2^n)$ воспользуемся леммой 8. Из этой леммы следует существование такой области D мощности M, что

$$L(f_D) \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{750q}.$$

При $M \geqslant 64q^3\ln(N(L(f),n)2^n)$ из леммы 7 следует, что существует такая область D мощности M, что

$$L(f_D) \geqslant L(f)\frac{\log(Mq/\ln(N(L(f),n)2^n))}{24q}.$$

Таким образом, при всех $M \geqslant L(f)\ln L(f)$ существует область D мощности M такая, что

$$L(f_D) \geqslant L(f)\frac{c_3\log(Mq/\ln(N(L(f),n)2^n))}{q}.$$

Так как $\frac{a+x}{b+x} \geqslant \frac{a}{b}$ при $b \geqslant a$, то при $2^n \geqslant M/\ln 2$ имеем

$$L(f_D) \geqslant L(f)\frac{c_3\log\left(\dfrac{M\log(2^n/\log(N(L(f),n)2^n))}{\ln 2\log(N(L(f),n))}\right)}{\log(2^n/\log N(L(f),n))}.$$

При $L(f) \geqslant n-1$ и $2^n \geqslant \log(N(L(f),n))$ последнее неравенство очевидными преобразованиями приводится к виду

$$L(f_D) \geqslant L(f)\frac{c_4\log\left(\dfrac{M\log(2^{n+2}/\log N(L(f),n))}{\log N(L(f),n)}\right)}{\log(2^{n+2}/\log N(L(f),n))}.$$

Теорема 4 доказана.

В следующей теореме для произвольных булевых функций доказывается нижняя оценка для мощности областей в $\{0,1\}^n$, сложность сужения на которые не более чем в постоянное число раз отличается от сложности самых сложных частичных функций, которые могут быть определены в областях подобной мощности. Неформально можно сказать, что в теореме 5 устанавливается локальная одинаковость с точки зрения сложности всех булевых функций, сложность которых превосходит некоторое пороговое значение.

Положим $\log^{(k)} n = \underbrace{\log\log\ldots\log}_{k \text{ раз}} n$ и $\log^* n = k$, если $0 < \log^{(k)} n \leqslant 1$.

Теорема 5. *Существуют такие константы c_5 и c_6, что для любой функции $f : \{0,1\}^n \to \{0,1\}$, которая существенно зависит от всех переменных и $L(f) \geqslant n^{2+\epsilon}$ (ϵ — произвольная положительная константа), найдется область $D \subseteq \{0,1\}^n$ такая, что сложность $L(f_D)$ минимального продолжения f_D удовлетворяет неравенствам:*

(a) $L(f_D)\log L(f_D) \leqslant 2|D|$,

(b) $L(f_D)\log L(f_D) \geqslant c_5|D|$,

(c) $L(f_D) \geqslant L(f)/(q \cdot c_6^{\log^* q})$,

где $q = \log(2^n/\ln(N(L(f),n)2^n))$.

Сначала сформулируем и докажем две используемые в этом доказательстве леммы.

Лемма 9. *Пусть $L \geqslant n\log n$, $D \subset \{0,1\}^n$, $a = |D|/2L\log L$, $f : D \to \{0,1\}$, $|D| \geqslant 2^{17}L\log L$. Далее, пусть для любой области D' такой, что $D' \subset D$, $|D'| \leqslant 4L\log L(\log a)^3$, справедливо неравенство $L(f_{D'}) \leqslant L$. Тогда*

$$L(f) \leqslant L^{\dfrac{24\log \dfrac{a}{\log a \cdot \log(a/\log a)}}{\log\log a}}.$$

Доказательство. Положим $d = (\log a)\cdot 2L\log L$. Нетрудно показать, что при выполнении условий настоящей леммы при всех n, больших некоторого n_0, справедливы неравенства

$$\ln(N(L,n)|D|) \leqslant L\log L, \quad a \geqslant 2^{16}, \quad d \geqslant 32\ln(N(L,n)|D|). \tag{20}$$

Тогда

$$2d(\log(4|D|/d))^2 \leqslant 2(\log a)\,2L\log L\cdot\left(\log\frac{4a}{\log a}\right)^2 \leqslant 4L\log L\cdot\left(\log\frac{|D|}{2L\log L}\right)^3. \tag{21}$$

Продолжая последнее неравенство, видим, что при $a \geqslant 2^{16}$ имеет место неравенство

$$2d(\log(4|D|/d))^2 \leqslant 4L\log L\,(\log a)^3 \leqslant |D|. \tag{22}$$

Из (21) следует, что для любой области D' такой, что $D' \subset D$ и

$$|D'| \leqslant 2d(\log(4|D|/d))^2,$$

справедливо неравенство $L(f_{D'}) \leqslant L$. Пользуясь этим фактом и соотношениями (20)–(22), видим, что можно воспользоваться леммой 5. Так

как $|D|/d = a/\log a$, то, учитывая неравенство $a \geqslant 2^{16}$, имеем

$$L(f) \leqslant L\frac{6\log\dfrac{|D|}{d\log(|D|/d)}}{\log(d/12L\log L)} \leqslant L\frac{6\log\dfrac{a}{\log a\cdot\log(a/\log a)}}{\log\log a - \log 6} \leqslant L\frac{24\log\dfrac{a}{\log a\cdot\log(a/\log a)}}{\log\log a}.$$

Лемма 9 доказана.

Лемма 10. *Пусть* $D \subset \{0,1\}^n$, $f : D \to \{0,1\}$, $|D| \geqslant 2^{17}L(f)\log L(f)$ *и* $L = L(f)\dfrac{\log\log(|D|/2L(f)\log L(f))}{24\log(|D|/2L(f)\log L(f))} \geqslant n\log n$. *Тогда среди областей* $\widetilde{D}$ *таких, что* $\widetilde{D} \subset D$ *и* $|\widetilde{D}| = \left\lfloor 4L\log L\cdot\left(\log\dfrac{|D|}{2L\log L}\right)^3\right\rfloor$, *найдется область* D' *такая, что*

$$L(f_{D'}) \geqslant L.$$

Доказательство. Положим $a = |D|/2L\log L$ и $b = |D|/2L(f)\log L(f)$. Докажем лемму методом от противного. Предположим, что для любой области $\widetilde{D}$, удовлетворяющей условиям леммы, справедливо неравенство

$$L(f_{\widetilde{D}}) < L = L(f)\frac{\log\log b}{24\log b}.$$

Положим $\widetilde{L} = \max_{\widetilde{D}} L(f_{\widetilde{D}})$. Тогда

$$\widetilde{L} < L(f)\frac{\log\log b}{24\log b}. \tag{23}$$

Из леммы 9 следует, что

$$L(f) \leqslant \widetilde{L}\frac{24\log\dfrac{a}{\log a\cdot\log(a/\log a)}}{\log\log a}. \tag{24}$$

Так как $L \geqslant n\log n$, $\log a < n$, то $L(f) < L^2$ и $\log L(f)/\log L < 2$. Поэтому

$$\frac{a}{b} = \frac{L(f)\log L(f)}{L\log L} < \frac{48\log a}{\log\log a}.$$

Следовательно,

$$b > \frac{a\log\log a}{48\log a}.$$

Объединив (23) с (24) и подставив последнее неравенство, получаем

$$\widetilde{L} < \widetilde{L}^{\frac{\log \frac{a}{\log a \cdot \log(a/\log a)}}{\log\log a} \cdot \frac{\log\log b}{\log b}} \leqslant \widetilde{L}^{\frac{\log \frac{a}{\log a \cdot \log(a/\log a)}}{\log b}} \leqslant \widetilde{L}^{\frac{\log \frac{a}{\log a \cdot \log(a/\log a)}}{\log \frac{a \log\log a}{48 \log a}}}.$$

Покажем, что дробь, стоящая в последнем неравенстве после $\widetilde{L}$, меньше единицы. Разделив аргумент логарифма числителя на аргумент логарифма знаменателя, видим, что

$$\frac{a}{\log a \cdot \log(a/\log a)} \cdot \frac{48 \log a}{a \log\log a} = \frac{48}{\log(a/\log a) \cdot \log\log a}.$$

Так как $a > b \geqslant 2^{16}$, то $\log(a/\log a) \cdot \log\log a \geqslant 48$. Следовательно, $\widetilde{L} < \widetilde{L}$. Противоречие. Лемма 10 доказана.

Доказательство теоремы 5. Пункт (a) — прямое следствие основных теорем из [1, 8]. Докажем пункты (b) и (c). Положим $D^0 = D$, $f^0 = f$. К функции f последовательно k раз применим лемму 10. В результате получим области D^i и функции $f^i : D^i \to \{0,1\}$, $1 \leqslant i \leqslant k$, такие, что

$$L(f^i) \geqslant L(f^{i-1}) \frac{\log\log(|D^{i-1}|/2L(f^{i-1})\log L(f^{i-1}))}{24\log(|D^{i-1}|/2L(f^{i-1})\log L(f^{i-1}))},$$

$$|D^i| = \left\lfloor 4L(f^{i-1})\log L(f^{i-1}) \left(\log \frac{|D^{i-1}|}{2L(f^{i-1})\log L(f^{i-1})}\right)^3 \right\rfloor.$$

Легко видеть, что применять эту лемму можно до тех пор, пока справедливы неравенства $|D^i| \geqslant 2^{20} L(f^i)\log L(f^i)$ и $L(f^i) \geqslant n\log n$. Будем использовать лемму 10, пока справедливо первое из этих неравенств. В конце доказательства покажем, что второе неравенство следует из первого. Положим $a^i = |D^i|/2L(f^i)\log L(f^i)$. Тогда

$$L(f^i) \geqslant L(f^{i-1}) \frac{\log\log a^{i-1}}{24\log a^{i-1}}, \tag{25}$$

$$|D^i| \leqslant 4L(f^{i-1})\log L(f^{i-1}) \cdot (\log a^{i-1})^3, \tag{26}$$

$$a^i \geqslant 2^{19}. \tag{27}$$

В условиях доказываемой теоремы нетрудно показать, что $(L(f^i))^2 \geqslant L(f^{i-1})$. Для этого достаточно заметить, что $\log a^0 \leqslant n$ и $\log a^1 \leqslant 5\log n$.

Следовательно, учитывая (25)–(27), получаем

$$a^i \leqslant \frac{4L(f^{i-1})\log L(f^{i-1})}{2L(f^i)\log L(f^i)}(\log a^{i-1})^3 \leqslant \frac{4L(f^i)\log L(f^i)}{2L(f^i)\log L(f^i)}\frac{2\cdot 24(\log a^{i-1})^4}{\log\log a^{i-1}}$$
$$\leqslant \frac{96(\log a^{i-1})^4}{\log\log a^{i-1}} \leqslant (4\log a^{i-1})^4. \quad (28)$$

Поэтому

$$\frac{\log\log a^{i-1}}{24\log a^i} \geqslant \frac{\log\log a^{i-1}}{24\log(4\log a^{i-1})^4} \geqslant \frac{\log\log a^{i-1}}{120\log\log a^{i-1}} = \frac{1}{120}.$$

Последовательное применение (25) и последнего неравенства дает

$$L(f^k) \geqslant \frac{\log\log a^{k-1}}{24\log a^{k-1}} \cdots \frac{\log\log a^0}{24\log a^0} L(f) \geqslant \frac{1}{120^{k-1}}\frac{\log\log a^{k-1}}{24\log a^0} L(f). \quad (29)$$

Рассмотрим числовую последовательность $\{b_i\}$, $b_1 = q$ и $b_i = (4\log b_{i-1})^4$ при $i > 1$. Дифференцируя функцию $(4\log x)^4 x^{-1}$, легко видеть, что последовательность $\{b_i\}$ убывает по крайней мере до тех пор, пока $b_i \geqslant 2^{20}$. Поэтому из неравенства (28) следует существование такого k, при котором $a^k < 2^{20} \leqslant a^{k-1}$. Оценим это k. Последовательно применяя (28), видим, что

$$a_k \leqslant (4\log a_{k-1})^4 \leqslant (4\log(4\log a_{k-2})^4)^4$$
$$\leqslant \underbrace{(4\log(4\log\ldots(4\log}_{k-1\text{ раз}} a_1)^4\ldots)^4)^4 \leqslant \underbrace{(4\log(4\log\ldots(4\log}_{k-1\text{ раз}} q)^4)^4\ldots)^4$$
$$\leqslant \underbrace{(\log(\log\ldots(\log}_{k-1\text{ раз}} q)^5)\ldots)^5)^5 \leqslant (\log^{(k-1)} q)^5.$$

Так как $a^{k-1} \geqslant 2^{20}$, то $2^{20} \leqslant a^{k-1} \leqslant (\log^{(k-2)} q)^5$. Следовательно, $1 \leqslant \log^{(k)} q$ и $k \leqslant \log^*(q)$. Подставляя последнее неравенство в (29), получаем

$$L(f^k) \geqslant \frac{1}{120^{\log^*(q)-1}}\frac{\log 20}{24q} L(f).$$

Так как $L(f) \geqslant n^{2+\epsilon}$, то очевидно, что $L(f^k) > n\log n$. Поэтому лемма 10 может быть использована необходимое число раз. Теорема 5 доказана.

В заключение данного пункта отметим, что задачи, аналогичные рассмотренным в теоремах 4 и 5, можно рассматривать и для булевых операторов. Нетрудно убедиться, что теорема 4 имеет векторный аналог. Утверждение, аналогичное теореме 5, для вектор-функций места не имеет. Это связано с тем, что области, существование которых гарантирует теорема 5, могут быть различны для различных компонент вектор-функции.

4. Функции с малым числом единиц

Для самой сложной функции фиксированного веса в приводимой ниже теореме устанавливаются верхние оценки для сложности сужений этой функции на области различной мощности. Далее будет показано, что полученные оценки по порядку совпадают с нижними оценками из теоремы 4.

Теорема 6. *Пусть f — самая сложная функция веса w, $n^3 \leqslant w \leqslant 2^n/a(n)$, где $a(n)$ — неограниченно возрастающая функция. Тогда для любой области $D \subseteq \{0,1\}^n$ такой, что $|D| \geqslant L(f)\log L(f)$, сложность $L(f_D)$ минимального продолжения функции f_D удовлетворяет неравенству*

$$L(f_D) \leqslant L(f)\frac{c_7 \log \dfrac{M \log(2^{n+2}/L(f)\log L(f)}{L(f)\log L(f)}}{\log(2^{n+2}/L(f)\log L(f))}.$$

Доказательство. Из результата О. Б. Лупанова [3] о сложности реализации полностью определенных булевых функций с малым числом единиц схемами из функциональных элементов легко следует неравенство

$$L(f) \leqslant \frac{2\log\binom{2^n}{w(f)}}{\log\log\binom{2^n}{w(f)}}.$$

Аналогичное неравенство справедливо и для частичных булевых функций. Из [7, лемма 6] следует, что существует константа c_9 такая, что для произвольной функции $h : D \to \{0,1\}$, $w(h) \geqslant n^3$, имеет место неравенство

$$L(h) \leqslant \frac{c_9 \log\binom{|D|}{w(h)}}{\log\log\binom{|D|}{w(h)}}.$$

Положим $M = |D|$ и $w = w(f)$. Тогда

$$\frac{\log\binom{M}{w}}{\log\log\binom{M}{w}} \leqslant \frac{w\log(3M/w)}{\log(w\log(3M/w))}.$$

Следовательно, для рассматриваемой в теореме функции f имеем

$$L(f_D)\log L(f_D) \leqslant c_9 w \log(3M/w),$$
$$w \geqslant \frac{L(f_D)\log L(f_D)}{c_9\log(3M/w)}. \tag{30}$$

Аналогичным образом получаем неравенство

$$w \geqslant \frac{L(f)\log L(f)}{c_9\log(3\cdot 2^n/w)}, \tag{31}$$

из которого следует, что

$$(2^n/w)^{1/2} \leqslant \frac{2^n}{w\log(2^n/w)} \leqslant \frac{c_{10}2^n}{L(f)\log L(f)}.$$

Подставляя (31) и последнее неравенство в (30), после несложных преобразований получаем

$$w \geqslant \frac{c_9 L(f_D)\log L(f_D)}{\log\left(\dfrac{3Mc_9\log\left(\dfrac{3\cdot 2^n c_{10}}{L(f)\log L(f)}\right)^2}{L(f)\log L(f)}\right)} \geqslant \frac{c_{11}L(f_D)\log L(f_D)}{\log\left(\dfrac{M\log\dfrac{2^n}{L(f)\log L(f)}}{L(f)\log L(f)}\right)}.$$

С другой стороны,

$$L(f)\log L(f) \geqslant \log\binom{2^n}{w} \geqslant w\log\frac{2^n}{w},$$

$$w \leqslant \frac{L(f)\log L(f)}{\log(2^n/w)} \leqslant \frac{L(f)\log L(f)}{\log\dfrac{2^n\log(2^n/w)}{L(f)\log L(f)}} \leqslant \frac{L(f)\log L(f)}{\log\dfrac{2^n}{L(f)\log L(f)}}.$$

Из двух последних неравенств для w следует, что

$$\frac{L(f_D)\log L(f_D)}{L(f)\log L(f)} \leqslant \frac{c_{11}\log\dfrac{M\log(2^n/(L(f)\log L(f)))}{L(f)\log L(f)}}{\log(2^n/L(f)\log L(f))}.$$

Поэтому

$$L(f_D) \leqslant L(f)\frac{c_{12}\log\left(\dfrac{M\log(2^{n+2}/L(f)\log L(f))}{L(f)\log L(f)}\right)}{\log(2^{n+2}/L(f)\log L(f))}.$$

Теорема 6 доказана.

Из теоремы 4 следует, что у функции f, рассматриваемой в теореме 6, существует сужение f_D такое, что

$$L(f_D) \geqslant L(f)\frac{c_2\log\left(\dfrac{M\log(2^{n+2}/N(L(f),n))}{\log N(L(f),n)}\right)}{\log(2^{n+2}/N(L(f),n)))}. \tag{32}$$

Так как $\frac{a+x}{b+x} \geqslant \frac{a}{b}$ при $b \geqslant a$ и $\log N(L(f),n) \leqslant 2L(f)\log L(f)$ при $L(f) \geqslant 3n$, то, преобразуя (32), получаем

$$L(f_D) \geqslant L(f)\frac{c_{13}\log\left(\dfrac{M\log(2^{n+2}/L(f)\log L(f))}{L(f)\log L(f)}\right)}{\log(2^{n+2}/L(f)\log L(f))}.$$

Очевидно, что верхняя оценка из теоремы 6 и нижняя оценка из теоремы 4 для $L(f_D)$ различается только постоянным множителем.

5. Нижние оценки для сложности сужений булевых функций. Контактные схемы и формулы

Аналоги теорем 4 и 5 для схем из функциональных элементов справедливы для контактных схем и формул. Эти теоремы (теоремы 7–10) приведем без доказательств. Для контактных схем эти доказательства практически дословно совпадают с соответствующими доказательствами для схем из функциональных элементов. Единственное отличие в доказательства вносит тот факт, что наименьшая известная в настоящее время оценка сложности реализации функции голосования контактными схемами нелинейна и по порядку равна $n(\ln n)^n/(\ln\ln n)^2$ [2]. В случае формул доказательства незначительно отличаются от доказательств аналогичных теорем из [6].

Пусть $\widetilde{N}_k(L,n)$ обозначает число неизоморфных контактных схем с контактами $2n$ видов, каждая из которых имеет один выходной полюс и сложность, не превосходящую L. Из результатов О. Б. Лупанова [3] следует, что

$$\widetilde{N}_k(L,n) \leqslant (c_1 nL)^L.$$

Положим $\widetilde{N}_k(L,n) = (c_1 nL)^L$.

Теорема 7. *Пусть функция $f : \{0,1\}^n \to \{0,1\}$ существенно зависит от всех аргументов. Тогда среди областей мощности M, $M \geqslant L_k(f)\log L_k(f)$, имеется область D такая, что сложность $L_k(f_D)$ минимального продолжения f_D удовлетворяет неравенству*

$$L_k(f_D) \geqslant \max\left(n, L_k(f)/S\left(\frac{c_{14}\log(2^{n+2}/N_k(L_k(f),n))}{\log\dfrac{M\log(2^{n+2}/(N_k(L_k(f),n)))}{\log N_k(L_k(f),n)}}\right)\right),$$

где $S(x) = c_{15}x(\ln x)^4/(\ln\ln x)^2$.

Теорема 8. *Существуют такие константы c_{16} и c_{17}, что для любой функции $f : \{0,1\}^n \to \{0,1\}$ такой, что $L_k(f) \geqslant n^{2+\epsilon}$ (ϵ — произвольная положительная константа), найдется такая область $D \subseteq \{0,1\}^n$, что сложность $L_k(f_D)$ минимального продолжения f_D удовлетворяет неравенствам*

(a) $L_k(f_D)\log L_k(f_D) \geqslant c_{16}|D|$,

(b) $L_k(f_D) \geqslant L_k(f)/S(n\cdot c_{17}^{\log^* n})$,

где $q = \log(2^n/\ln(N_k(L_k(f),n)2^n))$.

Обозначим через $\widetilde{N}_\phi(L,n)$ число таких неизоморфных формул в произвольном базисе, состоящем из двухместных функций и содержащем

дизъюнкцию и конъюнкцию, которые зависят от n переменных и имеют сложность не более L. Из [3] следует, что

$$\widetilde{N}_\phi(L,n) \leqslant (c_{18}n)^L. \tag{33}$$

Положим $N_\phi(L,n) = (c_{18}n)^L$.

Теорема 9. *Пусть функция $f : \{0,1\}^n \to \{0,1\}$ существенно зависит от всех аргументов. Тогда среди областей мощности M, $M \geqslant L_\phi(f)\log n$, имеется область D такая, что сложность $L_\phi(f_D)$ минимального продолжения f_D удовлетворяет неравенству*

$$L_\phi(f_D) \geqslant \max\left(n, L_\phi(f)\left(\frac{c_{19}\log\dfrac{M\log(2^{n+2}/N_\phi(L_\phi(f),n))}{\log N_\phi(L_\phi(f),n)}}{\log(2^{n+2}/N_\phi(L_\phi(f),n)))}\right)^2\right).$$

Теорема 10. *Существуют такие константы c_{20} и c_{21}, что для любой функции $f : \{0,1\}^n \to \{0,1\}$ такой, что $L_\phi(f) \geqslant n^{3+\epsilon}$ (ϵ — произвольная положительная константа), найдется такая область $D \subseteq \{0,1\}^n$, что сложность $L_\phi(f_D)$ минимального продолжения f_D удовлетворяет неравенствам*

(a) $L_\phi(f_D)\log n \geqslant c_{20}|D|$,

(b) $L_\phi(f_D) \geqslant c_{21}L_\phi(f)/q^2$,

где $q = \log(2^n/\ln(N_\phi(L_\phi(f),n)2^n))$.

Оценки из теорем 9 и 10 несколько слабее соответствующих оценок для схем из функциональных элементов и контактных схем (теоремы 4, 5, 7, 8). Возможно, это связано только с тем, что метод, использованный при доказательстве всех этих теорем, более приспособлен для схем из функциональных элементов и контактных схем, чем для формул. Поэтому можно предположить, что для формул справедливы более высокие, по сравнению с полученными в теоремах 9 и 10, оценки. Косвенным подтверждением этого предположения является следующая теорема — аналог теоремы 10 — справедливая «для почти всех функций». Подобный аналог имеет место и для теоремы 9, однако мы его не приводим.

Теорема 11. *Существуют такие константы c_{22} и c_{23}, что для почти каждой функции $f : \{0,1\}^n \to \{0,1\}$ такой, что $L_\phi(f) \geqslant n^{2+\epsilon}$ (ϵ — произвольная положительная константа), найдется такая область $D \subseteq \{0,1\}^n$, что сложность $L_\phi(f_D)$ минимального продолжения f_D удовлетворяет неравенствам*

(a) $L_\phi(f_D)\log n \geqslant c_{22}|D|$,

(b) $L_\phi(f_D) \geqslant \dfrac{c_{23}L_\phi(f)}{q(\log q)^2}$,

где $q = \log(2^n/L_\phi(f)\log n)$.

Справедливость теоремы легко вытекает из следующих трех лемм, приводимых без доказательства. Первая их них — тривиальное следствие теоремы 3 и определения функции $N_\phi(L,n)$.

Лемма 11. *Пусть* $q = \log(2^n/L_\phi(f)\log n)$. *Тогда для почти каждой функции* $f : \{0,1\}^n \to \{0,1\}$ *такой, что* $L_\phi(f) = L$, *и целого*

$$M = \lceil 128\log(2^{n+2}/L\log n)^3 L\log n\rceil$$

среди областей мощности M *найдется такая область* D', *что*

$$L_\phi(f_{D'}) \geqslant L\frac{4c_{24}\log q}{q}.$$

Вторая лемма получается из [6, лемма 5] заменой функции L_π на функцию L_ϕ и использованием неравенства (33).

Лемма 12. *Пусть* $D \subseteq \{0,1\}^n$, $f : D \to \{0,1\}$, $L_\phi \geqslant n$, $|D| \geqslant 2L_\phi\log n$. *Тогда имеется такая область* $D' \subseteq D$, *что*

(a) $|D'| \leqslant 2(2|D|L_\phi(f)\log n)^{1/2}$,

(b) $L_\phi(f'_D) \geqslant \frac{1}{4}L_\phi(f)$.

Третья лемма — простое следствие предыдущей леммы. Она доказывается так же, как и лемма 2 из [6].

Лемма 13. *Пусть* $D \subseteq \{0,1\}^n$, $f : D \to \{0,1\}$, $L_\phi(f) = L \geqslant n$, $|D| \geqslant 2L_\phi(f)\log n$. *Тогда имеется такая область* $D' \subseteq D$, *что*

$$\frac{|D'|}{L_\phi(f_{D'})\log n} \leqslant c_{25}\left(\frac{|D|}{L_\phi(f)\log n}\right)^{1/2}.$$

Доказательство теоремы 11. Пусть $q = \log(2^n/L_\phi(f)\log n)$. В силу леммы 11 для почти каждой функции f найдется такая область D_1, что

$$|D_1| \leqslant 130q^3 L\log n, \quad L_\phi(f_{D_1}) \geqslant L\frac{4c_{24}\log q}{q}. \tag{34}$$

Пусть f — одна из таких функций. К функции f_{D_1} несколько раз последовательно применим лемму 13. В результате получим области D_i и функции f_{D_i}. Положим

$$a^i = \frac{|D_i|}{L_\phi(f_{D_i})\log n}.$$

Тогда из условий леммы и неравенств (34) следует, что

$$a^1 \leqslant q^5, \quad a^k \leqslant c_{25}(a^{k-1})^{1/2} \leqslant \cdots \leqslant (c_{25})^2(a^1)^{1/2^{k-1}}. \tag{35}$$

Пусть k — такое минимальное целое, что $k \geqslant \log(\log(a^1)) + 1$. Тогда $a^k \leqslant 2(c_{25})^2$ и в силу (35) имеем

$$L_\phi(f_{D_k}) \geqslant \left(\frac{1}{4}\right)^{k-1} L_\phi(f_{D_1}) \geqslant \frac{1}{(\log(a^1))^2} L_\phi(f_{D_1})$$
$$\geqslant \frac{1}{(\log(q^5))^2} L \frac{4c_{23}\log q}{q} \geqslant \frac{c_{23}}{q(\log q)^2} L.$$

Положив $D = D_k$, получаем

$$L_\phi(f_D) \geqslant \frac{c_{25}}{q(\log q)^2} L_\phi(f), \quad |D| \leqslant 2(c_{23})^2 L_\phi(f_D) \log n.$$

Остается взять $c_{22} = 1/2(c_{25})^2$. Теорема 11 доказана.

Автор благодарен профессору О. Б. Лупанову за внимание к работе.

ЛИТЕРАТУРА

1. **Андреев А. Е.** О сложности реализации частичных булевых функций схемами из функциональных элементов // Дискрет. математика. 1989. Т. 1, вып. 4. С. 36–45.
2. **Красулина Е. Г.** О сложности реализации монотонных симметрических функций алгебры логики контактными схемами // Математические вопросы кибернетики. М.: Наука, 1988. Вып. 1. С. 140–167.
3. **Лупанов О. Б.** Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. М.: Наука, 1965. Вып. 14. С. 31–110.
4. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
5. **Чашкин А. В.** Об оценках сложности сужений булевых функций // Докл. РАН. 1996. Т. 348, № 5. С. 595–597.
6. **Чашкин А. В.** О сложности сужений булевых функций // Дискрет. математика. 1996. Т. 8, вып. 2. С. 133–150.
7. **Чашкин А. В.** О среднем времени вычисления значений булевых функций // Дискрет. анализ и исслед. операций. Серия 1. 1997. Т. 4, № 1. С. 60–78.
8. **Шоломов Л. А.** О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. М.: Наука, 1969. Вып. 21. С. 215–226.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва,
Россия

Статья поступила
7 апреля 1997 г.