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

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

# ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

## СБОРНИК ЛЕКЦИЙ

## VIII

Москва 2016

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

# ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

## СБОРНИК ЛЕКЦИЙ МОЛОДЕЖНЫХ НАУЧНЫХ ШКОЛ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

## VIII

Москва 2016

Д48
УДК 519.7

**Д48** Дискретная математика и ее приложения: Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск VIII. Под редакцией А. В. Чашкина. — М.: ИПМ им. М. В. Келдыша, 2016. — 45 с.

Восьмой выпуск лекций содержит лекции, прочитанные на X молодежной научной школе по дискретной математике и ее приложениям, проходившей в Москве в ИПМ им. М. В. Келдыша РАН с 5 по 11 октября 2015 г. Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

ДИСКРЕТНАЯ МАТЕМАТИКА
И ЕЕ ПРИЛОЖЕНИЯ
Сборник лекций
Выпуск VIII

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *А. Д. Яшунский*

# НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Ю. А. Комбаров

**Московский государственный университет им. М. В. Ломоносова,
механико-математический факультет,
Москва, Ленинские горы, д. 1, Главное здание**

e-mail: yuri.kombarov@gmail.com

## Введение

Рассматриваются реализации булевых функций схемами из функциональных элементов [1]. Напомним определение схемы из функциональных элементов.

**Определение.** Пусть $B$ — множество булевых функций. *Схемой из функциональных элементов* в базисе $B$ называется ориентированный граф без ориентированных циклов, вершины которого подписаны. Каждая вершина входной степени 0 подписана некоторой переменной из алфавита переменных $\{x_1, \ldots, x_n, \ldots\}$. Каждая вершина входной степени $k$ подписана некоторой $k$-местной функцией из $B$. Одна из вершин также дополнительно выделена и называется *выходной* вершиной схемы.

Вершины, помеченные переменными, называются *входами* схемы, а вершины, помеченные функциями, называются *элементами*.

Для каждой вершины схемы по индукции естественным образом определяется булева функция, *реализуемая* этой вершиной. Говорят, что схема реализует функцию $f$, если ее выходной элемент реализует функцию $f$.

Пусть $S$ — схема. *Сложностью* схемы $S$ будем называть количество функциональных элементов в $S$. Сложность схемы $S$ обозначается как $L(S)$. Пусть $f$ — булева функция. *Сложностью реализации* функции $f$ в базисе $B$ будем называть число $L_B(f) = \min L(S)$, где минимум берется по всем схемам $S$ в базисе $B$, реализующим $f$. Если схема $S$ в базисе $B$ реализует булеву функцию $f$ и $L(S) = L_B(f)$, то схема $S$ называется *минимальной*.

Известно, что сложность случайной булевой функции от $n$ переменных экспоненциально велика с вероятностью, стремящейся к единице. Строго это утверждение сформулировано в следующей теореме.

**Теорема (О. Б Лупанов, [1])**. *Пусть $f(x_1, \ldots, x_n)$ — булева функция от $n$ переменных, $B$ — полный конечный базис. Тогда*

$$L_B(f) \leqslant \rho_B \frac{2^n}{n}(1 + o(1)),$$

*где $\rho_B$ — константа, зависящая только от базиса $B$. Кроме того, для любой положительной постоянной $\varepsilon$ среди всех функций от $n$ переменных доля функций $f$, таких, что $L_B(f) < (1-\varepsilon)\rho_B \frac{2^n}{n}$, стремится к нулю с ростом $n$.*

Возникает следующая задача: дать описание последовательности булевых функций $\{f_n\}$, такой, что сложность (в некотором базисе $B$) функций последовательности растет как можно более быстро с ростом $n$. Эта задача имеет тривиальное решение: если взять в качестве $f_n$ самую сложную функцию от $n$ переменных, для такой последовательности будет выполнена высокая нижняя оценка $L_B(f_n) \geqslant \rho_B \frac{2^n}{n}$. К сожалению, такое описание последовательности сложных функций не имеет большой ценности: остается неясным, какими свойствами (кроме высокой сложности) обладают функции последовательности. Единственный известный способ построения $n$-ой функции такой последовательности — полный перебор всех схем, который останавливается только после обнаружения схемы для каждой функции от $n$ переменных. Этот способ имеет крайне высокую трудоемкость, даже десятая функция последовательности не будет найдена на современном компьютере за приемлемое время.

Возможно ли явно задать последовательность булевых функций сравнимой сложности? До сих пор ответ на этот вопрос неизвестен. Пока для явно заданных последовательностей булевых функций до сих пор получены только линейные по $n$ нижние оценки сложности. Отметим, что понятие «явно заданная последовательность функций» нуждается в какой-то формализации. Часто говорят (см., например [2]), что последовательность $\{f_n\}$ явно задана, если язык, составленный из единичных наборов всех функций последовательности, принадлежит сложностному классу $NP$. Также можно встретить такое определение: последовательность $\{f_n\}$ явно задана, если существует алгоритм, строящий вектор значений $f_n$ за время, полиномиальное от размера этого вектора (т.е. $2^n$). Некоторые авторы [3, 4] воздерживаются от выбора строгого определения, предпочитая неформализованное, интуитивное представление о явных функциях.

Выбор базиса, в котором строятся схемы, не имеет большого значения для описания последовательности сложных функций. Легко доказать, что для любых двух полных конечных базисов $Б_1, Б_2$ существуют константы $C_1, C_2$, такие, что для любой функции $f$ верно, что $C_1 L_{Б_1}(f) \leqslant L_{Б_2}(f) \leqslant C_2 L_{Б_1}(f)$. Поэтому, к примеру, если сложность какой-то последовательности функций нелинейна в каком-то одном полном конечном базисе, эта сложность нелинейна во всех полных конечных базисах.

В данном обзоре описаны известные нижние оценки сложности для явно заданных функций в базисе $B_2$, состоящем из всех булевых функций двух переменных, а также в базисе $U_2$, состоящем из всех нелинейных функций двух переменных.

## 1. Базис $B_2$: определения и вспомогательные утверждения

Базис $B_2$ состоит из следующих функций:
1. Линейные функции двух переменных: $x \oplus y$ и $x \oplus y \oplus 1$.
2. Нелинейные функции двух переменных: $x\&y$, $x \vee y$, $\overline{x}\&y$, $\overline{x} \vee y$, $\overline{x\&y}$, $\overline{x \vee y}$.
3. Функции менее, чем двух переменных: $x$, $\overline{x}$, 1 и 0.

Элементы, соответствующие константам, будем считать одновходовыми. Двухвходовые элементы, подписанные линейными функциями, мы будем называть $\oplus$-элементами, а элементы, подписанные нелинейными функциями — &-элементами. Часто используется следующее свойство &-элементов: для любого входа любого &-элемента существует константа $c \in \{0, 1\}$, такая, что при подаче константы $c$ на этот вход элемент реализует константу вне зависимости от функции, подаваемой на другой вход. Будем называть такую константу *забивающей* для соответствующего входа элемента $E$. К примеру, для левого (т. е. соответствующего переменной $x$) входа элемента, реализующего функцию $\overline{x} \vee y$ забивающая константа — ноль.

Легко убедиться в том, что любую схему можно преобразовать, избавившись от всех одновходовых элементов так, что сложность схемы не увеличится, а функция, реализуемая схемой, не изменится.

**Утверждение 1**. *Пусть $S$ — схема в базисе $B_2$, реализующая функцию $f$ и содержащая одновходовой невыходной элемент $E$. Тогда существует схема $S'$, также реализующая $f$, такая, что $L(S) - L(S') = 1$.*

**Доказательство.** Пусть $v$ — вершина схемы, соединенная со входом $E$, а элементы $E_1, \ldots, E_k$ это все элементы, входы которых соединены с выходом $E$.

Если элементу $E$ приписана функция $x$ (т. е. $E$ — тождественный элемент, на его входе та же функция, что и на выходе), то, очевидно, можно удалить $E$ и соединить $v$ с освободившимися входами элементов $E_1, \ldots, E_k$.

Если элементу $E$ приписана функция $\overline{x}$, то $E$ можно удалить, соединить $v$ с освободившимися входами элементов $E_1, \ldots, E_k$, а функции, приписанные элементам $E_1, \ldots, E_k$ изменить так, чтобы реализуемые ими функции остались теми же, что в исходной схеме (например, если $E_1$ в исходной схеме была приписана функция $x \vee y$ и $E$ подавался на его вход, соответствующей переменной $x$, то в новой схеме элементу $E_1$ будет приписана функция $\overline{x} \vee y$).

Наконец, пусть $E$ реализует константу. Выберем $i \in \{1, \ldots, k\}$. Элемент $E_i$ реализует некоторую функцию одной переменной от функции, которая подается на вход $E_i$, не соединенный с выходом $E$ (если $E_i$ двухвходовой) или константу (если $E_i$ одновходовой). В обоих этих случаях $E_i$ можно отсоединить от выхода $E$ и заменить одновходовым элементом. После замены всех элементов $E_1, \ldots, E_k$ выход элемента $E$ больше не будет подаваться на входы элементов, и его можно будет удалить из схемы.

Из утверждения 1 следует, что минимальные схемы не содержат одновходовых элементов, а также двухвходовых элементов, оба входа которых соединены с одной и той же вершиной схемы. Как правило, мы будем молчаливо

предполагать, что из рассматриваемых схем удалены такие тривиальные элементы. Другое следствие утверждения 1 — возможность удалять элементы, на входы которых подана константа, — сформулировано ниже.

**Утверждение 2**. *Пусть $S$ — схема в базисе $B_2$, реализующая функцию $f$ и содержащая элемент $E$, на вход которого подана константа* 0 *или* 1. *Тогда существует схема $S'$, также реализующая $f$, такая, что $L(S) - L(S') = 1$.*

**Доказательство.** Заметим, что элемент $E$ либо является одновходовым либо может быть заменен на одновходовой, и применим утверждение 1.

Пусть $f$ — булева функция, $\sigma \in \{0, 1\}$. Мы будем использовать обозначение $f^\sigma$, обозначающее $f$, если $\sigma = 1$ и $\overline{f}$, если $\sigma = 0$.

## 2. Нижние оценки в базисе $B_2$

Для всех функций, существенно зависящих от $n$ переменных, выполнена следующая тривиальная нижняя оценка.

**Теорема 1**. *Пусть $f(x_1, \ldots, x_n)$ — функция, существенно зависящая от $n$ переменных. Тогда*

$$L_{B_2}(f) \geqslant n - 1.$$

**Доказательство.** Пусть $S$ — схема, реализующая $f$. Так как $f$ существенно зависит от всех переменных, каждый вход $S$ должен быть соединен с выходным элементом $S$ ориентированным путем. Следовательно, граф, соответствующий схеме, должен быть связным. Удалим все элементы из схемы, тогда она разделится на $n$ компонент связности. Далее, будем возвращать в схему элементы по одному. Добавление одного элемента будет уменьшать число компонент связности не более, чем на один, поэтому прежде, чем граф станет связным, будет добавлено не менее $n - 1$ элемента.

Первая нетривиальная нижняя оценка сложности схем в базисе $B_2$ получена Клоссом и Малышевым в 1965 году [5] (также этот результат был независимо повторен Шнорром в 1974 году [6]). Эта нижняя оценка доказана для функций из достаточно широкого класса $Q_{2,3}$.

**Определение.** Функция $f(x_1, \ldots, x_n)$ принадлежит классу $Q_{2,3}^{(n)}$, если выполнены условия:
1. Для любых $i$ и $j$ среди подфункций $f|_{\substack{x_i=0\\x_j=0}}$, $f|_{\substack{x_i=0\\x_j=1}}$, $f|_{\substack{x_i=1\\x_j=0}}$ и $f|_{\substack{x_i=1\\x_j=1}}$ найдется хотя бы три различных.
2. $\forall i\ \exists c \in \{0, 1\} : f|_{x_i=c} \in Q_{2,3}^{(n-1)}$ (при $n \geqslant 3$).

Как $Q_{2,3}$ будем обозначать объединение всех классов $Q_{2,3}^{(n)}$ при всех возможных $n$.

Пример явно заданной последовательности булевых функций из $Q_{2,3}$ несложно предъявить. Определим функции $MOD^n_{3,i}$ (здесь $i \in \{0,1,2\}$) следующим образом:

$$MOD^n_{3,i}(x_1,\ldots,x_n) = 1 \quad \Leftrightarrow \quad x_1 + \ldots + x_n = i \mod 3.$$

Для любого $i$ верно, что $MOD^n_{3,i} \in Q^{(n)}_{2,3}$. Действительно, при $n \geqslant 3$ подставляя различные константы вместо любых переменных функции $MOD^n_{3,i}$ можно получить три различных функции (это функции $MOD^{n-2}_{3,0}$, $MOD^{n-2}_{3,1}$ и $MOD^{n-2}_{3,2}$ от оставшихся переменных) и это свойство сохраняется для всех подфункций $MOD^n_{3,i}$, зависящих хотя бы от трех переменных (так как все такие подфункции имеют вид $MOD^k_{3,i}$ для некоторого $k \geqslant 3$).

Следующая теорема показывает, что функции из класса $Q_{2,3}$ требуют достаточно больших схем.

**Теорема 2** [5,6]. *Если* $f_n \in Q^{(n)}_{2,3}$, *то* $L_{B_2}(f_n) \geqslant 2n-4$.

**Доказательство.** Пусть $S_n$ — минимальная схема, реализующая функцию $f_n$ из класса $Q^{(n)}_{2,3}$. Выберем в этой схеме элемент $E$, оба входа которого соединены со входами схемы. Такой элемент существует так как схема $S_n$ минимальна (и, следовательно, не содержит одновходовых элементов) и не содержит циклов; этот элемент можно найти, выбрав произвольный элемент схемы и «поднимаясь» по схеме до тех пор, пока это возможно.

Пусть $x_1$ и $x_2$ — входы схемы, соединенные со входами $E$. Покажем, что степень хотя бы одного из входов $x_1$, $x_2$ превосходит один. Предположим обратное. Пусть элемент $E$ реализует функцию $x_1 \circ x_2$ (здесь знаком «$\circ$» обозначена двухместная функция, приписанная элементу $E$). Так как оба входа $x_1$ и $x_2$ не соединены со входами элементов, отличных от $E$, функция $f_n$ зависит лишь от $x_1 \circ x_2$, а не от $x_1$ и $x_2$ по отдельности: существует такая функция $g$, что $f_n(x_1,x_2,\ldots,x_n) = g(x_1 \circ x_2, x_3, \ldots, x_n)$. Функция $x_1 \circ x_2$ принимает не более двух значений, поэтому среди функций $f_n|_{\substack{x_1=0\\x_2=0}}$, $f_n|_{\substack{x_1=0\\x_2=1}}$, $f_n|_{\substack{x_1=1\\x_2=0}}$ и $f_n|_{\substack{x_1=1\\x_2=1}}$ не более двух различных (это функции $g(0,x_3,\ldots,x_n)$ и $g(1,x_3,\ldots,x_n)$). Это противоречит тому, что $f_n$ лежит в классе $Q^{(n)}_{2,3}$.

Без ограничения общности будем считать, что степень $x_1$ больше или равна двум. Подадим на вход $x_1$ константу $c$ такую, что $f_n|_{x_1=c} \in Q^{(n-1)}_{2,3}$ (такая константа существует по определению класса $Q_{2,3}$). После подачи константы на вход в схеме появятся два элемента, на входы которых поданы константы. Удалим эти два элемента согласно утверждению 2, а также удалим из схемы все одновходовые элементы (если они появились) согласно утверждению 1. Полученная схема $S_{n-1}$ реализует функцию $f_n|_{x_1=c}$ из класса $Q^{(n-1)}_{2,3}$, причем $L(S_n) - L(S_{n-1}) \geqslant 2$.

Со схемой $S_{n-1}$ проведем аналогичное преобразование: удалим из нее не менее двух элементов, получив схему, реализующую функцию из $Q^{(n-2)}_{2,3}$. Про-

цесс удаления элементов можно повторить $n-2$ раза (столько, сколько констант можно подать вместо переменных функции из $Q^{(n)}_{2,3}$, так, что перед подаче каждой константы для подфункции будет выполнено свойство 1 из определения класса $Q_{2,3}$. Следовательно, в течение процесса удаления элементов будет удалено не менее $2n-4$ элементов, и, значит $L(S_n) \geqslant 2n-4$.

Подход, использованный при доказательстве теоремы 2, носит название «метод забивающих констант». Опишем типичный сценарий применения этого метода. Пусть задана последовательность функций $\{f_n\}$, для которой требуется доказать нижнюю оценку сложности. Вложим каждую функцию $f_n$ в какой-нибудь класс функций $F_n$ так, чтобы для классов $F_n$ было возможно доказать следующее утверждение: любую схему, реализующую функцию из $F_k$ можно превратить в схему для некоторой функции из $F_{k-1}$, удалив из нее не менее $d$ элементов. Такое утверждение влечет нижнюю оценку для функции $f_n$ вида $L(f_n) \geqslant dn - C$, где $C$ — некоторая константа. Действительно, из любой схемы, реализующей $f_n$, можно $n$ раз удалить по $d$ элементов, на каждом шагу получая схему для функции из класса $F_k$ для какого-то $k$. Следовательно, число элементов в любой схеме для $f_n$ превосходит $nd$. Отметим, что как правило утверждение о преобразовании схем удается доказать не для всех $k$, а для всех $k$, превосходящих некоторое фиксированное $k_0$. Это и уменьшает нижнюю оценку на константу.

Классы $\{F_n\}$ как правило выбираются так, что $F_n$ состоит из функций $n$ переменных, а преобразование схемы, строящее из схемы для функции из $F_n$ схему для функции из $F_{n-1}$ с удалением $d$ элементов, обычно заключается в подаче константы на один из входов схемы с последующим удалением элементов, ставших избыточными (например, с использованием утверждений 1 или 2). Все известные доказательства нижних оценок сложности схем в конечных базисах (за редчайшими исключениями) используют метод забивающих констант или его обобщения, нередко этот метод является основной или единственной идеей доказательства.

На протяжении долгого времени теорема 2 оставалась единственной нижней оценкой в базисе $B_2$ с достаточно компактным доказательством. Лишь в 2010 году Кожевников и Куликов предложили [7] нижнюю оценку с минорантой $2.33n$, имеющую простое доказательство. Для изложения этой оценки необходимо напомнить понятия полинома Жегалкина и мультипликативной сложности.

**Определение.** Пусть $f(x_1, \ldots, x_n)$ — булева функция. *Полином Жегалкина* для функции $f$ — представление $f$ в виде

$$f(x_1, \ldots, x_n) = \bigoplus_{\substack{k \in \{1,\ldots,n\},\\ \{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\}}} c_{i_1,\ldots,i_k} \cdot x_{i_1} \ldots x_{i_k} \oplus c_0,$$

где коэффициенты $c_{i_1,\ldots,i_k}$ и $c_0$ выбираются из множества $\{0,1\}$. Известно [8], что набор коэффициентов полинома определяется по булевой функции одно-

значно. *Степенью* булевой функции $f$ называется наибольшая длина конъюнкции, входящей в ее полином с единичным коэффициентом. Степень функции $f$ обозначается как $\deg f$.

**Определение.** *Мультипликативной сложностью* схемы $S$ в базисе $B_2$ называется количество &-элементов в $S$. *Мультипликативной сложностью* функции $f$ называется минимальное количество &-элементов в схеме в базисе $B_2$, реализующей $f$. Мультипликативная сложность функции $f$ обозначается как $M(f)$.

Мультипликативная сложность функции и ее степень связаны.

**Утверждение 3** [9]. *Пусть $f$ — булева функция. Тогда $M(f) \geqslant \deg f - 1$.*

Интуитивно утверждение 3 кажется естественным и даже очевидным: для того, чтобы схема реализовывала функцию степени $k$, она должна содержать не менее $k-1$ умножения. Строгое доказательство утверждения можно найти в [9].

Лучшая нижняя оценка мультипликативной сложности функции $n$ переменных, которая может быть получена из утверждения 3, имеет миноранту $n-1$ (для функции степени $n$). Степенная нижняя оценка является далеко не оптимальной для почти всех булевых функций: известно [10], что мультипликативная сложность почти всех функций $n$ переменных асимптотически равна $2^{\frac{n}{2}}$. Тем не менее, до сих пор не построено явно заданной последовательности функций, допускающей нижнюю оценку мультипликативной сложности, большую $n-1$.

Определим множество функций $R_{2,3}$.

**Определение.** Функция $f(x_1, \ldots, x_n)$ принадлежит классу $R_{2,3}^{(n)}$, если выполнены условия:
1. Для любых $i$ и $j$ среди подфункций $f|_{\substack{x_i=0\\x_j=0}}$, $f|_{\substack{x_i=0\\x_j=1}}$, $f|_{\substack{x_i=1\\x_j=0}}$ и $f|_{\substack{x_i=1\\x_j=1}}$ найдется хотя бы три различных.
2. $\forall i\ \forall c \in \{0,1\} : f|_{x_i=c} \in R_{2,3}^{(n-1)}$ (при $n \geqslant 3$).

Очевидно, $R_{2,3} \subset Q_{2,3}$. Следующая теорема улучшает нижнюю оценку теоремы 2 для функций высокой степени из $R_{2,3}$.

**Теорема 3** [7]. *Пусть $f_n(x_1, \ldots, x_n)$ — последовательность булевых функций, $f_n \in R_{2,3}^n$ и $\deg f_n = n - C$, где $C$ — константа. Тогда*

$$L_{B_2}(f_n) \geqslant \frac{7}{3}n + o(n).$$

**Доказательство.** Для схемы $S$ в базисе $B_2$ определим новую меру сложности $\mu(S)$ следующим образом:

$$\mu(S) = 3M(S) + 2N(S),$$

где $M(S)$ — число &-элементов в схеме, а $N(S)$ — число $\oplus$-элементов в схеме. Используя метод забивающих констант, докажем, что для любой схемы $S$, реализующей функцию из $R_{2,3}^{(n)}$, верно, что $\mu(S) \geqslant 6n - 12$. Для этого проверим, что из любой схемы, реализующей функцию из $R_{2,3}^{(n)}$ (при $n \geqslant 3$), можно удалить несколько элементов так, что новая схема будет реализовывать функцию из $R_{2,3}^{(n-1)}$, а значение меры $\mu$ уменьшится не менее, чем на шесть.

Пусть $S$ — схема, реализующая функцию $f$ из $R_{2,3}^{(n)}$. Удалим из нее все одновходовые элементы согласно утверждению 1 (значение $\mu(S)$ при этом, очевидно, не увеличится). Далее, пусть $E_2$ — двухвходовой элемент $S$, оба входа которого соединены со входами схемы $x_i$ и $x_j$. Из доказательства теоремы 2 следует, что степень одного из этих входов больше одного. Без ограничения общности считаем, что это вход $x_i$, пусть $E_2$ — элемент, отличный от $E_1$, вход которого соединен с входом $x_i$. Рассмотрим следующие случаи.

1. Один из элементов $E_1$, $E_2$ (без ограничения общности, элемент $E_1$) является &-элементом и выход $E_1$ соединен со входом элемента $E_3$, отличного от $E_2$ (см. рис. 1,а). Подадим на вход $x_i$ константу, забивающую элемент $E_1$ (согласно определению класса $R_{2,3}$ схема после подачи константы будет реализовывать функцию из $R_{2,3}^{(n-1)}$). После этого элемент $E_1$ будет реализовывать константу, и, следовательно, элементы $E_1$, $E_2$ и $E_3$ можно удалить согласно утверждению 2. Удаление трех элементов уменьшает значение меры сложности $\mu$ не менее, чем на шесть.

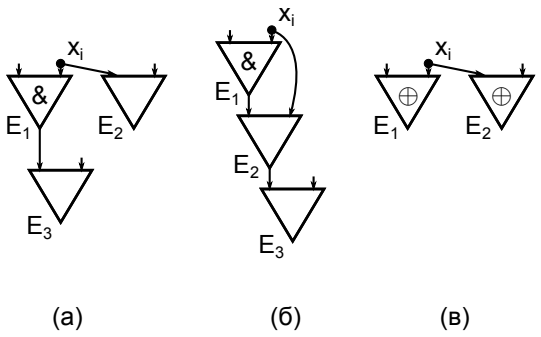


Рис. 1

2. Один из элементов $E_1$, $E_2$ (без ограничения общности, элемент $E_1$) является &-элементом и выход $E_1$ соединен лишь со входом элемента $E_2$ (см. рис. 1, б). Пусть $E_3$ — элемент, вход которого соединен со выходом элемента $E_2$ (элемент $E_2$ не является выходным т. к. функция из $P_{2,3}^{(n)}$ не может иметь вид $x\varphi$, где $x$ — переменная, $\varphi$ — булева функция, $n \geqslant 3$). Подадим на вход $x_i$ константу, забивающую элемент $E_1$. Элементы $E_1$ и $E_2$ будут реализовывать константы, поэтому элементы $E_1$, $E_2$ и $E_3$ можно удалить с использованием

утверждения 2.

3. Оба элемента $E_1, E_2$ являются $\oplus$-элементами (см. рис 1, в). Подав любую константу на вход $x_i$, удалим оба этих элемента. Удаление двух $\oplus$-элементов уменьшает значение меры $\mu$ на шесть.

Итак, мы доказали, что для любой схемы $S$, реализующей функцию из $R^{(n)}_{2,3}$, верно, что $\mu(S) = 2M(S) + 3N(S) \geqslant 6n - 12$. Кроме того, если эта схема реализует функцию степени $n - C$, из утверждения 3 следует, что $M(S) \geqslant n - C - 1$. Складывая два неравенства, получаем $3L(S) = 3(M(S) + N(S)) \geqslant 7n - C - 13$, откуда $L(S) \geqslant \frac{7}{3}n + o(n)$.

Доказательство теоремы 3 демонстрирует типичную особенность метода забивающих констант: для доказательства возможности удаления нескольких элементов необходимо рассматривать несколько случаев взаимного расположения элементов, находящихся «наверху» схемы. В доказательстве теоремы 3 таких случаев всего три, в более сложных доказательствах их число может достигать несколько десятков.

Пример явно заданной последовательности функций, удовлетворяющих условиям теоремы 3 предъявить легко: как и для теоремы 2 можно взять функции $MOD^n_{3,0}$.

**Утверждение 4**. *Для любого* $i \in \{0, 1, 2\}$, $n \geqslant 3$ *верно, что* $MOD^n_{3,i} \in R^{(n)}_{2,3}$ *и* $\deg MOD^n_{3,i} \geqslant n - 1$

**Доказательство.** Принадлежность функций $MOD^n_{3,i}$ классу $R^{(n)}_{2,3}$ обосновывается так же, как и принадлежность классу $Q^{(n)}_{2,3}$. Докажем, что эти функции имеют высокую степень.

Известно (см. [8], задача 10 к главе 3), что функция $n$ переменных имеет степень $n$ тогда и только тогда, когда ее вес нечетен (вес булевой функции $f$ — число наборов, на которых $f$ принимает значение 1; обозначение для веса — $\mathrm{wt}\, f$). Заметим, что среди функций $MOD^n_{3,0}, MOD^n_{3,1}, MOD^n_{3,2}$ есть ровно две функции нечетного веса. Для $n = 3$ это проверяется непосредственно, а для больших $n$ доказывается по индукциии с учетом равенства $\mathrm{wt}\, MOD^n_{3,i} = \mathrm{wt}\, MOD^{n-1}_{3,i} + \mathrm{wt}\, MOD^{n-1}_{3,i-1}$ (здесь $i - 1$ берется по модулю три). Значит, среди функций $MOD^n_{3,0}, MOD^n_{3,1}, MOD^n_{3,2}$ две имеют степень $n$, а третья имеет подфункцию $n-1$ переменной степени $n-1$ (и, следовательно, имеет степень $n - 1$).

Высокие нижние оценки сложности доказаны для различных обобщений функции выбора.

**Определение.** Пусть $n = 2^k$. *Функцией выбора* называется следующая функция $n + \log n$ переменных:

$$SA_n(a_1, \ldots, a_{\log n}, x_1, \ldots, x_n) = x_{|\tilde{a}|}$$

(здесь $|\tilde{a}|$ — число, двоичной записью которого является набор $(a_1, \ldots, a_{\log n})$). Переменные $a_1, \ldots, a_{\log n}$ называются *адресными* переменными функции $SA_n$, а переменные $x_1, \ldots, x_n$ — *информационными.*

Известно, что сложность функции $SA_n$ асимптотически равна $2n$. Нижняя оценка доказана в [11], а верхняя — в [12]. Таким образом, нижних оценок сильнее, чем нижняя оценка теоремы 2, для функции выбора не получить. Более сильную нижнюю оценку получил Пауль в 1974 году для функции, «составленной» из двух функций выбора, выходы которых поданы на вход некоторой функции трех переменных.

**Теорема 4** [11]. *Пусть $n = 2^k$, функция $SA'_n$ от $n + 2\log n + 1$ переменной определена следующим образом:*

$$SA'_n(a_1, \ldots, a_{\log n}, b_1, \ldots, b_{\log n}, q, x_1, \ldots, x_n) = \begin{cases} x_{|\tilde{a}|} \oplus x_{|\tilde{b}|}, & \text{если} \quad q = 0 \\ x_{|\tilde{a}|} \& x_{|\tilde{b}|}, & \text{если} \quad q = 1 \end{cases}$$

*Тогда $L_{B_2}(SA'_n) \geqslant 2.5n + o(n)$.*

Опишем, как проходит доказательство теоремы 4. Пусть $S$ — схема, реализующая $SA'_n$. На первом этапе доказательства на информационные входы схемы подаются константы, и из схемы удаляются элементы (по три элемента на каждый забитый вход). К сожалению подать так константы на все информационные входы (и получить нижнюю оценку сложности $3n$) не удается: возможна ситуация, когда удаление трех элементов невозможно. Для обработки таких ситуаций используется вторая часть доказательства: при помощи теоретико-графовых рассуждений доказывается, что в схеме, из которой нельзя удалить три элемента, подав константу, содержится не менее $2.5k$ элементов, где $k$ — число незабитых информационных входов.

Наиболее интересна вторая часть доказательства; это один из редких примеров доказательства нижних оценок сложности схем, не использующий метод забивающих констант. В нем из рассматриваемой схемы не «отрезаются» маленькие «кусочки» из нескольких элементов, а сразу доказывается, что в схеме должно быть много элементов. Чтобы дать представление об использованном подходе, докажем сильно ослабленную версию теоремы 4.

**Теорема 5** [11]. $L_{B_2}(SA'_n) \geqslant 2n - 2$.

**Доказательство.** Отметим, что теорему 5 легко доказать методом забивающих констант или вывести из нижней оценки $L_{B_2}(SA_n) \geqslant 2n-2$, пользуясь равенством $SA'_n(\tilde{a}, \tilde{a}, 1, \tilde{x}) = SA_n(\tilde{a}, \tilde{x})$. Здесь приводится другое, неиндуктивное доказательство этой теоремы.

Будем называть *ветвящейся* вершиной схемы вершину схемы исходящей степени большей единицы. Для любой минимальной схемы $S$, реализующей

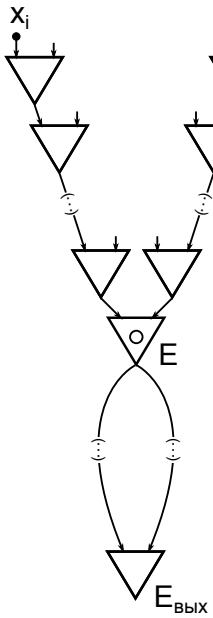


Рис. 2

функцию, существенно зависящую от $n$ переменных и содержащую $m$ ветвящихся вершин, верно, что

$$L(S) \geqslant n + m - 1. \tag{1}$$

Доказательство этого факта аналогично доказательству теоремы 1. Удалим из схемы все элементы, а затем будем добавлять их обратно по одному. На каждом шаге будем считать число вершин с не подключенными никуда выходами (с учетом кратности, т. е. вершину, исходящая степень которой в исходной степени равна двум мы считаем два раза). Изначально число неподключенных выходов превосходит $n + s$, где $s$ — число ветвящихся входов в схеме (каждый неветвящийся вход мы считаем один раз, каждый неветвящийся — не менее двух раз), после добавления всех элементов это число становится равным одному (т. к. схема минимальна, в ней нет «висячих» элементов). Добавление неветвящегося элемента уменьшает число неподключенных выходов на один, а добавление ветвящегося элемента не уменьшает это число. Поэтому в схему должно быть добавлено не менее $n + s - 1$ неветвящегося элемента. Число ветвящихся элементов в схеме равно $m - s$, следовательно общее число элементов не меньше $n + m - 1$.

Пусть $S$ — минимальная схема, реализующая $SA'_n$. Пусть $x_i$ и $x_j$ — два входа этой схемы (соответствующие информационным переменным). Выберем в

схеме два ориентированных пути так, чтобы первый путь соединял $x_i$ и выходной элемент, а второй — $x_j$ и выходной элемент. Пусть $E$ — самый близкий к входам схемы элемент, общий для обоих путей (см. рис 2). Докажем, что хотя бы один из путей содержит ветвящийся элемент, находящийся выше (т. е. ближе к входам) элемента $E$.

Предположим обратное: ни один из двух путей не ветвится выше $E$. Пусть «$\circ$» — двухместная функция, приписанная элементу $E$. Подадим произвольные константы на все входы схемы кроме $x_i$ и $x_j$. Тогда все элементы схемы будут реализовывать какие-то функции переменных $x_i$ и $x_j$, причем элементы первого пути (начинающегося с $x_i$) выше $E$ будут реализовывать одну из функций $x_i$, $\overline{x_i}$, 0, 1, а элементы второго пути выше $E$ — одну из функций $x_j$, $\overline{x_j}$, 0, 1. Элемент $E$ будет реализовывать функцию вида $x_i^\alpha \circ x_j^\beta$ или функцию одной переменной. Поскольку оба рассматриваемых пути не ветвятся выше $E$ значение на выходе схемы зависит только от значения на выходе $E$, а не от значений $x_i$ и $x_j$ по отдельности, поэтому функция на выходе схемы также имеет вид $(x_i^\alpha \circ x_j^\beta)^\gamma$ или является функцией одной переменной. Следовательно, если $\circ$ — линейная функция, то на выходе схемы не получить $x\&y$ ни при каком выборе констант, подаваемых на остальные входы, а если $\circ$ — нелинейная функция, то нельзя получить $x \oplus y$. Это противоречит определению $SA'_n$.

Далее, докажем, что в схеме есть не менее $n-1$ ветвящейся вершины. Выберем $n$ путей в схеме так, чтобы $i$-ый путь соединял вход $x_i$ с выходным элементом. Согласно доказанному выше во всех этих путях (кроме, быть может одного) есть ветвящийся элемент. Действительно, пусть в $i$-ом пути нет ветвящейся вершины. Выберем произвольное $j$, не равное $i$. Пути с номерами $i$ и $j$ пересекаются, значит один из них должен содержать ветвящуюся вершину выше элемента, в котором они пересекаются. Так как $i$-ый путь не содержит ветвящихся вершин, ветвящуюся вершину содержит $j$-ый путь. Таким образом, доказано, что все пути, кроме $i$-ого содержат ветвящуюся вершину.

Без ограничения общности считаем, что ветвящуюся вершину содержат все пути кроме, быть может $n$-ого. Пусть $v_1, \ldots, v_{n-1}$ — вершины схемы, такие, что $v_i$ — самая высокая ветвящаяся вершина на $i$-ом пути. Все эти вершины различны: если бы $v_i$ и $v_j$ совпали, то на $i$-ом и $j$-ом путях не было бы ветвящихся элементов выше вершины $v_i$, в которой эти два путя пересекаются, что невозможно.

Итак, мы выделили в схеме $n-1$ ветвящуюся вершину. Значит, из соотношения (1) следует, что $L(S) \geqslant 2n-2$.

Неясно, можно ли улучшить нижнюю оценку теоремы 4. В работе [11] сложность функции $SA'_n$ оценивается сверху следующим образом: $L_{B_2}(SA'_n) \leqslant 6n + o(n)$. Используя методы работы [12], легко получить более сильную верхнюю оценку $L_{B_2}(SA'_n) \leqslant 4n + o(n)$. Более компактные схемы для $SA'_n$ автору этого обзора неизвестны.

Обобщая методы, использованные при доказательстве теоремы 4, в 1981 году Блюм получил [13] нижнюю оценку $3n$ для еще более сложной функции, также сконструированной из нескольких функций выбора.

**Теорема 6** [13]. *Пусть* $n = 2^k$ *и* $SA''_n$ *— булева функция* $n + 3\log n + 3$ *переменных, определяемая следующим образом*:

$$SA''_n(\tilde{a}, \tilde{b}, \tilde{c}, p, q, r, x_1, \ldots, x_n) = q(x_{|\tilde{a}|}x_{|\tilde{b}|} \vee px_{|\tilde{b}|}x^r_{|\tilde{c}|}) \vee \overline{q}(x_{|\tilde{a}|} \oplus x_{|\tilde{b}|})$$

(*здесь* $\tilde{a}$, $\tilde{b}$ *и* $\tilde{c}$ *— наборы из* $\log n$ *переменных*). *Тогда верно, что* $L_{B_2}(SA''_n) \geqslant \geqslant 3n + o(n)$.

На протяжении более 30 лет теорема 6 была единственной доказанной нижней оценкой сложности явно заданной последовательности булевых функций с минорантой, большей или равной $3n$. Совсем недавно более сильные оценки были получены для класса функций, называемых *аффинными дисперсерами*.

**Определение.** Подмножество множества $\{0,1\}^n$ называется *линейным подпространством*, если оно замкнуто относительно покомпонентного сложения по модулю два. Размерность линейного подпространства — максимальное число линейно независимых наборов, которые можно выбрать из подпространства. *Аффинным подпространством* размерности $d$ называется множество вида $\{\tilde{a} + \tilde{x} | \tilde{x} \in L\}$, где $\tilde{a} \in \{0,1\}^n$, а $L$ — линейное подпространство $\{0,1\}^n$ размерности $d$.

**Определение.** Булева функция $f(x_1, \ldots, x_n)$ называется *аффинным дисперсером* размерности $d$, если она не постоянна на любом афинном подпространстве $\{0,1\}^n$ размерности, большей или равной $d$.

Пользуясь вероятностным методом, легко доказать, что почти все булевы функции $n$ переменных являются аффинными дисперсерами размерности $2\log n$. Однако, вероятностный метод не позволяет предъявить явно заданные функции, являющиеся аффинными дисперсерами небольшой размерности. Явно заданные аффинные дисперсеры пока построены лишь для существенно более высоких, чем $2\log n$ размерностей.

Можно проверить, что функция $IP(x_1, \ldots, x_{n/2}, y_1, \ldots y_{n/2}) = x_1y_1 \oplus \ldots \ldots \oplus x_{n/2}y_{n/2}$, определенная только для четных $n$ является аффинным дисперсером размерности $n/2 + 1$. Более того, таким дисперсером будет любая бент-функция $n$ переменных.

Явно заданные дисперсеры меньших размерностей построить значительно сложнее. В работе [14] построена явно заданная функция $n$ переменных, являющаяся дисперсером размерности $\Theta(n^{\frac{4}{5}})$. Приведем описание такой функции.

Пусть задано $n$. Выберем $m$ — наименьшее простое число, не превосходящее $2n^{4/5}$, а также $r = \lceil m/n \rceil$ и $t = \lceil \sqrt{r} \rceil$. Будем интерпретировать наборы из $\{0,1\}^n$ как элементы $\mathbb{F}^r_{2^m}$, где $\mathbb{F}_{2^m}$ — конечное поле из $2^m$ элементов (т. е.

набор их $n$ единиц делится на $r$ блоков по $m$ единиц в каждом, и каждый блок интерпретируется как элемент $\mathbb{F}_{2^m}$). Определим функцию

$$f(x_1,\dots,x_r) = \operatorname{Tr}\operatorname{Sym}_r^t(x_1^3, x_2^7, \dots, x_r^{2^{r+1}-1}),$$

где $x_1,\dots,x_r$ — элементы $\mathbb{F}_{2^m}$, $\operatorname{Sym}_r^t(y_1,\dots,y_r) = \sum\limits_{1\leqslant i_1<\dots<i_t\leqslant r} y_{i_1}\dots y_{i_r}$ — $t$-ый симметрический многочлен, $\operatorname{Tr} y = y + y^2 + y^4 + \dots + y^{2^{m-1}}$ — след элемента конечного поля $\mathbb{F}_{2^m}$, все операции сложения и умножения понимаются как операции $\mathbb{F}_{2^m}$. В [14] доказано, что $f$ (понимаемая как булева функция, действующая на $\{0,1\}^n$) является аффинным дисперсером размерности $\Theta(n^{\frac{4}{5}})$.

Так как степень элемента конечного поля и симметрические многочлены вычислимы за полиномиальное время, так определенная функция удовлетворяет распространенным определениям явной заданности. Также разумно согласится, что приведенное выше описание не менее конкретно чем, скажем, определение функции $SA''_n$ из теоремы 6.

Функция из работы [14] не является явным аффинным дисперсером с самыми лучшими параметрами: в работе [15] построен дисперсер размерности $2^{\log^{0.9} n}$.

В 2011 году Деменков и Куликов доказали следующую теорему.

**Теорема 7** [16]. *Пусть булева функция $f(x_1,\dots,x_n)$ является аффинным дисперсером размерности $o(n)$. Тогда $L_{B_2}(f_n) \geqslant 3n - o(n)$.*

Доказательство теоремы 7 существенно проще, чем доказательство теоремы 6, в которой нижняя оценка $3n$ доказывается для другой функции. Впрочем, необходимо подчеркнуть, что теорема 7 опирается на крайне нетривиально доказываемый факт — существование явно заданных аффинных дисперсеров размерности $o(n)$. Без этого факта теорема не давала бы оценку для последовательности явно заданных функций.

В 2015 году нижняя оценка теоремы 7 была улучшена.

**Теорема 8** [17]. *Пусть булева функция $f(x_1,\dots,x_n)$ является аффинным дисперсером размерности $o(n)$. Тогда $L_{B_2}(f_n) \geqslant (3 + \frac{1}{86})n - o(n)$.*

Теорема 8 является первой оценкой сложности явно заданной функции в базисе $B_2$ с минорантой, большей $3n$, и самой высокой нижней оценкой сложности на данный момент. В целом ее доказательство является применением метода забивающих констант, при этом оно использует целый ряд нетривиальных приемов.

В качестве промежуточного объекта доказательство теоремы 8 использует схемы из функциональных элементов с циклами. Опишем, как определяются функции, реализуемые элементами в схеме с циклами. Пусть дана схема с входами $x_1,\dots,x_n$ и элементами $E_1,\dots,E_k$, быть может, содержащая ориентированные циклы, запрещенные обычным определением схем. Такой схеме

можно сопоставить систему $k$ уравнений с переменными $E_1, \ldots, E_k, x_1, \ldots, x_n$ (например, конъюнктору $E_1$, на входы которого подаются вход схемы $x_3$ и выход элемента $E_2$ сопоставляется уравнение $E_1 = x_3 \& E_2$). Если при подстановке в систему произвольных значений вместо переменных $x_1, \ldots, x_n$ значения переменных $E_1, \ldots, E_n$ определяются однозначно, то такая схема считается правильной; значение, реализуемое элементом $E_i$ на наборе $\sigma_1, \ldots, \sigma_n$ определяется как значение переменной $E_i$ в системе при подставленных значениях $\sigma_1, \ldots, \sigma_n$ вместо $x_1, \ldots, x_n$. Если же при каких-то значениях переменных $x_1, \ldots, x_n$ решение системы не определено или не единственно, схема считается неправильной и не рассматривается. Заметим, что в работе [17] рассматриваются лишь схемы с циклами, находящимися лишь в линейной части схемы (состоящей из $\oplus$-элементов).

При «обрезании» схемы (т. е. удалении блоков из нескольких элементов) методом забивающих констант используются не только константные подстановки (вида $x_i = c$), но и линейные (вида $x_i = \bigoplus_{j \in J} x_j \oplus c$) и квадратичные (вида $x_i = x_j^{\alpha} \& x_k^{\beta}$). Применение подстановки $x_i = \varphi(x_1, \ldots, x_n)$ к схеме $S$ означает, что схема $S$ перестраивается таким образом, что ее выходное значение не изменяется на подмножестве наборов $\{0,1\}^n$, для которых верно, что $x_i = \varphi(x_1, \ldots, x_n)$. В работе [17] проверяется, что к любой схеме, реализующий аффинный дисперсер от $n$ переменных размерности $o(n)$ можно применить $n - o(n)$ подстановок (к различным переменным), на каждом шаге удаляя несколько элементов (и меняя другие параметры схемы).

## 3. Нижние оценки в базисе $U_2$

Более высокие нижние оценки сложности можно получить для схем в базисе $U_2$, состоящего лишь из &-элементов. Уже для линейной функции от $n$ переменных применением метода забивающих констант легко получить нижнюю оценку с минорантой $3n$.

**Теорема 9** [6]. *Пусть* $l(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$. *Тогда* $L_{U_2}(l_n) = 3n - 3$.

**Доказательство.** Верхнюю оценку легко получить с учетом того, что схему из $3n-3$ элементов для $l_n$ можно составить из $n-1$ трехэлементного блока с двумя входами, реализующего сумму по модулю два функций, подаваемых на входы. Пример такого блока изображен на рис. 3. Два верхних элемента в схеме на рисунке реализуют функции $\overline{x}\&y$ и $x\&\overline{y}$.

Чтобы получить нижнюю оценку, докажем, что из любой схемы в базисе $U_2$, реализующей $l_n$ или $\overline{l_n}$, можно удалить три элемента, получив схему, реализующую $l_{n-1}$ или $\overline{l}_{n-1}$. После того, как это будет доказано, нижняя оценка теоремы 9 может быть получена по индукции.

Пусть $S$ — схема, реализующая $l_n$. Удалим из нее все элементы, на входы которых подаются константы согласно утверждению 2. Ни один из входов $S$ не соединен со входом единственного элемента. Действительно, пусть

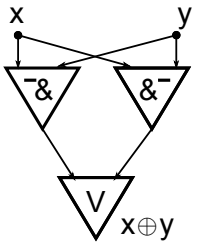


Рис. 3

$x_i$ — такой вход. Пусть единственный элемент, со входом которого соединен этот вход — элемент $E$. Пусть на второй вход элемента подается функция $\varphi$. Так как схема по определению не содержит циклов, функция $\varphi$ не зависит от $x_i$. Поэтому мы можем подобрать значения остальных переменных (кроме переменной $x_i$), такие, что функция $\varphi$ обращается в константу, забивающую элемент $E$ (напомним, мы рассматриваем базис $U_2$, все элементы которого — &-элементы). После этого выходная функция схемы перестанет зависеть от $x_i$. Но для линейной функции это невозможно: какие бы константы мы не подставили вместо части переменных линейной функции полученная подфункция будет зависеть от всех оставшихся.

Пусть $x_i$ — произвольный вход $S$. По доказанному выше он соединен со входами хотя бы двух элементов, скажем элементов $E_1$ и $E_2$. Подадим на вход $x_i$ константу, забивающую элемент $E_1$. После этого схема будет реализовывать $l_{n-1}$ или $\overline{l_n}$. В зависимости от того, существует ли элемент $E_3$, вход которого соединен с выходом $E_1$ мы можем удалить три элемента, пользуясь утверждением 2. Это элементы $E_1$, $E_2$ и $E_3$ или элементы $E_1$, $E_2$ и элемент, вход которого соединен с выходом $E_2$ (см. рис. 4).

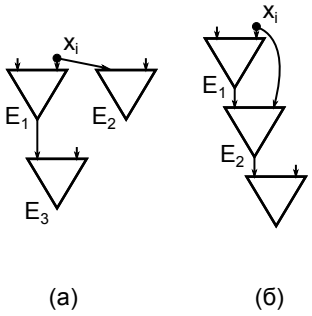


Рис. 4

Если провести перебор различных конфигураций элементов, которые могут быть в верхней части схемы, более аккуратно, с помощью метода забива-

ющих констант можно доказать следующее утверждение, усиливающее теорему 9.

**Утверждение 5** [18]. *Всякая минимальная схема в базисе $U_2$, реализующая $l_n$ или $\overline{l_n}$ состоит из $n-1$ трехэлементного блока с двумя входами, реализующего сумму по модулю два или отрицание суммы по модулю два функций, подаваемых на его входы (пример такого блока изображен на рис. 4). Более точно, всякая минимальная схема для $l_n$ или $\overline{l_n}$ является двоичным деревом, в листьях которого расположены входы схемы, а во внутренних вершинах — трехэлементные блоки.*

Аналогичные утверждения доказаны и для ряда других базисов [19, 20].

Более высокая нижняя нижняя оценка была доказана Цвиком в 1991 году.

**Теорема 10** [21]. $L_{U_2}(MOD^n_{3,0}) \geqslant 4n - 9$.

Отметим, что в работе [21] нижняя оценка $4n$ доказана для более широкого класса симметрических функций. Доказательство основано на методе забивающих констант.

Самая высокая на настоящее время нижняя оценка имеет миноранту $5n$. Она доказана для класса булевых функций, называемых сильно-2-зависимыми.

**Определение.** Булева функция $f$ называется *2-зависимой*, если для любых $i$ и $j$ подфункции $f|_{\substack{x_i=0\\x_j=0}}$, $f|_{\substack{x_i=0\\x_j=1}}$, $f|_{\substack{x_i=1\\x_j=0}}$ и $f|_{\substack{x_i=1\\x_j=1}}$ попарно различны.
Булева функция $f(x_1, \ldots, x_n)$ называется $(n,k)$-*сильно-2-зависимой*, если любая подфункция $f$, зависящая от $k$ и более переменных, является 2-зависимой.

Важно отметить сходство этого определения с определением класса $Q_{2,3}$. Построить явно заданную $(n, o(n))$-сильно-2-зависимую функцию непросто. Впервые это было сделано в работе [22] с использованием нетривиального утверждения о суммах подмножеств конечного поля $\mathbb{F}_p$. Для таких функций в 2002 году была доказана следующая нижняя оценка.

**Теорема 11** [23]. *Пусть $f$ является $(n, o(n))$-сильно-2-зависимой. Тогда $L_{U_2}(f) \geqslant 5n - o(n)$.*

Доказательство теоремы основано на методе забивающих констант. Для доказательства потребовалось рассмотреть несколько десятков случаев взаимного расположения элементов в верхней части схемы.

В работе [24] построена $(n, o(n))$-сильно-2-зависимая булева функция, которую можно реализовать схемой в базисе $U_2$ сложности $5n+o(n)$. Поэтому нижнюю оценку, большую $5n$, пользуясь лишь свойством сильно-2-зависимости, доказать невозможно.

## Заключение

До сих пор получены лишь невысокие линейные нижние оценки сложности явно заданных булевых функций в полных базисах. Основной метод получения известных нижних оценок — метод забивающих констант — состоит в последовательном удалении из схемы элементов, причем при удалении одного входа удаляется небольшое количество элементов. Представляется маловероятным, что использование этого метода позволит получить нелинейные нижние оценки.

Нелинейные нижние оценки известны для других классов управляющих систем. Так, лучшая нижняя оценка для формул [25] имеет, порядок $n^3$, а для контактных схем известна [26] нижняя оценка порядка $(n/\log n)^2$. Очень высокие (сверхполиномиальные) нижние оценки доказаны для некоторых классов схем, на которые наложены дополнительные ограничения, например, для схем ограниченной глубины [27] и для схем в неполном базисе $\{\&, \vee\}$ [28]. Таким образом, схемы в полных базисах являются одним из самых сложных классов для получения нижних оценок.

Нижним оценкам сложности булевых функций посвящено значительное количество литературы. Отдельно отметим монографию [3], обзор [4] и главы книг [29, 30], использованные при подготовке этой работы.

Работа выполнена при финансовой поддержке РФФИ (проект 14–01–00598).

## Литература

**1.** Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

**2.** Jukna S. Boolean function complexity: advances and frontiers. — Springer-Verlag Berlin Heidelberg, 2012.

**3.** Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.

**4.** Храпченко В.М. Нижние оценки сложности схем из функциональных элементов (обзор) // Кибернетический сборник. Новая серия. Вып. 21. — 1984. — С. 3–54.

**5.** Клосс Б. М., Малышев В. А. Оценки сложности некоторых классов функций // Вестник Моск. ун-та, сер. матем., мех. — 1965. — №4. — С.44–51.

**6.** Schnorr C. P. Zwei lineare untere Schranken für die Komplexität Boolescher Funktionen // Computing. — 1974. — 13. — S. 155-171.

**7.** Kojevnikov A., Kulikov A. Circuit Complexity and Multiplicative Complexity of Boolean Functions // Proc. of Computability in Europe (CiE 2010), Lecture Notes in Computer Science 6158. — 2010. — P. 239–245.

**8.** Редькин Н. П. Дискретная математика. — М.: Физматлит, 2009.

**9.** Schnorr C.P. The multiplicative complexity of boolean functions // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. — 1989. — P. 45–58.

**10.** Нечипорук Э. И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. — 1962. — Вып. 8. — С. 123–160.

**11.** Пауль В. Дж. Оценка $2.5n$ для комбинаторной сложности булевых функций // Кибернетический сборник. Вып. 16. — 1979. — С. 23–44.

**12.** Коровин В.В. О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — 1995. — Т. 7, вып. 2. — С. 95–102.

**13.** Blum N. A Boolean function requiring 3n network size // TCS. — 1984. — 28. — P. 337–345.

**14.** Ben-Sasson E., Koparty S. Affine dispersers from subspace polynomials // Proc. of STOC. — 2009. — 679. — P. 65–74.

**15.** Shaltiel R. Dispersers for Affine Sources with Sub-polynomial Entropy // 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. — 2013. — P. 247–256.

**16.** Demenkov E., Kulikov A. An Elementary Proof of a $3n - o(n)$ Lower Bound on the Circuit Complexity of Affine Dispersers. // Proc. of 36th International Symposium on Mathematical Foundations of Computer Science (MFCS 2011) — 2011. — P. 256–265.

**17.** Find M., Golovnev A., Hirsch E., Kulikov A. A better-than-3n lower bound for the circuit complexity of an explicit function. // ECCC. — 2015.

**18.** Комбаров Ю. А. О минимальных схемах для линейных функций в некоторых базисах // Дискретная математика. — 2013. — 25, 1. — С. 33–44.

**19.** Комбаров Ю. А. О минимальных реализациях линейных булевых функций // Дискретный анализ и исследование операций. — 2012. — Т. 19, вып. 3. — С. 39–57.

**20.** Комбаров Ю. А. О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискретный анализ и исследование операций. — 2013. — Т. 20, вып. 4. — С. 65–87.

**21.** Zwick U. A 4n lower bound on the combinational complexity of certain symmetric Boolean functions over the basis of unate dyadic Boolean functions // SIAM J. Comput. — 1991. — 20(3). — P. 499–505.

**22.** Savicky P., Zack S. A large lower bound for 1-branching programs // ECCC rep. No 96-030. — 1996.

**23.** Iwama K., Lachish O., Morizumi H., Raz R., An explicit lower bound of $5n - o(n)$ for Boolean circuits // Proceeding of the 33rd STOC, 2001. — P. 399–408.

**24.** Amano T., Tauri J. A Well-Mixed Function with Circuit Complexity $5n \pm o(n)$: Tightness of the Lachish-Raz-Type Bounds // Theory and Applications of Models of Computation. — 2008. — 342–350.

**25.** Hastard J. The Shrinkage Exponent of de Morgan Formulas is 2 // SIAM J. Comput. — 1998. — 27(1). — P. 48–64.

**26.** Ничепорук Э.И. Об одной булевской функции // Докл. АН СССР. — 1966. — 196(4). — С. 765–766.

**27.** Furst M., Saxe J., Sipster M. Parity, circuits and the polynomial time hierarchy // Mathematical Systems theory. — 1984. — 17. — P. 13–27.

**28.** А. А. Разборов. Нижние оценки монотонной сложности логического перманента // Матем. заметки. — 1985. — 37(6). — С. 887–900.

**29.** Сэвидж Дж. Сложность вычислений. — М.: Факториал, 1998.

**30.** Wegener I. The complexity of Boolean functions — Teubner, Stuttgart: Willey-Teubner Ser. Comput. Sci., 1987.

# О СЛОЖНОСТИ ФУНКЦИЙ $k$-ЗНАЧНЫХ ЛОГИК В КЛАССАХ ПОЛИНОМИАЛЬНЫХ ФОРМ

С. Н. Селезнева

**Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики, 119991, Москва, Ленинские горы, д. 1, стр. 52, 2-й учебный корпус**

e-mail: selezn@cs.msu.su

## Введение

В лекции предложен обзор о сложности представлений функций $k$-значных логик полиномиальными формами.

Пусть $k \geqslant 2$ — натуральное число, $E_k = \{0, 1, \ldots, k-1\}$. Функцией $k$-значной логики называется отображение $f^{(n)} : E_k^n \to E_k$, $n = 0, 1, 2, \ldots$. Полиномиальная форма (ПФ) — это сумма по модулю $k$ произведений каких-то базисных функций одной переменной. Длиной $l(P)$ ПФ $P$ называется число ее попарно различных слагаемых. Классы ПФ различаются видом базисных функций. Длиной $l^K(f)$ функции $k$-значной логики $f$ в классе $K$ называется наименьшая длина среди всех ПФ из класса $K$, представляющих эту функцию. Исследуется сложность представления функций в классе $K$ как наибольшая длина $L_k^K(n)$ в классе $K$ функций $k$-значной логики, зависящих от $n$ переменных.

Первая часть лекции посвящена функциям алгебры логики ($k = 2$). Во второй части лекции рассматриваются функции многозначных логик ($k \geqslant 3$). При этом проводится сравнение сложности функций $k$-значной логики в различных классах ПФ, для функций алгебры логики кроме того сравнивается длина ПФ с длиной ДНФ. Наконец, рассматривается сходство и различие ситуаций в двузначном и многозначном случаях.

## 1. Полиномиальные формы функций алгебры логики

В этом разделе мы рассмотрим полиномиальные формы функций алгебры логики, в том числе, в сравнении с дизъюнктивными нормальными формами (ДНФ). Один из доводов в пользу такого сравнения лежит в прикладной области. Дело в том, что существуют особые виды интегральных схем, называемые программируемыми логическими матрицами (ПЛМ). ПЛМ бывают двух видов, и на логическом уровне в одном случае в них представляются некоторые ДНФ, а в другом случае — некоторые ПФ. При этом в обоих случаях чем меньше слагаемых входит в соответствующие ДНФ или ПФ, тем меньшие ПЛМ требуются для их представления.

Элементарной конъюнкцией (ЭК) назовем произведение попарно различных переменных или их отрицаний. Дизъюнктивной нормальной формой (ДНФ) и, соответственно, полиномиальной нормальной формой (ПНФ) называются дизъюнкция и, соответственно, сумма по модулю два ЭК. ДНФ или ПНФ называется совершенной, если каждое ее слагаемое содержит все ее переменные. Совершенной ДНФ и совершенной ПНФ каждая функция алгебры логики представима однозначно, причем длина каждой из этих форм равна числу единичных значений функции. ЭК монотонна, если она не содержит отрицаний переменных, при этом константу 1 считаем монотонной ЭК. Каждая функция алгебры логики представима однозначным полиномом Жегалкина, т.е. суммой по модулю два монотонных ЭК. Здесь уже проявляется различие между ДНФ и ПНФ: ДНФ без отрицаний переменных представимы только монотонные функции алгебры логики. В случае ПФ понятие полинома Жегалкина можно обобщить и получить поляризованные полиномиальные формы (ППФ), к рассмотрению которых мы и перейдем.

**Поляризованные полиномиальные формы**. Если $\delta = (d_1, \ldots, d_n) \in E_2^n$, то поляризованной полиномиальной формой (ППФ) по вектору поляризации $\delta$ назовем сумму по модулю два ЭК, в которых переменная $x_i$ может встречаться только без отрицания при $d_i = 0$ и только с отрицанием при $d_i = 1$. Несложно заметить, что переменная $x_i$ может встречаться в ЭК только в виде выражения $x_i \oplus d_i$. Каждая функция алгебры логики $f(x_1, \ldots, x_n)$ представима однозначной ППФ $P^\delta(f)$ по каждому вектору $\delta \in E_2^n$. При нулевом векторе поляризации мы получаем полином Жегалкина $P(f)$. Отметим, что функцию алгебры логики представить ДНФ, в которой каждая переменная $x_i$ может входить в ЭК только в виде $x_i \oplus d_i$, возможно только в случае ее монотонности по переменным $x_i$ при $d_i = 0$ и антимонотонности по переменным $x_i$ при $d_i = 1$.

Итак, какова оценка длины $L_2^{\text{ППФ}}(n) = \max\limits_{f(x_1,\ldots,x_n)} \min\limits_{\delta \in E_2^n} l(P^\delta(f))$? В 1990 г. Т. Сасао, П. Безлич [1] рассмотрели представление функций алгебры логики в виде ППФ в ПЛМ. В 1993 г. В. П. Супрун [2] нашел некоторые оценки $L_2^{\text{ППФ}}(n)$, и вскоре Н. А. Перязев [3] получил окончательное решение: $L_2^{\text{ППФ}}(n) = \lfloor \frac{2}{3} 2^n \rfloor$. В его работе предложен интересный метод построения ППФ, основанный на разбиении слагаемых на непересекающиеся множества. Важно также отметить, что нижняя оценка Н. А. Перязевым получена не мощностным методом (как можно было бы ожидать), а предъявлением функций, на которых достигается доказанная им верхняя оценка. Эти функции являются симметрическими.

**Полиномиальные нормальные формы**. Теперь вернемся к ПНФ. В 1990-е г.г. опубликованы работы, в которых вычисляется длина ПНФ функций, зависящих от малого числа переменных. Это прикладные исследования, они связаны с представлением функций в ПЛМ. В частности, Т. Сасао [4] выяснил, что для функций четырех переменных средняя длина ДНФ рав-

на 4,13, а средняя длина ПНФ равна 3,66. Это показывает, что для функций четырех переменных ПНФ предпочтительней ДНФ (с точки зрения сложности представления). В 2005 г. К. Д. Кириченко [5] получил оценку длины $L_2^{\text{ПНФ}}(n)$. Остановимся на этом подробнее. В своей работе К. Д. Кириченко описал остроумный метод построения ПНФ функций алгебры логики на основе затеняющего множества куба $E_2^n$. Он доказал, что если $T$, $T \subseteq E_2^n$ — затеняющее множество куба $E_2^n$, то для произвольной функции алгебры логики $f(x_1, \ldots, x_n)$ можно построить ПНФ с длиной, не превосходящей $|T| + 1$, откуда $L_2^{\text{ПНФ}}(n) \leqslant |T| + 1$. Однако мощность затеняющего множества в этой работе оценивалась не очень удачно. В итоге получилась оценка $L_2^{\text{ПНФ}}(n) \leqslant \frac{2^{n+1}}{n}(\log_2 n + 1)$. Но уже отсюда следует, что длина ПНФ самых сложных функций по порядку меньше длины ДНФ самых сложных функций (даже если рассматривать ДНФ для почти всех функций). Но вернемся к вопросу об оценке. Несколько позднее М. А. Башов, изучая двусторонние тени в кубе $E_2^n$, нашел работу [6], в которой доказано, что можно построить затеняющее множество куба $E_2^n$ с мощностью, не превосходящей $c\frac{2^n}{n}$, где $c$ — постоянная величина. Отсюда по методу К. Д. Кириченко сразу получается, что $L_2^{\text{ПНФ}}(n) = O\left(\frac{2^n}{n}\right)$, т.к. нижняя мощностная оценка $L_2^{\text{ПНФ}}(n) \geqslant \frac{2^n}{n \log_2 3}$ была найдена [7] еще в 1967 г.

**Системы функций**. В ПЛМ представляются не отдельные функции, а системы функций. Поэтому целесообразно исследовать сложность систем функций алгебры логики в классах ПФ. Рассмотрим ППФ. Сложностью системы ППФ по вектору поляризации $\delta$ называется число попарно различных слагаемых во всех ППФ этой системы. Отметим, что такое определение сложности системы ППФ соответствует сложности представлений в ПЛМ. Сложностью $l^{\text{ППФ}}(F)$ системы функций $F = \{f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\}$ называется наименьшая сложность среди всех таких систем ППФ $\{P_1, \ldots, P_m\}$ с одним и тем же вектором поляризации, что ППФ $P_i$ представляет функцию $f_i$, $i = 1, \ldots, m$. Рассматривается сложность самых сложных систем с $m$ функциями: $L_2^{\text{ППФ}}(m, n) = \max\limits_{F=\{f_1,\ldots,f_m\}} l^{\text{ППФ}}(F)$, где $f_i = f_i(x_1, \ldots, x_n)$, $i = 1, \ldots, m$. Из определения следует, что $L_2^{\text{ППФ}}(m, n) \leqslant 2^n$. В 2015 г. С. Н. Селезневой [8] показано, что уже при $m = 2$ для всех $n \geqslant 1$ справедливо равенство $L_2^{\text{ППФ}}(m, n) = 2^n$, откуда получаем равенство при всех $m \geqslant 2$. Для доказательства были предъявлены системы функций, на которых достигается верхняя оценка. Примечательно, что эти системы образованы функциями из доказательства нижней оценки Н. А. Перязева.

## 2. Полиномиальные формы функций многозначных логик

В многозначных логиках возможности более широки. Во-первых, каждая функция $k$-значной логики представима полиномом по модулю $k$ только в

случае простых $k$. Поэтому везде в дальнейшем считаем $k$ простым числом. Во-вторых, в ПФ появляются степени переменных и коэффициенты слагаемых. Наконец, отрицание при $k \geqslant 3$ уже можно определять по-разному. Все это приводит к тому, что сначала следует аккуратно перенести задачи о сложности ППФ и ПНФ на многозначный случай.

**Поляризованные полиномиальные формы**. В [9] рассмотрены некоторые возможности определения ППФ при $k \geqslant 3$, в частности, предложено рассматривать базисные функции переменной $x_i$ из множества $\{1, x_i + d_i, (x_i+d_i)^2, \ldots, (x_i+d_i)^{k-1}\}$, причем $d_i \in E_k$ определяется вектором поляризации $\delta = (d_1, \ldots, d_n) \in E_k^n$. Такие ПФ в многозначном случае назовем также поляризованными полиномиальными формами (ППФ). Какие получены оценки для длины $L_k^{\text{ППФ}}(n) = \max\limits_{f(x_1,\ldots,x_n)} \min\limits_{\delta \in E_k^n} l(P^\delta(f))$? В 2002 г. С. Н. Селезневой [9] найдена верхняя оценка $L_k^{\text{ППФ}}(n) \leqslant \frac{k(k-1)}{k(k-1)+1} k^n$. Мощностным методом получена нижняя оценка $\frac{k-1}{k} k^n \lesssim L_k^{\text{ППФ}}(n)$ в [10]. Опираясь на ситуацию в двузначном случае, возможно было ожидать, что мощностная оценка не является точной. И в самом деле, в 2012 г. Н. К. Маркеловым [11] доказано, что $L_3^{\text{ППФ}}(n) \geqslant \lfloor \frac{3}{4} 3^n \rfloor$, предъявлением функций трехзначной логики, на которых достигается эта оценка. В 2015 г. этот результат был усилен С. Н. Селезневой [8] построением симметрических функций трехзначной логики с такой же длиной в классе ППФ. Отметим, что в 2004 г. было также показано [12], что $L_k^{\text{ППФ}}(1) = k - 1$.

В [13,14] предложена другая возможность определения базисных функций. Пусть $\{s_{0,i}(x_i), s_{1,i}(x_i), \ldots, s_{k-1,i}(x_i)\}$ — множество, образующее базис функций одной переменной. Если заданы такие множества для всех переменных $x_1, \ldots, x_n$, то каждая функция $k$-значной логики представляется ПФ, в которой сомножители в слагаемых только из этих базисных множеств. Если для каждого базисного множества степени полиномов по модулю $k$ составляющих его функций принимают значения от 0 до $k-1$, то такие ПФ назовем обобщенно поляризованными (ОППФ), в общем случае — квазиполиномиальными формами (КВПФ). В 2009 г. С. Н. Селезневой в [13] доказано, что $L_k^{\text{ОППФ}}(n) \leqslant \frac{k}{k+1} k^n$. В 2014 г. А. С. Балюк [15] показал, что $L_k^{\text{КВПФ}}(n) \leqslant \frac{k-1}{k-k^{1-k}} k^n$. Что касается нижней оценки, то известна только нижняя мощностная оценка $\frac{k-1}{k} k^n \lesssim L_k^{\text{ОППФ}}(n)$ [13], которая верна и для КВПФ.

**Полиномиальные нормальные формы**. Для полиномиальных нормальных форм ситуация в многозначных логиках оказалась более податливой в том смысле, что удалось получить результаты, аналогичные двузначному случаю. Определим в $k$-значном логике ПНФ как сумму по модулю $k$ произведений выражений $x_i + d$, $d \in E_k$. По совокупности работ С. Н. Селезневой, А. Б. Дайняка, М. А. Башова [16, 17] в 2008–2014 г.г. получено, что

$L_k^{\text{ПНФ}}(n) = O\left(\frac{k^n}{n}\right)$. Отметим, что верхняя оценка получена обобщением метода К. Д. Кириченко из [5]. При этом была найдена оценка затеняющего множества единичного куба $E_k^n$ [17]. Нижняя оценка доставляется мощностным методом [16].

**Системы функций**. Сложность систем функций $k$-значной логики в классе ППФ определяется аналогично двузначному случаю. В 2015 г. С. Н. Селезневой [8] доказано равенство $L_3^{\text{ПНФ}}(m,n) = 3^n$ при всех $m \geqslant 2$ и $n \geqslant 1$. Доказательство при $m = 2$ получено предъявлением систем из двух функций трехзначной логики, на которых достигается эта оценка. При этом подошли симметрические функции из [8], которые улучшают нижнюю мощностную оценку длины функций трехзначной логики в классе ППФ. При произвольных простых $k \geqslant 5$ пока вопрос остается открытым.

## Заключение

Предложенный обзор сложности полиномиальных форм функций $k$-значной логики не претендует на полноту. В нем присутствует подход к изучению ПФ как аналога ДНФ в алгебре логики с дальнейшим обобщениям на многозначный случай. При этом выделяются виды ПФ, которые являются каноническими. Однако существуют другие подходы. В [18] (гл. 3) подробно освещены вопросы полиномиальных операторных представлений функций алгебры логики. В [19] рассматриваются аналогичные вопросы функций $k$-значных логик. Полиномиальные операторные представления являются каноническими формами для функций $k$-значных логик.

Что касается приведенных оценок, то некоторые из них не окончательны (в смысле длины самой сложной функции), остается много открытых задач. Но эти задачи исследуются, появляются новые результаты. Уже после прочтения лекции вышла работа А. С. Балюка, Г. В. Янушковского [20], в которой улучшены оценки длины функций в классах ППФ и ОППФ: $L_k^{\text{ППФ}}(n) \leqslant \frac{k(k-1)-1}{k(k-1)}$ $(k \geqslant 3)$ и $L_k^{\text{ОППФ}}(n) \leqslant \frac{k+(k-1)^{-1}-1}{k+(k-1)^{-1}}k^n$. Конечно, основная операция сложения по модулю $k$ и введение некоторых ПФ через базисы пространства функций одной переменной почти обязывают нас при их изучении применять алгебру, в частности, свойства конечных полей и линейных пространств. Однако постановка задачи как исследования длины и сложности ПФ оставляют автора в убеждении, что завершенные результаты могут быть получены красивым сочетанием алгебраических свойств с кибернетическими методами.

## Литература

**1.** Sasao T., Besslich P. On the complexity of mod-2 sum PLA's // IEEE Trans. on Comput. — 1990. — V. 39, N 2. — P. 262–266.

**2.** Супрун В. П. Сложность булевых функций в классе канонических поляризованных полиномов // Дискретная математика. — 1993. — Т. 5,

вып. 2. С. 111–115.

**3.** Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. С. 323–326.

**4.** Sasao T. Representations of logic functions by using EXOR operators // In Representations of Discrete Functions. — Boston: Kluwer Academic Publishers, 1996. — P. 29–54.

**5.** Кириченко К. Д. Верхняя оценка сложности полиномиальных нормальных форм булевых функций // Дискретная математика. — 2005. — Т. 17, вып. 3. — С. 80–88.

**6.** Cooper J. N., Ellis R. B., Kahng A. B. Asymmetric binary covering codes // J. of Comb. Theory. Ser. A. — 2002. — V. 100, N 2. — P. 232–249.

**7.** Even S., Kohavi I., Paz A. On minimal modulo 2 sums of products for switching functions // IEEE Trans. Elect. Comput. — 1967. — P. 671–674.

**8.** Селезнева С. Н. Сложность систем функций алгебры логики и систем функций трехзначной логики в классах поляризованных полиномиальных форм // Дискретная математика. — 2015. — Т. 27, вып. 1. — С. 111–122.

**9.** Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

**10.** Алексеев В. Б., Вороненко А. А., Селезнева С. Н. О сложности реализации функций $k$-значной логики поляризованными полиномами // Сб. Труды V Международной конференции «Дискретные модели в теории управляющих систем» (Ратмино, 26–29 мая 2003 г.). — М.: МАКС Пресс, 2003. — С. 8–9.

**11.** Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2012. — вып. 3. — С. 40–45.

**12.** Селезнева С. Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 117–121.

**13.** Селезнева С. Н. О сложности обобщенно-поляризованных полиномов $k$-значных функций // Дискретная математика. — 2009. — Т. 21, вып. 4. — С. 20–29.

**14.** Селезнева С. Н. О сложности $k$-значных функций в одном классе полиномов // Сб. Проблемы теоретической кибернетики. Материалы XVI Международной конференции (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Издательство Нижегородского университета, 2011. — С. 430–434.

**15.** Балюк А. С. О верхней оценке сложности задания квазиполиномами функций над конечными полями // Известия Иркутского государственного университета. Серия: Математика. — 2014. — Т. 10. — С. 3–12.

**16.** Селезнева С. Н., Дайняк А. Б. О сложности обобщенных полиномов $k$-значных функций // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2008. — № 3. — С. 34–39.

**17.** Башов М. А., Селезнева С. Н. О длине функций $k$-значной логики в классе полиномиальных нормальных форм по модулю $k$ // Дискретная математика. — 2014. — Т. 26, вып. 3. — С. 3–9.

**18.** Избранные вопросы теории булевых функций. Под ред. С. Ф. Винокурова и Н. А. Перязева. — М.: Физматлит, 2001.

**19.** Зинченко А. С., Пантелеев В. И. Полиномиальные операторные представления $k$-значной логики // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, вып. 3. — С. 13–26.

**20.** Балюк А. С., Янушковский Г. В. Верхние оценки функций над конечными полями в некоторых классах кронекеровых форм // Известия Иркутского государственного университета. Серия: Математика. — 2015. — Т. 14. — С. 3–17.

# О ВЫЧИСЛЕНИИ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

А. В. Чашкин

**Московский государственный университет имени М.В.Ломоносова,
механико-математический факультет,
Москва, Ленинские горы, д. 1, Главное здание**

e-mail: chashkin@inbox.ru

## Введение

Множество монотонных булевых функций по своим свойствам достаточно сильно отличается от множества всех булевых функций. Эти отличия естественным образом проявляются при реализации монотонных булевых функций в различных моделях вычислений. В настоящей лекции рассматриваются три связанных с вычислениями монотонных булевых функций сюжета, в которых своеобразие этих функций проявляется достаточно ярко.

## 1. Монотонные функции

**1.** Множество $\{0,1\}^n$ всех булевых наборов длины $n$ называется булевым кубом размерности $n$ и обозначается символом $B^n$. Все наборы с $k$ единицами называются $k$-м слоем $B^n$. Расстоянием Хемминга между наборами $\boldsymbol{u}$ и $\boldsymbol{v}$ из $B^n$ называется число $d(\boldsymbol{u},\boldsymbol{v}) = \sum_{i=1}^{n} |u_i - v_i|$, равное количеству несовпадающих разрядов $\boldsymbol{u}$ и $\boldsymbol{v}$. Булев куб является частично упорядоченным множеством с частичным порядком $\preceq$, при котором набор $\boldsymbol{u}$ не больше набора $\boldsymbol{v}$ ($\boldsymbol{u} \preceq \boldsymbol{v}$), если $u_i \leqslant v_i$ при всех $i = 1, 2, \ldots, n$. Если $\boldsymbol{u} \preceq \boldsymbol{v}$ и $\boldsymbol{u} \neq \boldsymbol{v}$, то говорят, что набор $\boldsymbol{u}$ строго меньше набора $\boldsymbol{v}$ ($\boldsymbol{u} \prec \boldsymbol{v}$). Наборы $\boldsymbol{u}$ и $\boldsymbol{v}$ называются сравнимыми, если либо $\boldsymbol{u} \preceq \boldsymbol{v}$, либо $\boldsymbol{v} \preceq \boldsymbol{u}$. Если ни одно из этих отношений не выполняется, то наборы называются несравнимыми. Последовательность наборов $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k)$ называется цепью, если $d(\boldsymbol{u}_i, \boldsymbol{u}_{i+1}) = 1$ и $\boldsymbol{u}_i \preceq \boldsymbol{u}_{i+1}$ для всех $i = 1, 2, \ldots, k-1$. Длиной $|\boldsymbol{\alpha}|$ цепи $\boldsymbol{\alpha}$ называется число наборов в этой цепи. Говорят, что цепь связывает наборы $\boldsymbol{u}$ и $\boldsymbol{v}$ и проходит через набор $\boldsymbol{w}$, если $\boldsymbol{u}$ и $\boldsymbol{v}$ являются, соответственно, первым и последним наборами цепи, а $\boldsymbol{w}$ принадлежит этой цепи. Цепь называется максимальной, если она не является частью цепи большей длины. Множество попарно несравнимых вершин называется антицепью. Антицепь называется максимальной, если она не является подмножеством другой антицепи, состоящей из большего количества наборов. Классическая комбинаторная теорема Дилуорса обнаруживает связь между цепями и антицепями в частично упорядоченном множестве. Эта теорема утверждает, что минимальное число цепей, которыми можно покрыть

частично упорядоченное множество, равно мощности максимальной антицепи этого множества. Другая, не менее известная теорема — теорема Шпернера — утверждает, что максимальная антицепь в $n$-мерном булевом кубе состоит из $\binom{n}{\lfloor n/2 \rfloor}$ наборов. Поэтому, в силу этих двух теорем, $n$-мерный булев куб можно покрыть $\binom{n}{\lfloor n/2 \rfloor}$ непересекающимися цепями. Такое покрытие в явном виде было построено Анселем [1].

**2.** Напомним, что $n$-местная булева функция $f : B^n \to B^1$ называется монотонной, если

$$f(\alpha_1, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_n)$$

для любых наборов $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ таких, что $\boldsymbol{\alpha} \preceq \boldsymbol{\beta}$. Набор $\boldsymbol{\alpha}$ называется нижней единицей монотонной функции $f$, если $f(\boldsymbol{\alpha}) = 1$ и $f(\boldsymbol{\beta}) = 0$ для всех $\boldsymbol{\beta} \prec \boldsymbol{\alpha}$. Легко видеть, что нижние единицы любой $n$-местной монотонной функции образуют антицепь в $B^n$, и в тоже время любая антицепь является множеством всех нижних единиц монотонной функции. Из этого соответствия следует очевидная нижняя оценка для $M(n)$ — числа всех $n$-местных монотонных булевых функций, которую приведем в логарифмическом виде:

$$\log_2 M(n) \geqslant \binom{n}{\lfloor n/2 \rfloor} \sim \frac{2^n}{\sqrt{\pi n/2}}. \tag{1}$$

Для доказательства (1) достаточно заметить, что любое подмножество $\lfloor n/2 \rfloor$-го слоя в $B^n$ является антицепью. Аналогичное верхнее асимптотическое неравенство

$$\log_2 M(n) \lesssim \binom{n}{\lfloor n/2 \rfloor}$$

доказывается достаточно сложно. Это неравенство было установлено Клейтменом в работе 1969 года. В следующем году вышел русский перевод [2] этой работы. Позднее асимптотически точную формулу для $M(n)$ установил А. Д. Коршунов. Здесь эта формула не приводится, так как она достаточно громоздка (формула и ее полное доказательство опубликованы в [3]).

**3.** Приведем простую верхнюю оценку числа $n$-местных монотонных булевых функций, позволяющую установить порядок функции $\log_2 M(n)$. Для этого потребуется следующее утверждение.

**Лемма 1** [4]. *Пусть $\boldsymbol{\alpha}$ — цепь в $B^n$, $\boldsymbol{\beta}$ — цепь в $B^m$. На прямом произведении $\boldsymbol{\alpha} \times \boldsymbol{\beta}$ существует ровно $\binom{|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|}{|\boldsymbol{\alpha}|}$ монотонных булевых функций.*

**Доказательство.** Монотонную функцию на прямом произведении цепей $\alpha_1 \prec \cdots \prec \alpha_s$ и $\beta \prec \cdots \prec \beta_t$ можно однозначно определить, указав набор $k_1, \ldots, k_t$, где $k_i$ равно числу пар вида $(\alpha_j, \beta_i)$, на которых эта функция равна единице. Так как $0 \leqslant k_1 \leqslant \ldots \leqslant k_t \leqslant s$, то набору $k_1, \ldots, k_t$ можно поставить в соответствие набор из $t$ нулей и $s$ единиц так, что $k_i$ будет равно числу единиц, которые стоят в булевом наборе левее $i$-го нуля. Легко видеть, что такое соответствие будет взаимно однозначным. Лемма доказана.

**Лемма 2**. *При при достаточно больших $n$*

$$\log_2 M(n) \leqslant 3\binom{n}{\lfloor n/2 \rfloor}.$$

**Доказательство.** Для простоты изложения ограничимся случаем четного $n$, для нечетных $n$ доказательство аналогично рассматриваемому случаю. Пусть $n = 2k$. Представим $n$-мерный булев куб $B^n$ в виде прямого произведения двух $k$-мерных кубов $B_1^k$ и $B_2^k$, каждый из которых, в свою очередь, представим в виде объединения $\binom{k}{\lfloor k/2 \rfloor}$ непересекающихся цепей — $B_1^k = \bigcup_{\boldsymbol{\alpha}} \boldsymbol{\alpha}$ и $B_2^k = \bigcup_{\boldsymbol{\beta}} \boldsymbol{\beta}$. Нетрудно видеть, что в этом случае куб $B^n$ является объединением

$$B^{2k} = \left(\bigcup_{\boldsymbol{\alpha}} \boldsymbol{\alpha}\right) \times \left(\bigcup_{\boldsymbol{\beta}} \boldsymbol{\beta}\right) = \bigcup_{\boldsymbol{\alpha}} \bigcup_{\boldsymbol{\beta}} (\boldsymbol{\alpha} \times \boldsymbol{\beta}) \tag{2}$$

$\binom{k}{\lfloor k/2 \rfloor}^2$ прямых произведений цепей. Следовательно, с учетом леммы 1,

$$M(2k) \leqslant \prod_{\boldsymbol{\alpha}} \prod_{\boldsymbol{\beta}} \binom{|\boldsymbol{\alpha}| + |\boldsymbol{\beta}|}{|\boldsymbol{\alpha}|} \leqslant \prod_{\boldsymbol{\alpha}} \prod_{\boldsymbol{\beta}} 2^{|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|} = 2^{\sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} (|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|)}.$$

Так как

$$\begin{aligned} \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} (|\boldsymbol{\alpha}| + |\boldsymbol{\beta}|) &= \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} |\boldsymbol{\alpha}| + \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} |\boldsymbol{\beta}| = \\ &= \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} |\boldsymbol{\alpha}| + \sum_{\boldsymbol{\beta}} \sum_{\boldsymbol{\alpha}} |\boldsymbol{\beta}| = 2 \sum_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta}} |\boldsymbol{\alpha}| = \\ &= 2 \sum_{\boldsymbol{\alpha}} |\boldsymbol{\alpha}| \sum_{\boldsymbol{\beta}} 1 = 2 \sum_{\boldsymbol{\alpha}} |\boldsymbol{\alpha}| \binom{k}{\lfloor k/2 \rfloor} = 2^{k+1} \binom{k}{\lfloor k/2 \rfloor}, \end{aligned} \tag{3}$$

то

$$\log_2 M(2k) \leqslant 2^{k+1} \binom{k}{\lfloor k/2 \rfloor}.$$

Теперь для доказательства леммы достаточно воспользоваться формулой Стирлинга и с ее помощью показать, что при достаточно больших $k$

$$2^{k+1} \binom{k}{\lfloor k/2 \rfloor} \sim \frac{2^{k+1} \cdot 2^k}{\sqrt{\pi k/2}} = \frac{2^{3/2} \cdot 2^{2k}}{\sqrt{\pi k}} \leqslant 3\binom{2k}{k}. \tag{4}$$

Лемма доказана.

## 2. Сложность вычисления

**1.** Пусть $\mathcal{B}$ — подмножество множества всех не более чем двуместных булевых функций. Схемой $\mathsf{S}$ в базисе $\mathcal{B}$ над множеством независимых булевых переменных $X = \{x_1, \ldots, x_n\}$ называется последовательность $s_1, \ldots, s_L$, в которой ее $i$-й элемент является равенством $y_i = f_i(z_1, z_2)$, где $f_i \in \mathcal{B}$, $z_1, z_2 \in X \bigcup \{y_1, \ldots, y_{i-1}\}$. Величины $y_i$ называются внутренними переменными схемы $S$, а число равенств $L$ — сложностью схемы. Легко видеть, что каждая внутренняя переменная $y_i$ является булевой функцией от переменных из $X$. Будем говорить, что схема $\mathsf{S}$ вычисляет функцию $f(x_1, \ldots, x_n)$, если $f \equiv y_L$. Вычисляющая функцию $f$ схема $\mathsf{S}$ называется минимальной (в базисе $\mathcal{B}$) схемой этой функции, если ее сложность не больше сложности любой другой вычисляющей $f$ схемы в базисе $\mathcal{B}$. Сложностью $L_{\mathcal{B}}(f)$ функции $f$ в базисе $\mathcal{B}$ называется сложность ее минимальной схемы в этом базисе. Далее будем рассматривать монотонный базис $\{\&, \vee\}$ и полный базис $\{\&, \vee, \neg\}$.

**2.** Сложность вычисления монотонных булевых функций схемами в полном базисе рассматривалась многими авторами, начиная с конца 50-х годов XX века. Асимптотически точный результат был получен А. Б. Угольниковым в 1976 году в [5]. Из результатов этой работы следует, что при $n \to \infty$ для сложности каждой $n$-местной монотонной булевой функции $f$ справедливо асимптотическое неравенство

$$L_{\{\&, \vee, \neg\}}(f) \lesssim \frac{2^n}{n\sqrt{\pi n/2}}. \tag{5}$$

Задача о вычислении монотонных функций схемами в монотонном базисе оказалась значительно сложнее. Первые существенные результаты в этом направлении были получены Н. П. Редькиным в конце 70-х годов XX века. Из опубликованной в 1979 году работы [4] следует, что для сложности каждой $n$-местной монотонной булевой функции $f$ предыдущее неравенство справедливо с точностью до постоянного множителя, т. е.

$$L_{\{\&, \vee\}}(f) = \mathcal{O}\left(\frac{2^n}{n\sqrt{n}}\right). \tag{6}$$

Асимптотически точная оценка для монотонного базиса

$$L_{\{\&, \vee\}}(f) \lesssim \frac{2^n}{n\sqrt{\pi n/2}} \tag{7}$$

установлена А. Е. Андреевым в 1988 году [6]. Нижняя оценка

$$L(f) \gtrsim \frac{2^n}{n\sqrt{\pi n/2}}, \tag{8}$$

справедливая в этих базисах при $n \to \infty$ для почти каждой $n$-местной монотонной булевой функции, легко получается применением стандартного мощ-

ностного метода к неравенству (1). Доказательства неравенств (5) и (7) существенным образом опирались на метод перечисления монотонных функций из [2].

**3.** Далее установим справедливость неравенства (6). Сделаем это, упростив соответствующее доказательство из [4].

При вычислении монотонных функций схемами в монотонном базисе будем использовать монотонное разложение этих функции по части их переменных. Напомним, что для каждой $n$-местной монотонной булевой функции $f(x_1,\dots,x_n)$ при любом $m$, $1\leqslant m\leqslant n$, справедливо ее монотонное разложение

$$f(x_1,\dots,x_m,x_{m+1},\dots,x_n)= \\ =\bigvee_{\sigma_1,\dots,\sigma_m} x_1^{\sigma_1}\cdot\ldots\cdot x_m^{\sigma_m}\cdot f(\sigma_1,\dots,\sigma_m,x_{m+1},\dots,x_n) \qquad (9)$$

по переменным $x_1,\dots,x_m$, где $x^1=x$ и $x^0=1$. Из (9) легко следует, что

$$f(x_1,\dots,x_n)=\bigvee_{\boldsymbol{\alpha}=(\alpha_1,\dots,\alpha_n)} x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}, \qquad (10)$$

где $\{\boldsymbol{\alpha}\}$ — множество всех нижних единиц функции $f$.

Пусть $\boldsymbol{\alpha}$ — цепь в $B^n$, $\boldsymbol{\beta}$ — цепь в $B^m$. Периметром прямого произведения $\boldsymbol{\alpha}\times\boldsymbol{\beta}$ цепей $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$ назовем сумму $|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|$ длин этих цепей. Вернемся к рассмотренному выше (2) представлению $2k$-мерного булева куба в виде объединения прямых произведений цепей $k$-мерных кубов:

$$B^{2k}=\left(\bigcup_{\boldsymbol{\alpha}}\boldsymbol{\alpha}\right)\times\left(\bigcup_{\boldsymbol{\beta}}\boldsymbol{\beta}\right)=\bigcup_{\boldsymbol{\alpha}}\bigcup_{\boldsymbol{\beta}}(\boldsymbol{\alpha}\times\boldsymbol{\beta}). \qquad (11)$$

Это объединение состоит из $\binom{k}{\lfloor k/2\rfloor}^2$ прямых произведений, периметры которых могут меняться от 2 до $2k+2$, а сумма периметров всех прямых произведений в силу (3) не превосходит $2^{k+1}\binom{k}{\lfloor k/2\rfloor}$. Нетрудно показать, что прямые произведения в (11) можно объединить в блоки $I_j$ так, что сумма периметров в каждом блоке не превосходит $2k+2$ и в каждом блоке, кроме быть может одного, не меньше $k+2$. Следовательно, число блоков $I_j$ в представлении

$$B^{2k}=\bigcup_j I_j \qquad (12)$$

при $k\to\infty$ асимптотически не превосходит величины

$$2^{k+1}\binom{k}{\lfloor k/2\rfloor}\Big/k\lesssim\frac{2^{2k}}{k^{3/2}}. \qquad (13)$$

Из леммы 1 легко следует, что число различных монотонных функций, определенных на блоке $I$ периметра $P$, не превосходит $2^P$. Этот факт вместе с неравенством (13) лежит в основе доказательства следующей теоремы.

**Теорема 1**. *При $n \to \infty$ для каждой $n$-местной монотонной булевой функции $f$*

$$L_{\{\&,\vee\}}(f) \lesssim \frac{16 \cdot 2^n}{n\sqrt{\pi n/2}}.$$

**Доказательство.** Воспользуемся представлением (12) для вычисления монотонной $n$-местной функции $f$. Пусть $n = 2k + m$ и $k \to \infty$ вместе с $n$. Разложим функцию $f$ по последним $m$ переменным

$$f(x_1, \ldots, x_n) = \bigvee_{\gamma_1,\ldots,\gamma_m} f(x_1, \ldots, x_{2k}, \gamma_1, \ldots, \gamma_m) x_{2k+1}^{\gamma_1} \cdot \ldots \cdot x_{2k+m}^{\gamma_m}.$$

Напомним, что здесь $x^1 = x$ и $x^0 = 1$. Пусть $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_m)$. Положим

$$f_{\boldsymbol{\gamma}}(x_1, \ldots, x_{2k}) = f(x_1, \ldots, x_{2k}, \gamma_1, \ldots, \gamma_m).$$

Через $f_{I,\boldsymbol{\gamma}}(x_1, \ldots, x_{2k})$ обозначим монотонную функцию, все нижние единицы которой находятся в $I$ и которая на $I$ совпадает с функцией $f_{\boldsymbol{\gamma}}(x_1, \ldots, x_{2k})$. В этом случае

$$f_{\boldsymbol{\gamma}}(x_1, \ldots, x_{2k}) = \bigvee_{I \subseteq B^{2k}} f_{I,\boldsymbol{\gamma}}(x_1, \ldots, x_{2k}),$$

где $f_{I,\boldsymbol{\gamma}}(x_1, \ldots, x_{2k})$ — одна из не более чем $2^{2k+2}$ определенных на блоке $I$ монотонных функций $h_{I,s}(x_1, \ldots, x_{2k})$. Следовательно,

$$\begin{aligned} f(x_1, \ldots, x_n) &= \bigvee_{\boldsymbol{\gamma}} \left( \bigvee_{I \subseteq B^{2k}} f_{I,\boldsymbol{\gamma}}(x_1, \ldots, x_{2k}) \right) x_{2k+1}^{\gamma_1} \cdot \ldots \cdot x_{2k+m}^{\gamma_m} = \\ &= \bigvee_{I \subseteq B^{2k}} \bigvee_{s} h_{I,s}(x_1, \ldots, x_{2k}) \cdot \bigvee_{\boldsymbol{\gamma} \,|\, f_{I,\boldsymbol{\gamma}} = h_{I,s}} x_{2k+1}^{\gamma_1} \cdot \ldots \cdot x_{2k+m}^{\gamma_m}. \end{aligned} \tag{14}$$

Отметим, что в правой формуле равенства (14) для каждого $I$ число внутренних (правых) дизъюнкций не превосходит $2^m$ — числа наборов $\boldsymbol{\gamma}$, числа конъюнкций и средних дизъюнкций не превосходят $2^{2k+2}$ — числа возможных монотонных функций на $I$, а число внешних дизъюнкций (см. (13)) асимптотически не больше $2^{k+1}\binom{k}{\lfloor k/2 \rfloor}/k$ — числа блоков в (12).

Вычисление $f$ проведем в соответствии с правой формулой равенства (14). Выполним следующие действия.

1. Вычислим все монотонные мономы вида $x_{2k+1}^{\gamma_1} \cdot \ldots \cdot x_{2k+m}^{\gamma_m}$. Легко видеть, что для этого достаточно $2^m$ конъюнкций.

2. Для каждого блока $I$ из $B^{2k}$ вычислим все определенные на этом блоке монотонные функции $h_{I,s}(x_1, \ldots, x_{2k})$. Функции будем вычислять как дизъюнкции монотонных конъюнкций, соответствующих нижним единицам этих функций. Так как на каждом блоке определено не более $2^{2k+2}$ различных

функций и число блоков асимптотически не превосходит $2^{2k}/k^{3/2}$, то нетрудно показать, что общее количество использованных для этого дизъюнкций и конъюнкций асимптотически не превосходит $2^{2k+2}\cdot 2^{2k}/k^{3/2}$.

3. Используя вычисленные в пп. 1 и 2 функции, для каждого блока $I$ вычислим дизъюнкцию

$$f_I = \bigvee_s h_{I,s}(x_1,\ldots,x_{2k})\cdot \bigvee_{\boldsymbol{\gamma}\,|\,f_{I,\boldsymbol{\gamma}}=h_{I,s}} x_{2k+1}^{\gamma_1}\cdot\ldots\cdot x_{2k+m}^{\gamma_m}.$$

Из сказанного выше следует, что для этого потребуется асимптотически не более чем $(2^m+2\cdot 2^{2k+2})\cdot 2^{k+1}\binom{k}{\lfloor k/2\rfloor}/k$ дизъюнкций и конъюнкций.

4. Вычислим дизъюнкцию $\bigvee_I f_I$ найденных в п. 3 функций $f_I$. Для этого потребуется асимптотически не более чем $2^{k+1}\binom{k}{\lfloor k/2\rfloor}/k$ дизъюнкций.

Таким образом, для монотонной сложности произвольной $n$-местной монотонной булевой функции $f$ справедливо асимптотическое неравенство

$$L_{\{\&,\vee\}}(f)\lesssim 2^m+2^{2k+2}\cdot\frac{2^{2k}}{k^{3/2}}+\frac{2^{k+1}\binom{k}{\lfloor k/2\rfloor}}{k}\cdot(2^m+2^{2k+3})+\frac{2^{k+1}\binom{k}{\lfloor k/2\rfloor}}{k}\lesssim$$
$$\lesssim\frac{2^{k+1}\binom{k}{\lfloor k/2\rfloor}}{k}\cdot 2^m+\mathcal{O}\left(\frac{2^{4k}}{k^{3/2}}\right),$$

где $2k+m=n$. Положим $k=\lfloor n/4-\log_2 n\rfloor$. Тогда

$$L_{\{\&,\vee\}}(f)\lesssim\frac{2^{k+1}\binom{k}{\lfloor k/2\rfloor}}{k}\cdot 2^{n-2k}+\mathcal{O}\left(\frac{2^{4k}}{k^{3/2}}\right)\lesssim\frac{16\cdot 2^n}{n\sqrt{\pi n/2}}.$$

Теорема доказана.

## 3. Сложность приближенного вычисления

**1.** Одним из вспомогательных результатов, позволивших найти асимптотику для $M(n)$, стал следующий замечательный факт о строении «типичной» монотонной булевой функции [3]:

*при $n\to\infty$ почти все $n$-местные монотонные булевы функции равны нулю на наборах, содержащих менее чем $n/2-2$ единиц, и равны единице на наборах, содержащих более чем $n/2+2$ единиц.* (15)

Из (15) следует, что если вместо $n$-местной монотонной функции $f$ можно использовать какое-либо ее достаточно точное приближение — функцию, отличающуюся от $f$ на $o\big(2^n\big)$ наборах, то вместо вычисления почти каждой $n$-местной монотонной булевой функции $f$ можно с линейной сложностью вычислить значения пары симметрических пороговых функций с порогами $\lfloor n/2-3\rfloor$ и $\lceil n/2+3\rceil$. Если значения этих функций на наборе $\boldsymbol{x}$ совпадут и

будут равны $\alpha$, то и $f(\boldsymbol{x}) = \alpha$. Если значения не совпадают, то набор $\boldsymbol{x}$ лежит между $\lfloor n/2 - 3 \rfloor$-м и $\lceil n/2 + 3 \rceil$-м слоями, т. е. принадлежит множеству из $\mathcal{O}\left(2^n/\sqrt{n}\right)$ наборов. Таким образом, пока еще неформально можно сказать, что при $n \to \infty$ сложность приближенного вычисления почти каждой $n$-местной монотонной булевой функции есть $\mathcal{O}(n)$.

Далее дадим необходимые определения и покажем, что некоторый аналог указанного свойства — существование достаточно простого и достаточно точного приближения, имеет место для каждой монотонной булевой функции.

**2.** Сложностью вычисления $n$-местной булевой функции $f$ с точностью $1 - \varepsilon$ называется $\min L(h)$, где минимум берется по всем таким функциям $h$, что

$$\sum_{\boldsymbol{x} \in B^n} f(\boldsymbol{x}) \oplus h(\boldsymbol{x}) \leqslant \varepsilon 2^n. \tag{16}$$

Известно (см., например, теорему 3.5 в [7]), что при $n \to \infty$ для почти всех $n$-местных булевых функций сложность их вычисления с точностью $1 - o(1)$ асимптотически совпадает со сложностью их точного вычисления и асимптотически равна $2^n/n$ — сложности самой сложной $n$-местной булевой функции, т. е. для почти всех булевых функций невозможно за счет редких неправильно вычисленных значений сколько-нибудь заметно уменьшить сложность вычислений. Для монотонных функций ситуация иная — поступившись точностью, можно существенно уменьшить сложность вычислений.

Будем говорить, что монотонные булевы функции $f_m$ и $f_M$ вычисляют $n$-местную монотонную булеву функцию $f$ с точностью $1-\varepsilon$, если $f_m(x) \leqslant f(\boldsymbol{x}) \leqslant f_M(\boldsymbol{x})$ для любого $\boldsymbol{x} \in B^n$ и $f_m(\boldsymbol{x}) \neq f_M(\boldsymbol{x})$ не более чем на $\varepsilon 2^n$ наборах длины $n$. Сложностью вычисления $n$-местной монотонной булевой функции $f$ с точностью $1 - \varepsilon$ назовем $\min L(f_m, f_M)$, где минимум берется по всем парам монотонных функций $f_m, f_M$, вычисляющих $f$ с точностью $1 - \varepsilon$.

Отметим, что пара монотонных функций приближает монотонную функцию «сильнее» чем одна функция $h$ приближает с такой же точностью немонотонную в общем случае булеву функцию $f$ в (16), так как для конкретного $\boldsymbol{x}$ не известно совпадает вычисленное значение $h(\boldsymbol{x})$ с $f(\boldsymbol{x})$ или нет, в то время как пара значений $f_m(\boldsymbol{x})$ и $f_M(\boldsymbol{x})$ позволяет это сделать для каждого $\boldsymbol{x}$.

**3.** Сложность приближенного вычисления монотонных булевых функций оценивается в следующей теореме.

**Теорема 2**. *При $n \to \infty$ и $n^{-1/2} \ll \varepsilon < 1$ любая монотонная $n$-местная булева функция может быть вычислена с точностью $1 - \varepsilon$ и сложностью, не превосходящей*

$$\frac{2^n}{n\sqrt{\pi n/2}} \cdot 2^{-\varepsilon\sqrt{n}}.$$

Доказательство теоремы существенным образом опирается на верхнюю оценку количества непостоянных интервалов произвольной монотонной буле-

вой функции. Дадим необходимые определения и получим требуемую оценку, являющуюся некоторым аналогом упоминавшейся выше теоремы Шпернера.

Пусть $\boldsymbol{\alpha}, \boldsymbol{\beta} \in B^n$, $\boldsymbol{\alpha} \preceq \boldsymbol{\beta}$, $d(\boldsymbol{\alpha}, \boldsymbol{\beta}) = k$ и $\boldsymbol{i} = (i_1, i_2, \ldots, i_k)$, где $\alpha_{i_j} \neq \beta_{i_j}$. Множество $I(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \{\boldsymbol{\gamma} \,|\, \boldsymbol{\alpha} \preceq \boldsymbol{\gamma} \preceq \boldsymbol{\beta}\}$ вершин $n$-мерного булева куба называется интервалом размерности $k$, проходящим в направлении $\boldsymbol{i}$. Интервал $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$ назовем непостоянным, если $f(\boldsymbol{\alpha}) = 0$ и $f(\boldsymbol{\beta}) = 1$. Будем говорить, что максимальная цепь $\boldsymbol{\alpha}_0, \ldots, \boldsymbol{\alpha}_n$ проходит через интервал $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$, если $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \{\boldsymbol{\alpha}_0, \ldots, \boldsymbol{\alpha}_n\}$.

**Лемма 3**. *Для любой $n$-местной монотонной булевой функции число непостоянных интервалов размерности $k$ не превосходит*

$$k\binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}.$$

**Доказательство.** Пусть $N$ — множество всех непостоянных интервалов $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$ размерности $k$, а $N_s$ — его подмножество, состоящее из всех тех интервалов $I(\boldsymbol{\alpha}, \boldsymbol{\beta})$, в которых вершина $\boldsymbol{\alpha}$ лежит в $s$-м слое. Если $I(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in N_s$, то через этот интервал проходит ровно $s!k!(n-k-s)!$ максимальных цепей. Так как в $n$-мерном булевом кубе существует ровно $n!$ различных максимальных цепей и каждая максимальная цепь проходит не более чем через $k$ непостоянных интервалов размерности $k$, то

$$k \cdot n! \geqslant \sum_{s=0}^{n-k} s!k!(n-k-s)!|N_s| = \sum_{s=0}^{n-k} \frac{s!k!(n-k-s)!n!(n-k)!|N_s|}{n!(n-k)!} =$$

$$= n!\Big(\sum_{s=0}^{n-k} |N_s| \Big/ \binom{n}{k}\binom{n-k}{s}\Big) \geqslant n!|N| \Big/ \binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}.$$

Следовательно, $|N| \leqslant k\binom{n}{k}\binom{n-k}{\lfloor (n-k)/2 \rfloor}$. Лемма доказана.

Так как в $n$-мерном кубе интервал размерности $k$ может проходить в одном из $\binom{n}{k}$ возможных направлений, то из леммы 3 легко извлекается следующий результат.

**Лемма 4**. *Для любой $n$-местной монотонной булевой функции найдется направление $\boldsymbol{i}$, в котором проходит не более*

$$k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$$

*непостоянных интервалов размерности $k$.*

Пусть $\boldsymbol{i} = (i_1, i_2, \ldots, i_k)$ и $\boldsymbol{\alpha} = (\alpha_1 \alpha_2 \ldots \alpha_k)$. Символом $f_{\boldsymbol{i}}^{\boldsymbol{\alpha}}(\boldsymbol{x})$ обозначим $n$-местную функцию с $k$ фиктивными переменными, получающуюся из $n$-местной булевой функции $f$ подстановкой констант $\alpha_j$ вместо ее $i_j$-х аргументов, а символом $\boldsymbol{x}_{\boldsymbol{i}}^{\boldsymbol{\alpha}}$ — булев набор длины $n$, у которого $i_j$-е разряды равны величинам $\alpha_j$.

**Лемма 5**. *Для любой $n$-местной монотонной булевой функции $f$ найдется такой набор $\boldsymbol{i}$ длины $k$, что $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ не более чем для $k2^k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ различных наборов $\boldsymbol{x}$ длины $n$.*

**Доказательство.** Если $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{\gamma}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{\gamma})$ для некоторого $\boldsymbol{\gamma}$, то этот набор $\boldsymbol{\gamma}$ лежит в непостоянном интервале $I(\boldsymbol{\gamma}_{\boldsymbol{i}}^{\boldsymbol{0}}, \boldsymbol{\gamma}_{\boldsymbol{i}}^{\boldsymbol{1}})$. При этом аналогичное неравенство $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ будет справедливо для всех $2^k$ наборов $\boldsymbol{x}$ длины $n$ из интервала $I(\boldsymbol{\gamma}_{\boldsymbol{i}}^{\boldsymbol{0}}, \boldsymbol{\gamma}_{\boldsymbol{i}}^{\boldsymbol{1}})$. Поэтому число наборов, удовлетворяющих неравенству $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$, равно умноженному на $2^k$ числу непостоянных интервалов размерности $k$, проходящих в направлении $\boldsymbol{i}$. Следовательно, для направления $\boldsymbol{i}$, в котором у функции $f$ проходит не более $k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ непостоянных интервалов размерности $k$, найдется не более чем $k2^k\binom{n-k}{\lfloor (n-k)/2 \rfloor}$ различных наборов $\boldsymbol{x}$ длины $n$, для которых $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$. Лемма доказана.

Воспользуемся формулой Стирлинга и преобразуем лемму 5 в следующее утверждение.

**Лемма 6**. *При $n \to \infty$ и $k = o(n)$ для любой $n$-местной монотонной булевой функции $f$ найдется такой набор $\boldsymbol{i}$ длины $k$, что $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \neq f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ не более чем для*

$$\frac{k \cdot 2^n}{\sqrt{\pi n/2}}(1 + o(1))$$

*различных наборов $\boldsymbol{x}$ длины $n$.*

Заметим, что $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x}) \leqslant f(x) \leqslant f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$. Поэтому функции $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x})$ и $f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ являются хорошими кандидатами для приближенного вычисления $f(\boldsymbol{x})$.

**Доказательство теоремы 2.** Положим $k = \lfloor \varepsilon\sqrt{3n/2} \rfloor$. Тогда начиная с некоторого $n$ справедливо неравенство $k \geqslant \varepsilon\sqrt{n} + 1$. Пусть $\boldsymbol{i}$ — набор длины $k$, существующий в силу леммы 6. Из этой леммы следует, что значения функций $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x})$ и $f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ не совпадают не более чем на

$$\frac{\varepsilon\sqrt{3n/2} \cdot 2^n}{\sqrt{\pi n/2}}(1 + o(1)) \leqslant \varepsilon \cdot 2^n$$

наборах $\boldsymbol{x}$ длины $n$. Так как функции $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x})$ и $f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ имеют по $n - k$ существенных переменных, то в силу (5) сложность их совместного вычисления асимптотически не превосходит

$$\frac{2 \cdot 2^{n-k}}{(n-k)\sqrt{\pi(n-k)/2}} \sim \frac{2^n}{n\sqrt{\pi n/2}} \cdot 2^{-\varepsilon\sqrt{n}}.$$

Таким образом, функции $f_{\boldsymbol{i}}^{\boldsymbol{0}}(\boldsymbol{x})$ и $f_{\boldsymbol{i}}^{\boldsymbol{1}}(\boldsymbol{x})$ приближенно вычисляют функцию $f(\boldsymbol{x})$ с требуемыми точностью и сложностью. Теорема доказана.

Заметим, что из неравенства (8) и основного результата работы Л. А. Шоломова [8] легко следует, что при $\varepsilon \ll n^{-1/2}$ сложность приближенного вычисления почти каждой $n$-местной монотонной булевой функции не может быть асимптотически меньше $\frac{2^n}{n\sqrt{\pi n/2}}$.

## 4. Средняя сложность

**1.** Снова обратимся к свойству (15). Из этого свойства следует простой «в среднем» способ вычисления почти каждой $n$-местной монотонной функции $f(\boldsymbol{x})$ в случае, когда возможно досрочное прекращение вычислений. Сделать это можно в два этапа следующим образом. Сначала, как и при приближенном вычислении, для каждого $\boldsymbol{x}$ из $B^n$ надо воспользоваться схемой сложности $\mathcal{O}(n)$ для вычисления значений симметрических пороговых функций с порогами $\lfloor n/2-3\rfloor$ и $\lceil n/2+3\rceil$. Если значения этих функций на наборе $\boldsymbol{x}$ совпадут и будут равны $\alpha$, то вычисления прекращаются, так как $f(\boldsymbol{x})=\alpha$. Если значения пороговых функций не совпадают, то набор $\boldsymbol{x}$ лежит между $\lfloor n/2-3\rfloor$-м и $\lceil n/2+3\rceil$-м слоями и принадлежит множеству из $\mathcal{O}\left(2^n/\sqrt{n}\right)$ наборов. Для вычисления $f$ на каждом таком наборе можно воспользоваться схемой, сложность которой есть $\mathcal{O}(2^n/n\sqrt{n})$. Нетрудно видеть, что в среднем число элементарных операций, выполненных для вычисления значения $f$ на одном наборе, определяется следующим выражением

$$\frac{1}{2^n}\left(\mathcal{O}(n\cdot 2^n)+\mathcal{O}\left(\frac{2^n}{n\sqrt{n}}\cdot\frac{2^n}{\sqrt{n}}\right)\right)=\mathcal{O}\left(\frac{2^n}{n^2}\right)=o\left(\frac{2^n}{n\sqrt{n}}\right).$$

Далее покажем, что при $n\to\infty$ аналогичная оценка «в среднем» справедлива для каждой $n$-местной монотонной булевой функции.

**2.** Пусть $\mathcal{B}$ — подмножество множества всех не более чем двуместных булевых функций. Неветвящейся программой с условной остановкой $\mathsf{P}$ в базисе $\mathcal{B}$ над множеством независимых булевых переменных $X=\{x_1,\ldots,x_n\}$ называется список $\mathsf{p}_1,\ldots,\mathsf{p}_L$ последовательно выполняемых команд двух видов — вычислительных команд и команд остановки. Если $\mathsf{p}_i$ — вычислительная команда, то она присваивает внутренней переменной $y_i$ значение $f_i(z_1,z_2)$, где $f_i\in\mathcal{B}$ и $z_1,z_2\in X\bigcup\{y_1,\ldots,y_{i-1}\}$. Если $\mathsf{p}_i$ — команда остановки $\mathtt{Stop}(z_1,z_2)$, где $z_1,z_2\in X\bigcup\{y_1,\ldots,y_{i-1}\}$, то эта команда останавливает вычисления, если $z_1=1$, и объявляет результатом работы значение $z_2$. Если $z_1=0$, то выполняется следующая команда программы. Если ни одна команда остановки не остановила программу, то ее значением объявляется значение последней внутренней переменой. Число команд называется сложностью программы $C(\mathsf{P})$. Величина

$$T(\mathsf{P})=2^{-n}\sum_{\boldsymbol{x}\in B^n}T_{\mathsf{P}}(\boldsymbol{x}),$$

где $T_{\mathsf{P}}(\boldsymbol{x})$ — число команд, выполненных программой на наборе $\boldsymbol{x}$ до ее остановки, называется средним временем работы программы $\mathsf{P}$. Если для булевой

функции $f$ и любого двоичного набора $\boldsymbol{x}$ справедливо равенство $f(\boldsymbol{x}) = \mathsf{P}(\boldsymbol{x})$, то будем говорить, что программа $\mathsf{P}$ вычисляет функцию $f$. Величину

$$T_{\mathcal{B}}(f) = \min T(\mathsf{P}),$$

где минимум берется по всем программам, вычисляющим $f$ в базисе $\mathcal{B}$, назовем средней сложностью функции $f$ в этом базисе. Программу $\mathsf{P}$, вычисляющую функцию $f$, для которой справедливо равенство $T(\mathsf{P}) = T_{\mathcal{B}}(f)$, назовем минимальной программой.

Далее будем рассматривать только программы с базисом, состоящим из всех двуместных булевых функций. Поэтому символ базиса в формулах будем опускать.

**3.** Из результатов работы [9] следует, что для средней сложности каждой $n$-местной булевой функции $f$ справедливо неравенство

$$T(f) = \mathcal{O}\left(\frac{2^n}{n}\right), \tag{17}$$

а при $n \to \infty$ аналогичная нижняя оценка

$$T(f) = \Omega\left(\frac{2^n}{n}\right) \tag{18}$$

справедлива для почти каждой $n$-местной булевой функции.

Среднюю сложность монотонных булевых функций изучал Р. Н. Забалуев. В его опубликованной в 2006 году работе [10] доказаны аналоги неравенств (17) и (18) для средней сложности монотонных функций, из которых в частности следует, что для каждой $n$-местной монотонной функции $f$

$$T(f) = \mathcal{O}\left(\frac{2^n}{n^2}\right), \tag{19}$$

а при $n \to \infty$ для почти каждой $n$-местной монотонной булевой функции $f$

$$T(f) = \Omega\left(\frac{2^n}{n^2}\right). \tag{20}$$

**4.** В следующей теореме установим справедливость неравенства (19). Сделаем это, упростив соответствующее доказательство из [10] и уменьшив извлекаемый из этого доказательства постоянный множитель в «$\mathcal{O}$».

**Теорема 3**. *При $n \to \infty$ для любой $n$-местной монотонной булевой функции $f$*

$$T(f) \leqslant \frac{12 \cdot 2^n}{\pi n^2}(1 + o(1)).$$

**Доказательство.** Пусть $n \to \infty$. Положим $s = \lceil \log_2 \log_2 n \rceil$. В силу леммы 6 для любого $k \in \{1, \ldots, s\}$ найдется такой набор $\boldsymbol{i}_k$ длины $2^k$, что $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{y}) \neq f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{y})$ не более чем для

$$\frac{2^k \cdot 2^n}{\sqrt{\pi n/2}}(1 + o(1)) \tag{21}$$

различных наборов $\boldsymbol{y}$ длины $n$. Пусть $A_k$ — множество всех таких наборов, $A_{s+1} = B^n$. Нетрудно видеть, что функция $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x}) \oplus f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ будет характеристической функцией множества $A_k$, и что функции $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ можно вычислить схемой, сложность которой в силу (5) не превосходит

$$\frac{2 \cdot 2^{n-2^k}}{(n-2^k)\sqrt{\pi(n-2^k)/2}}(1 + o(1)) = \frac{2^{n-2^k+1}}{n\sqrt{\pi n/2}}(1 + o(1)). \tag{22}$$

Вычисляющую функцию $f(\boldsymbol{x})$ программу $\mathsf{P}$ представим в виде последовательности подпрограмм

$$\mathsf{P} = \mathsf{P}_s \mathsf{P}_{s-1} \ldots \mathsf{P}_k \ldots \mathsf{P}_1 \mathsf{P}_0.$$

Здесь для $k = s, \ldots, 1$ каждая подпрограмма $\mathsf{P}_k$ выполняет следующие действия: 1) вычисляет значения функций $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})$ и $f^{\mathbf{1}}_{\boldsymbol{i}_k}(x)$; 2) объявляет значением программы значение $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x})$; 3) останавливает вычисления, если $f^{\mathbf{0}}_{\boldsymbol{i}_k}(\boldsymbol{x}) = f^{\mathbf{1}}_{\boldsymbol{i}_k}(\boldsymbol{x})$. Подпрограмма $\mathsf{P}_0$ является схемой, вычисляющей $f(\boldsymbol{x})$.

Так как в программе $\mathsf{P}$ каждая подпрограмма $\mathsf{P}_k$ работает только на наборах множества $A_{k+1}$, то

$$T(\mathsf{P}) = 2^{-n} \sum_{k=s}^{0} |A_{k+1}| C(\mathsf{P}_k). \tag{23}$$

В силу (21), (22) и неравенства $k+1 \leqslant 2^k - k + 1$ слагаемые в (23) удовлетворяют неравенствам

$$\begin{aligned}
|A_{s+1}| C(\mathsf{P}_s) &\lesssim 2^n \cdot \frac{2^{n-2^s+1}}{n\sqrt{\pi n/2}} \leqslant \frac{2^{2n+1}}{\pi n^2 \sqrt{\pi n/2}}, \\
|A_{k+1}| C(\mathsf{P}_k) &\lesssim \frac{2^{k+1} \cdot 2^n}{\sqrt{\pi n/2}} \cdot \frac{2^{n-2^k+1}}{n\sqrt{\pi n/2}} \leqslant \frac{2^{2n+3-k}}{\pi n^2}, \ k = 1, \ldots, s-1 \\
|A_1| C(\mathsf{P}_0) &\lesssim \frac{2 \cdot 2^n}{\sqrt{\pi n/2}} \cdot \frac{2^n}{n\sqrt{\pi n/2}} \leqslant \frac{2^{2n+2}}{\pi n^2}.
\end{aligned} \tag{24}$$

Таким образом, из (23) и (24) следует, что

$$T(\mathsf{P}) \lesssim \frac{2^{n+1}}{n^2\sqrt{\pi n/2}} + \sum_{k=s-1}^{1} \frac{2^{n+3-k}}{\pi n^2} + \frac{2^{n+2}}{\pi n^2} \sim \frac{12 \cdot 2^n}{\pi n^2}.$$

Теорема доказана.

Теперь докажем справедливость неравенства (20), т. е. покажем, что установленная в предыдущей теореме верхняя оценка точна по порядку. Пусть $f$ — булева функция, $\mathsf{P}$ — программа, вычисляющая $f$. Каждому двоичному набору $\boldsymbol{x}$ длины $n$, рассматриваемому как двоичная запись натурального числа, поставим в соответствие его номер $N_{\mathsf{P}}(\boldsymbol{x})$ такой, что $1 \leqslant N_{\mathsf{P}}(\boldsymbol{x}) \leqslant 2^n$; $N_{\mathsf{P}}(\boldsymbol{x}) < N_{\mathsf{P}}(\boldsymbol{y})$, если $T_{\mathsf{P}}(\boldsymbol{x}) < T_{\mathsf{P}}(\boldsymbol{y})$; $N_{\mathsf{P}}(\boldsymbol{x}) < N_{\mathsf{P}}(\boldsymbol{y})$, если $T_{\mathsf{P}}(\boldsymbol{x}) = T_{\mathsf{P}}(\boldsymbol{y})$ и $\boldsymbol{x} < \boldsymbol{y}$.

**Теорема 4** [10]. *При $n \to \infty$ для почти всех $n$-местных монотонных булевых функций $f$ справедливо неравенство*

$$T(f) \gtrsim \frac{2^n}{4\pi n^2}.$$

**Доказательство.** Пусть $f$ — $n$-местная монотонная булева функция, $\mathsf{P}$ — минимальная программа, вычисляющая $f$. Пусть $\boldsymbol{x}_0$ такое, что $N_{\mathsf{P}}(\boldsymbol{x}_0) = 2^n - \frac{2^n}{2\sqrt{\pi n/2}}$. Оценим число $n$-местных монотонных булевых функций, у минимальных программ которых

$$T_{\mathsf{P}}(\boldsymbol{x}_0) \leqslant \frac{(1-2\varepsilon)\cdot 2^n}{4n\cdot\sqrt{\pi n/2}}, \tag{25}$$

где $\varepsilon$ — сколь угодно малая положительная постоянная. Каждая такая функция однозначно определяется первыми $T_{\mathsf{P}}(\boldsymbol{x}_0)$ командами своей минимальной программы и двоичным вектором длины не более чем $2^n - N_{\mathsf{P}}(\boldsymbol{x}_0) = \frac{2^n}{2\sqrt{\pi n/2}}$ — значениями на тех аргументах, время работы на которых больше времени работы на $\boldsymbol{x}_0$. Легко видеть, что для числа $N_0$, равного числу различных программ, сложность которых не превосходит $T_{\mathsf{P}}(\boldsymbol{x}_0)$, справедливо неравенство

$$N_0 \leqslant \left(c_1\left(T_{\mathsf{P}}(\boldsymbol{x}_0)+n\right)\right)^{2T_{\mathsf{P}}(\boldsymbol{x}_0)},$$

из которого при $n \to \infty$ после подстановки (25) и несложных преобразований получаем оценку

$$N_0 \leqslant \left(c_1\left(\frac{(1-2\varepsilon)\cdot 2^n}{4n\cdot\sqrt{\pi n/2}}+n\right)\right)^{\frac{2(1-2\varepsilon)2^n}{4n\sqrt{\pi n/2}}} \leqslant 2^{\frac{(1-2\varepsilon)2^n}{2\sqrt{\pi n/2}}}.$$

Следовательно, $M$ — число рассматриваемых функций, не превосходит величины

$$2^{\frac{(1-2\varepsilon)2^n}{2\sqrt{\pi n/2}}}\cdot 2^{\frac{2^n}{2\sqrt{\pi n/2}}} = 2^{\frac{(1-\varepsilon)2^n}{\sqrt{\pi n/2}}} = o\left(M(n)\right).$$

Из полученной оценки величины $M$ видно, что все минимальные программы почти всех $n$-местных монотонных функций удовлетворяют условию:

$$\text{если } \boldsymbol{x}_0 \text{ такое, что } N_{\mathsf{P}}(\boldsymbol{x}_0) = 2^n - \frac{2^n}{2\sqrt{\pi n/2}}, \text{ то } T_{\mathsf{P}}(\boldsymbol{x}_0) > \frac{(1-2\varepsilon)\cdot 2^n}{4n\cdot\sqrt{\pi n/2}}.$$

Поэтому для среднего времени работы каждой такой программы справедлива оценка

$$T(\mathsf{P}) = 2^{-n} \sum_{\boldsymbol{x}\in B^n} T_{\mathsf{P}}(x) \geqslant 2^{-n} \sum_{\boldsymbol{x}\,|\,N_{\mathsf{P}}(\boldsymbol{x})\geqslant N_{\mathsf{P}}(\boldsymbol{x}_0)} T_{\mathsf{P}}(\boldsymbol{x}) \geqslant$$
$$\geqslant 2^{-n} \cdot \frac{(1-2\varepsilon)\cdot 2^n}{4n\cdot\sqrt{\pi n/2}} \cdot \frac{2^n}{2\sqrt{\pi n/2}} = \frac{(1-2\varepsilon)\cdot 2^n}{4\pi n^2},$$

из которой, в силу произвольной малости $\varepsilon$, следует утверждение теоремы. Теорема доказана.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 14–01–00598.

### Литература


**1.** Ансель Ж. О числе монотонных булевых функций $n$ переменных // Кибернетический сборник. Новая серия. Вып. 5. — М.: Мир, 1968. С. 53–63.

**2.** Клейтмен Д. О проблеме Дедекинда: число монотонных булевых функций // Кибернетический сборник. Новая серия. Вып. 7. — М.: Мир, 1970. С. 43–52.

**3.** Коршунов А. Д. О числе монотонных булевых функций // Проблемы кибернетики. Вып. 38. — М.: Наука, 1981. С. 5–108.

**4.** Редькин Н. П. О реализации монотонных функций контактными схемами // Проблемы кибернетики. Вып. 35. — М.: Наука, 1979. С. 87–110.

**5.** Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 31. — М.: Наука, 1976. С. 167–185.

**6.** Андреев А. Е. О синтезе схемам из функциональных элементов в полных монотонных базисах // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. С. 114–139.

**7.** Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. С. 31–110.

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

**9.** Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. Серия 1. — 1997. — Т. 4, вып. 1. — С. 60–78.

**10.** Забалуев Р. Н. О средней сложности монотонных функций // Дискретная математика. — 2006. — Т. 18, вып. 2. — С. 71–83.

# СОДЕРЖАНИЕ