

Нижние оценки сложности схем

Ю. А. Комбаров

Задача данной работы — познакомить читателя с основными приемами, используемыми при доказательстве нижних оценок сложности схем из функциональных элементов. Работа носит учебно-методический характер и может рассматриваться как учебное пособие по курсу «Элементы теории сложности схем». Работа самодостаточна, от читателя требуется лишь знакомство с базовыми определениями дискретной математики и теории дискретных функций.

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 $\{x_1, \dots, x_n, \dots\}$. 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* S будем 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 от n переменных экспоненциально велика с вероятностью, стремящейся к единице. Строго это утверждение сформулировано в следующей теореме.

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

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

где ρ_B — константа, зависящая только от базиса B . Кроме того, среди всех функций от n переменных доля функций f , таких, что $L_B(f) < \rho_B \frac{2^n}{n}$, 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 $L_B(f_n) \geq \rho_B \frac{2^n}{n}$. 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 какого-то 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 B_1, B_2 существуют константы C_1, C_2 , такие, что для любой функции f верно, что $C_1 L_{B_1}(f) \leq L_{B_2}(f) \leq C_2 L_{B_1}(f)$. 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.

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: $x \& y$, $x \vee y$, $\bar{x} \& y$, $\bar{x} \vee y$, $\overline{x \& y}$, $\overline{x \vee y}$.
3. Функции менее, чем двух переменных: x , $\bar{x}$, 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 $\bar{x} \vee y$ забивающая константа — ноль.

Легко убедиться в том, что любую схему можно преобразовать, избавившись от всех двухвходовых 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 $E_1, \dots, E_k$ 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 $E_1, \dots, E_k$.

Если элементу E приписана функция $\bar{x}$, то E можно удалить, соединить v с освободившимися входами элементов $E_1, \dots, E_k$, а функции, приписанные элементам $E_1, \dots, E_k$ 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 $\bar{x} \vee y$).

Наконец, пусть E реализует константу. Выберем $i \in \{1, \dots, k\}$. 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 $E_1, \dots, E_k$ выход элемента E больше не будет подаваться на входы элементов, и его можно будет удалить из схемы. $\square$

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 одноходовым либо может быть заменен на одноходовой, и применим утверждение 1. $\square$

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

Нижние оценки в базисе B_2

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

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

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

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. $\square$

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 $f(x_1, \dots, x_n)$ принадлежит классу $Q_{2,3}^{(n)}$, если выполнены условия:

1. Для любых i и j среди подфункций $f|_{x_i=0, x_j=0}$, $f|_{x_i=0, x_j=1}$, $f|_{x_i=1, x_j=0}$ и $f|_{x_i=1, x_j=1}$ найдется хотя бы три различных.
2. $\forall i \exists c \in \{0, 1\} : f|_{x_i=c} \in Q_{2,3}^{(n-1)}$ (при $n \geq 3$).

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 $MOD_{3,i}^n$ (здесь $i \in \{0, 1, 2\}$) следующим образом:

$$MOD_{3,i}^n(x_1, \dots, x_n) = 1 \Leftrightarrow x_1 + \dots + x_n = i \pmod{3}.$$

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

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

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

Доказательство. Пусть S_n — минимальная схема, реализующая функцию f_n из класса $Q_{2,3}^{(n)}$. 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 $f_n(x_1, x_2, \dots, x_n) = g(x_1 \circ x_2, x_3, \dots, x_n)$.

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 $g(0, x_3, \dots, x_n)$ и $g(1, x_3, \dots, x_n)$). Это противоречит тому, что f_n лежит в классе $Q_{2,3}^{(n)}$.

Без ограничения общности будем считать, что степень x_1 больше или равна двум. Подадим на вход x_1 константу c такую, что $f_n|_{x_1=c} \in Q_{2,3}^{(n-1)}$ (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 $Q_{2,3}^{(n-1)}$, причем $L(S_n) - L(S_{n-1}) \geq 2$.

Со схемой S_{n-1} проведем аналогичное преобразование: удалим из нее не менее двух элементов, получив схему, реализующую функцию из $Q_{2,3}^{(n-2)}$. Процесс удаления элементов можно повторить $n - 2$ раза (столько, сколько констант можно подать вместо переменных функции из $Q_{2,3}^{(n)}$, 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 $L(S_n) \geq 2n - 4$. $\square$

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 $L(f_n) \geq dn - C$, 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 $f(x_1, \dots, x_n)$ — булева функция. *Полином Жегалкина* для функции f — представление f в виде

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

где коэффициенты $c_{i_1, \dots, i_k}$ и c_0 выбираются из множества $\{0, 1\}$. Известно [8], что набор коэффициентов полинома определяется по булевой функции однозначно. *Степень* 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 $M(f) \geq \deg f - 1$.

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 $f(x_1, \dots, x_n)$ принадлежит классу $R_{2,3}^{(n)}$, если выполнены условия:

1. Для любых i и j среди подфункций $f|_{x_i=0, x_j=0}$, $f|_{x_i=0, x_j=1}$ и $f|_{x_i=1, x_j=1}$ найдется хотя бы три различных.
2. $\forall i \forall c \in \{0, 1\} : f|_{x_i=c} \in R_{2,3}^{(n-1)}$ (при $n \geq 3$).

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 $f_n(x_1, \dots, x_n)$ — последовательность булевых функций, $f_n \in R_{2,3}^n$ и $\deg f_n = n - C$, где C — константа. Тогда

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

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 $\mu(S) \geq 6n - 12$. Для этого проверим, что из любой схемы, реализующей функцию из $R_{2,3}^{(n)}$ (при $n \geq 3$), можно удалить несколько элементов так, что новая схема будет

реализовывать функцию из $R_{2,3}^{(n-1)}$, а значение меры μ уменьшится не менее, чем на шесть.

Пусть S — схема, реализующая функцию f из $R_{2,3}^{(n)}$. Удалим из нее все одноводовые элементы согласно утверждению 1 (значение $\mu(S)$ при этом, очевидно, не увеличится). Далее, пусть E_2 — двухводовой 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 μ не менее, чем на шесть.

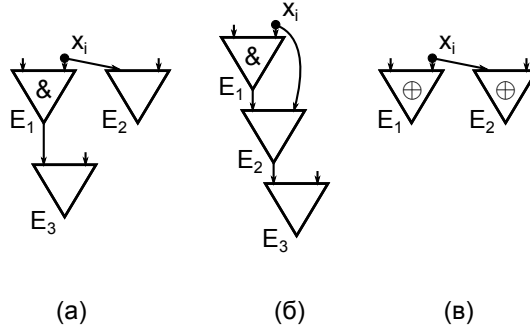


Рис. 1

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 $x\phi$, где x — переменная, ϕ — булева функция, $n \geq 3$). 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 μ на шесть.

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

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 $MOD_{3,0}^n$.

Утверждение 4. Для любого $i \in \{0, 1, 2\}$, $n \geq 3$ верно, что $MOD_{3,i}^n \in R_{2,3}^{(n)}$ и $\deg MOD_{3,i}^n \geq n - 1$

Доказательство. Принадлежность функций $MOD_{3,i}^n$ классу $R_{2,3}^{(n)}$ обосновывается так же, как и принадлежность классу $Q_{2,3}^{(n)}$. 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 — $\text{wt } f$). Заметим, что среди функций $MOD_{3,0}^n, MOD_{3,1}^n, MOD_{3,2}^n$ есть ровно две функции нечетного веса. Для $n = 3$ это проверяется непосредственно, а для больших n доказывается по индукции с учетом равенства $\text{wt } MOD_{3,i}^n = \text{wt } MOD_{3,i}^{n-1} + \text{wt } MOD_{3,i-1}^{n-1}$ (здесь $i - 1$ берется по модулю три). Значит, среди функций $MOD_{3,0}^n, MOD_{3,1}^n, MOD_{3,2}^n$ две имеют степень n , а третья имеет подфункцию $n - 1$ переменной степени $n - 1$ (и, следовательно, имеет степень $n - 1$). $\square$

Высокие нижние оценки сложности доказаны для различных обобщений функции выбора.

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

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

(здесь через $|\tilde{a}|$ обозначается число, двоичной записью которого является набор $(a_1, \dots, a_{\log n})$). Переменные $a_1, \dots, a_{\log n}$ называются *адресными* переменными функции SA_n , а переменные $x_1, \dots, x_n$ — *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 $n + 2 \log n + 1$ переменных определена следующим образом:

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

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

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 удастся: 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]). $L_{B_2}(SA'_n) \geq 2n - 2$.

Доказательство. Отметим, что теорему 5 легко доказать методом забывающих констант или вывести из нижней оценки $L_{B_2}(SA_n) \geq 2n - 2$, 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 функцию, существенно зависящую от n переменных и содержащую m ветвящихся вершин, верно, что

$$L(S) \geq n + m - 1. \quad (1)$$

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 .

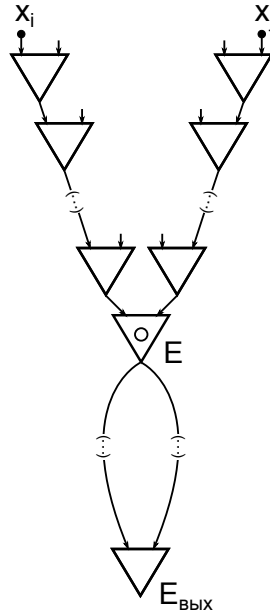


Рис. 2

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 $x_i, \bar{x}_i, 0, 1$, а элементы второго пути выше E — одну из функций $x_j, \bar{x}_j, 0, 1$. 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 $x \& y$ не 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 $v_1, \dots, v_{n-1}$ — 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 пути пересекаются, что невозможно.

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

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

$$SA''_n(\tilde{a}, \tilde{b}, \tilde{c}, p, q, r, x_1, \dots, x_n) = q(x_{|\tilde{a}|} x_{|\tilde{b}|} \vee p x_{|\tilde{b}|} x_{|\tilde{c}|}^r) \vee \bar{q}(x_{|\tilde{a}|} \oplus x_{|\tilde{b}|})$$

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

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 $f(x_1, \dots, x_n)$ называется *аффинным дисперсером* размерности d , если она не постоянна на любом аффинном 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 $IP(x_1, \dots, x_{n/2}, y_1, \dots, y_{n/2}) = x_1 y_1 \oplus \dots \oplus x_{n/2} y_{n/2}$, 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 $\Theta(n^{4/5})$. 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 $\mathbb{F}_{2^m}^r$, где $\mathbb{F}_{2^m}$ — конечное поле из 2^m элементов (т.е. набор из n единиц делится на r блоков по m единиц в каждом, и каждый блок интерпретируется как элемент $\mathbb{F}_{2^m}$). Определим функцию

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

где $x_1, \dots, x_r$ — элементы $\mathbb{F}_{2^m}$, $\text{Sym}_r^t(y_1, \dots, y_r) = \sum_{1 \leq i_1 < \dots < i_t \leq r} y_{i_1} \dots y_{i_t}$ — t -ый симметрический многочлен, $\text{Tr } y = y + y^2 + y^4 + \dots + y^{2^{m-1}}$ — 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 $\Theta(n^{4/5})$.

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 $L_{B_2}(f_n) \geq 3n - o(n)$.

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 оценки 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 $L_{B_2}(f_n) \geq (3 + \frac{1}{86})n - o(n)$.

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 $E_1, \dots, E_k, x_1, \dots, x_n$ (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 $x_1, \dots, x_n$ значения переменных $E_1, \dots, E_n$

определяются однозначно, то такая схема считается правильной; значение, реализуемое элементом E_i на наборе $\sigma_1, \dots, \sigma_n$ определяется как значение переменной E_i в системе при подставленных значениях $\sigma_1, \dots, \sigma_n$ вместо $x_1, \dots, x_n$. Если же при каких-то значениях переменных $x_1, \dots, x_n$ 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 $x_i = \phi(x_1, \dots, x_n)$ 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 $x_i = \phi(x_1, \dots, x_n)$. 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).

Нижняя оценка теоремы 8 улучшена в работе [18] до $3.1n - o(n)$ в 2021 г.

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 $l(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$. 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 рисунке 3. Два верхних элемента в схеме на рисунке реализуют функции $\bar{x} \& y$ и $x \& \bar{y}$.

Чтобы получить нижнюю оценку, докажем, что из любой схемы в базисе U_2 , реализующей l_n или $\bar{l}_n$, можно удалить три элемента, получив

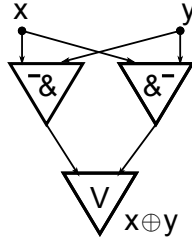


Рис. 3

схему, реализующую l_{n-1} или $\bar{l}_{n-1}$. 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 x_i — такой вход. Пусть единственный элемент, со входом которого соединен этот вход — элемент E . Пусть на второй элемент подается функция ϕ . Так как схема по определению не содержит циклов, функция ϕ не зависит от x_i . Поэтому мы можем подобрать значения остальных переменных (кроме переменной x_i), такие, что функция ϕ 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 $\bar{l}_n$. 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).

□

Если провести перебор различных конфигураций элементов, которые могут быть в верхней части схемы, более аккуратно, с помощью метода забивающих констант можно доказать следующее утверждение, усиливающее теорему 9.

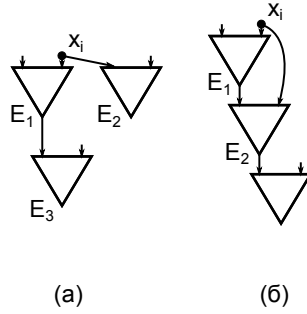


Рис. 4

Теорема 10 ([19]). *Всякая минимальная схема в базисе U_2 , реализующая l_n или $\bar{l}_n$ 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 рисунке 4). Более точно, всякая минимальная схема для l_n или $\bar{l}_n$ является двоичным деревом, в листьях которого расположены входы схемы, а во внутренних вершинах — трехэлементные блоки.*

Аналогичные утверждения доказаны и для ряда других базисов [20, 21].

Более высокая нижняя оценка была доказана Цвиком в 1991 году.

Теорема 11 ([22]). $L_{U_2}(MOD_{3,0}^n) \geq 4n - 9$.

Отметим, что в работе [22] 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 $f(x_1, \dots, x_n)$ 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 [23] с использованием нетривиального утверждения о суммах подмножеств конечного поля $\mathbb{F}_p$. Для таких функций в 2002 году была доказана следующая нижняя оценка.

Теорема 12 ([24]). *Пусть f является $(n, o(n))$ -сильно-2-зависимой. Тогда $L_{U_2}(f) \geq 5n - o(n)$.*

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

В работе [25] 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 [26] составляет $n^{(3-o(1))}$, а для контактных схем известна [27] 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 [28] и для схем в неполном базисе $\{\&, \vee\}$ [29]. 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 [30, 31], использованные при подготовке этой работы.

Список литературы

- [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. — 1984. — вып. 21. — 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. — 1979. — 16. — 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] Li J., Yang T. $3.1n - o(n)$ Circuit Lower Bounds for Explicit Functions. // ECCC. — 2021.
- [19] Комбаров Ю. А. О минимальных схемах для линейных функций в некоторых базисах // Дискретная математика. — 2013. — 25, 1. — С. 33–44.
- [20] Комбаров Ю. А. О минимальных реализациях линейных булевых функций // Дискретный анализ и исследование операций. — 2012. — 19, 3. — С. 39–57.
- [21] Комбаров Ю. А. О минимальных схемах в базисе Шеффера для линейных булевых функций // Дискретный анализ и исследование операций. — 2013. — 20, 4. — С. 65–87.
- [22] 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.

- [23] Savicky P., Zack S. A large lower bound for 1-branching programs // ECCC rep. No 96-030. — 1996.
- [24] 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.
- [25] 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.
- [26] Hastard J. The Shrinkage Exponent of de Morgan Formulas is 2 // SIAM J. Comput. — 1998. — 27(1). — P. 48–64.
- [27] Ничепорук Э.И. Об одной булевской функции // Докл. АН СССР. — 1966. — 196(4). — С. 765–766.
- [28] Furst M., Saxe J., Sipster M. Parity, circuits and the polynomial time hierarchy // Mathematical Systems theory. — 1984. — 17. — P. 13–27.
- [29] А. А. Разборов Нижние оценки монотонной сложности логического перманента // Матем. заметки. — 1985. — 37(6). — С. 887–900.
- [30] Сэвидж Дж. Сложность вычислений. — М.: Факториал, 1998.
- [31] Wegener I. The complexity of Boolean functions — Teubner, Stuttgart: Willey-Teubner Ser. Comput. Sci., 1987.