MATHEMATICAL PROBLEMS IN COMPUTATION THEORY
BANACH CENTER PUBLICATIONS, VOLUME 21
PWN – POLISH SCIENTIFIC PUBLISHERS
WARSAW 1988

ЛИНЕЙНЫЕ НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ И ИХ МАТЕМАТИЧЕСКИЕ МОДЕЛИ*

Р. Г. НИГМАТУЛЛИН

Казанский государственный университет им. В. И. Ульянова-Ленина, Казань, СССР

1. Введение

Проблема нижних оценок сложности (НОСЛ) — одна из наиболее острых открытых проблем математики. Она состоит в том, чтобы доказать высокие НОСЛ для явно заданных булевых функций или языков при вычислении их булевыми схемами или алгоритмами. В данной работе мы ограничимся рассмотрением одной модели вычислений, а именно, схем из функциональных элементов, которые для краткости будем называть просто схемами. Трудности доказательства высоких НОСЛ проявляются на этой модели наиболее выпукло. В чем состоят эти трудности? В том, что несмотря на значительные усилия, не удается доказать высокие НОСЛ для конкретных булевых функций. В частности, все доказанные к настоящему времени НОСЛ в классе схем из функциональных элементов не выше линейных, хотя известно, что почти все булевы функции имеют сложность не менее $2^n/n$. Последние оценки мы не берем во внимание при решении проблемы НОСЛ, поскольку они установлены не для конкретной, а для „случайной" булевой функции.

В данной работе описываются наиболее распространенные методы доказательства НОСЛ для схем из функциональных элементов. При этом не ставится цель назвать все оценки, полученные этими методами. Напротив, конкретные результаты приводятся лишь для иллюстрации методов. Более подробное изложение можно найти в обзоре О. Б.

---

* Работа является записью лекции, прочитанной автором в ноябре 1985 г. в Международном математическом центре им. С. Банаха (г. Варшава). Эта лекция является составной частью курса „Асимптотические оценки сложности управляющих систем", прочитанного в Центре группой советских математиков (научный руководитель курса чл.-корр. АН СССР О. Б. Лупанов).

Лупанова [3], монографиях Дж. Сэвиджа [9] и Р. Г. Нигматуллина [4] и в обзоре В. М. Храпченко [10].

В конце работы строятся математические модели доказательств НОСЛ, которые позволяют рассмотреть различные доказательства НОСЛ с единых позиций и пролить свет на природу трудностей доказательства НОСЛ.

2. Основные понятия и обозначения

Множество двоичных слов (наборов) длины n обозначим B^n. Оно является областью определения булевых функций n переменных. На множестве B^n определена метрика Хэмминга: для $\tilde{a} = (a_1, \ldots, a_n)$ и $\tilde{b} = (b_1, \ldots, b_n)$ из B^n, $\varrho(\tilde{a}, \tilde{b}) = \sum_{i=1}^{n} |a_i - b_i|$. Наборы $\tilde{a}$ и $\tilde{b}$ из B^n называются соседними, если $\varrho(\tilde{a}, \tilde{b}) = 1$.

$X = \{x_1, \ldots, x_n\}$ есть стандартное множество булевых переменных. Помимо стандартных переменных иногда будут встречаться дополнительные булевы переменные Y.

$\wedge$, $\vee$, $^-$, $\oplus$ и $\sim$ обозначают соответственно коньюнкцию, дизьюнкцию, отрицание, сложение по модулю 2 и эквивалентность.

Иногда мы пишем x^d вместо $x \sim d$.

Пусть $A \subseteq X$. *Подстановкой констант* (на места переменных A) называется отображение c: $A \to \{0, 1\}$. Функция, полученная из булевой функции $f(X)$ при подстановке констант, называется *подфункцией функции* f.

Переменная $x_i \in X$ называется *существенной для булевой функции* $f(X)$, если при подстановках констант 0 и 1 вместо x_i получаются различные подфункции функции $f(X)$.

Пусть $D \subseteq B^n$. Функция $f(X)$, определенная на D и принимающая на D значения из $\{0, 1\}$, называется *частичной булевой функцией* (ч.б.ф.). Будем считать, что на множестве $B^n \setminus D$ она равна Λ. Булева функция $h(X)$ называется *доопределением* ч.б.ф. $f(X)$, если на множестве $Dh = f$. Функция f называется в этом случае *частичной функцией функции* h.

Пусть $\mathscr{F}$ есть произвольное множество, элементами которого могут быть булевы функции и ч.б.ф. Булева функция $N(X)$ называется *надфункцией множества* $\mathscr{F}$ и обозначается $N(\mathscr{F})$, если каждая функция из $\mathscr{F}$ является подфункцией функции N или ее частичной функцией.

Пример 1. Функция $\left(\left(\sum_{i=1}^{n} x_i\right) \bmod 3\right) \bmod 2$ является надфункцией множества

$$\mathscr{F} = \{x_i \oplus x_j,\ x_i \wedge x_j \mid\ 1 \leqslant i < j \leqslant n\}. \tag{1}$$

Действительно, при $x_3 = \ldots = x_n = 0$ получается подфункция $x_1 \oplus x_2$, а при $x_3 + \ldots + x_n = 2$ подфункция $x_1 \wedge x_2$. Ввиду симметричности функции аналогично получаются остальные подфункции.

Обобщением понятия надфункции является понятие универсальной функции. Функция $U(X, Y)$ называется *универсальной для множества* $\mathscr{F}$, если для каждой функции $f \in \mathscr{F}$ существует подстановка констант на места дополнительных переменных Y, при которой получается доопределение функции f. Если число q дополнительных переменных удовлетворяет условию $2^q \geqslant |\mathscr{F}|$ ([1]), то универсальная функция $U(\mathscr{F})$ множества $\mathscr{F}$ существует для произвольного множества $\mathscr{F}$, чего нельзя сказать о надфункции.

Схемы (из функциональных элементов) понимаются в обычном смысле (см. напр., [4]). Полагается, что каждая схема имеет 1 выход, который обозначается символом t. Путь, ведущий из вершины v в вершину w, обозначается $(v \Rightarrow w)$.

Внутренние вершины (т.е. отличные от входных) схемы называются ее *элементами*. В данной работе рассматриваются базисы $B_1 = \{\wedge, \vee, \bar{}\}$ и базис B_2, состоящий из всех булевых функций двух переменных.

Сложность схемы S (обозначение $L(S)$) — это число внутренних вершин схемы S. *Сложность функции* f (обозначение $L(f)$) *в базисе* B — это минимальная сложность схемы в базисе B, вычисляющей функцию f.

Функции базиса B_2 разбиваются на 3 класса: функции типа $\wedge$ — это 8 функций вида $(x^a \wedge y^b)^c$, функции типа $\oplus$ — это функции $x \oplus y$ и $x \sim y$ и 6 функций от одной или нуля переменных. Очевиден следующий факт:

Утверждение 1. *Если минимальная схема в базисе* B_2 *реализует функцию, зависящую существенно от двух или более переменных, то она содержит только элементы типов* $\wedge$ *и* $\oplus$ ([2]).

3. Техника доказательств: подстановки констант

Одним из наиболее распространенных приемов при доказательстве НОСЛ является подстановка констант (как правило, на места переменных). Особенно широко этот прием используется в базисе $B_1 = \{\wedge, \vee, \bar{}\}$. Его применение основано на следующем свойстве схем:

Утверждение 2. *Если на вход некоторого элемента схемы в базисе* B_1 *подается константа* 0 *или* 1, *то этот элемент можно удалить из схемы, сохранив функцию схемы.*

([1]) Символ $|A|$ обозначает мощность множества A.

([2]) Здесь считается, что элемент имеет тот тип, каков тип функции, приписанной этому элементу. Элемент отрицание называется еще инвертором.

Доказательство очевидно ввиду соотношений $x \vee 0 = x$, $x \vee 1 = 1$, $y \wedge 0 = 0$, $y \wedge 1 = y$.

При этом для каждой из функций $\wedge$ и $\vee$ существует константа, при подаче которой на место одной переменной функция обращается в константу, т.е. не зависит от второй переменной. Эта константа (0 для $\wedge$ и 1 для $\vee$) называется *забивающим значением переменной*, а операция подачи этой константы называется *забиванием второй переменной.*

Замечание. Операция забивания применима не только к $\wedge$ и $\vee$, но и к произвольной функции типа $\wedge$, т.е. к функции вида $(u^a \wedge v^b)^c$. Это свойство будет использовано в последующих пп.

Продемонстрируем прием забивания на примере линейной функции $l_n = x_1 \oplus \ldots \oplus x_n$. Обозначим $\bar{l}_n = l_n \oplus 1$.

Лемма 1 [8]. *Пусть $S_n^{\min}$ — произвольная минимальная схема, реализующая одну из функций l_n или $\bar{l}_n$ ($n \geqslant 3$). Если в схеме есть полюсы* 0 *и* 1, *то найдутся* 4 *или более элементов, после удаления которых получится схема S_{n-1}, реализующая l_{n-1} или $\bar{l}_{n-1}$.*

Доказательство основано на тщательном переборе возможных структур схемы. Упорядочение перебора ведется по таким признакам, так:

— есть ли переменная, которая подается на вход инвертора,

— если нет, то существует ли переменная, которая подается на входы ровно одного или не менее трех элементов схемы.

Мы не будем разбирать все возможные случаи, поскольку их слишком много. Проиллюстрируем прием забивания на одном из возможных случаев. Этот случай изображен на рис. 1 и характеризуется следующим:

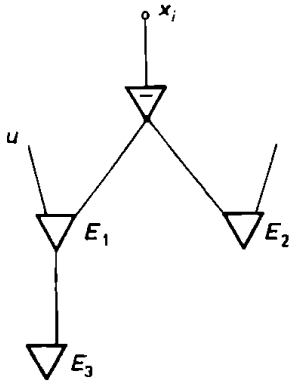

Рис. 1

некоторая переменная подается на вход инвертора, выход которого „ветвится". Элементы E_1 и E_2 отличны от инверторов в силу минимальности схемы. Далее, они не могут быть выходными (иначе переменная x_i забила бы все остальные переменные, что противоречит линей-

ности функций l_n и $\bar{l}_n$). Элементы E_1 и E_2 не могут одновременно подаваться на входы друг друга, поскольку это привело бы к образованию ориентированного цикла в схеме. Поэтому в схеме существует элемент E_3 (см. рис. 1). Выберем такое значение переменной x_i, которое забивает u. Тогда в силу утверждения 2 можно удалить все 4 элемента на рис. 1. Полученная схема реализует l_{n-1} или $\bar{l}_{n-1}$.

Из леммы 1 легко вытекает

Теорема 1 [8]. *В базисе* $B_1 = \{\wedge, \vee, \bar{}\}$

$$L(l_n) \geqslant 4n-4.$$

В работе [8] доказана минимальность схемы для функции l_n, а также для ряда других функций.

Прием подстановки констант работает и в базисе B_2, поскольку для этого базиса с небольшой модификацией сохраняет силу утверждение 2. Эта модификация состоит в том, что при удалении элемента может понадобиться замена операции, приписанной последующему элементу. К примеру, пусть элемент $\varphi(x, y)$ подается на первый вход вершины с операцией $\psi(u, v)$. Пусть далее, к примеру $\varphi(x, 0) = \bar{x}$. Тогда при подаче 0 на второй вход элемента $\varphi(x, y)$ можно удалить этот элемент, заменив операцию $\psi(u, v)$ на $\chi(u, v) = \psi(u, v)$.

4. Техника доказательств: взаимное размещение элементов

Одна из первых нетривиальных нижних оценок сложности в базисе B_2, состоящем из всех булевых функций двух переменных, была установлена в работе Б. М. Клосса и В. А. Малышева [2]. При доказательстве нижней оценки в этой работе было учтено взаимное расположение элементов в минимальной схеме. В этом п. описывается этот прием. Символ $L(\ )$ обозначает в этом п. сложность в базисе B_2.

Схема называется *приведенной*, если из каждой ее вершины, кроме выходной, выходит хотя бы одна дуга. Очевидно, для каждой схемы существует эквивалентная ей приведенная схема не большей сложности.

Утверждение 3. *Пусть приведенная схема S сложности L содержит p_i полюсов с выходной степенью i и v_i элементов с выходной степенью i $(i = 1, \ldots, L)$. Тогда*

$$L(S) \geqslant p_1 + 2p_2 + \ldots + Lp_L + v_2 + 2v_3 + \ldots + (L-1)v_L - 1.$$

Справедливость утверждения следует из того, что входящих дуг в схеме не более $2L$, а выходящих $p_1 + 2p_2 + \ldots + Lp_L + L - 1$ {комментарий: все элементы, кроме выходного, имеют хотя бы по одной выходящей дуге} $+ v_2 + 2v_3 + \ldots + (L-1)v_L$.

Функция f называется *парно-разделимой*, если для любой пары различных аргументов x_i, x_j из X и любых двух пар (a_i, a_j), (b_i, b_j) значений этих аргументов таких, что $a_i + a_j \neq b_i + b_j$ (сложение обычное, а не по модулю 2!) существует подфункция $\varphi(x_i, x_j)$ функции f, разделяющая эти две пары (a_i, a_j) и (b_i, b_j) (функция $\varphi(x_i, x_j)$ разделяет по определению пары (a_i, a_j) и (b_i, b_j), если $\varphi(a_i, a_j) \neq \varphi(b_i, b_j)$).

В качестве примера парно-разделимой функции можно рассмотреть универсальную функцию множества функций $\mathscr{F}$ из (1).

Существуют парно-разделимые функции, не имеющие дополнительных переменных, например, функция из примера 1 (параграф 2).

Отметим характеристические свойства функций типов $\wedge$ и $\oplus$ применительно к парной разделимости.

Утверждение 4. *Функция типа* $\oplus$ *не разделяет пары* (0, 0) *и* (1, 1), *а функция типа* $\wedge$ *не разделяет одну из пар* (0, 1), (1, 0) *с одной из пар* (0, 0), (1, 1).

Нижеследующая теорема 2 является небольшой модификацией теоремы из [2]. Модификация состоит в том, что функции f разрешается иметь дополнительные переменные Y.

Теорема 2. *Если функция* $f(X, Y)$ *парно-разделима, то*

$$L(f) \geqslant (10n-5)/9.$$

Доказательство. Мы повторим доказательство из [2] с небольшими упрощениями, чтобы убедиться, что оно сохраняет силу при введении дополнительных переменных.

Пусть S есть произвольная минимальная схема, реализующая функцию $f(X, Y)$. В силу утверждения 1 схема содержит только элементы типов $\wedge$ и $\oplus$.

Функция f в силу парной разделимости зависит существенно от всех переменных из X. Поэтому в схеме S есть полюсы $x_1, \ldots, x_n$, причем $n \geqslant 2$. Пусть p_1 из них имеют выходную степень 1. Назовем эти полюсы *отмеченными*.

Предположим, что в схеме S есть вершина a, на оба входа которой подаются отмеченные полюсы x_i и x_j. Они должны быть различными в силу минимальности схемы. На выходе вершины a вычисляется функция одного из типов $\wedge$ и $\oplus$. Поэтому на выходе этой вершины (а следовательно, и всей схемы) не может вычисляться парно-разделимая функция в силу утверждения 4. Поэтому такой вершины a в схеме S быть не может. Следовательно, схема S содержит p_1 различных вершин, на входы которых подаются отмеченные полюсы. Если такая вершина имеет выходную степень 1, будем называть ее отмеченной (она по определению отличная от полюса).

Обозначим символом l число отмеченных вершин. Тогда $p_1 - l$

вершин, на входы которых подаются отмеченные полюсы, имеют выходную степень не менее двух. Из утверждения 3 следует

$$L \geqslant p_1 + 2(n-p_1) + p_1 - l - 1 = 2n - l - 1. \tag{2}$$

Докажем теперь, что $L \geqslant 1.25l$. Для этого рассмотрим взаимное расположение вершин.

Лемма 2. *Пусть a и b — отмеченные вершины минимальной схемы S, причем a непосредственно предшествует b. Тогда вершина a типа $\wedge$, а вершина b типа $\oplus$.*

Доказательство. Пусть на входы вершин a и b подаются соответственно отмеченные полюсы x_i и x_j. Если вершина b типа $\wedge$, то пусть d есть забивающее значение на входе этой вершины. Тогда на выходе этого элемента не разделяются пары $(0, d)$ и $(1, d)$ значений переменных x_i, x_j. Ввиду отмеченности вершин a и b не разделяются они и на выходе схемы. Поэтому вершина b имеет тип $\oplus$ в силу минимальности схемы и утверждения 1. Если бы и вершина a имела тип $\oplus$, то на выходе вершины b вычислялась бы функция вида $x_i \oplus x_j \oplus h(X \setminus \{x_i, x_j\})$, которая не может разделять пары $(0, 0)$ и $(1, 1)$ значений переменных x_i, x_j. Лемма доказана.

Следствие. *Вершина b из условия леммы 2 не может подаваться на вход отмеченной вершины схемы S.*

Отсюда вытекает, что выходы по крайней мере половины отмеченных вершин подаются на входы неотмеченных вершин. Поэтому число последних не менее $l/4$. Следовательно,

$$L \geqslant l + l/4 = 5l/4,$$

т.е.

$$4L \geqslant 5l. \tag{3}$$

Переписав (2) в виде $5L \geqslant 10n - 5l - 5$ и сложив его с (3), получим утверждение теоремы.

Следствие. *Если $f(X)$ есть произвольная надфункция множества функций $\mathscr{F}$ из* (1), *то $L(f) \geqslant (10n-5)/9$.*

Если свойство парной разделимости выполняется и для подфункций функции f, можно получить для f и более высокую нижнюю оценку. Функция $f(X)$ называется *m раз парно-разделимой*, если при подстановке вместо любых $m-1$ переменных произвольных констант получившаяся функция снова парно-разделима.

Пример. Функция $C_n(x_1, \ldots, x_n) = \sum\limits_{1 \leqslant i < j \leqslant n} x_i x_j$ $(n-2)$ раза парно-разделима.

Теорема 3 [2]. $L(C_n(x_1, \ldots, x_n)) \geqslant 2(n-1)$.

Доказательство индукцией по n. При $n = 3$ перебором убеждаемся, что $L(C_3) \geqslant 4$. Выберем теперь в схеме полюс x_i с выходной степенью не менее двух (он существует в силу парной разделимости) и положим $x_i = 0$. Тогда полученная схема реализует функцию C_{n-1} и содержит по крайней мере на 2 элемента меньше (в силу аналога утверждения 2).

5. Техника доказательств: учет расщеплений

Под расщеплением понимается вершина схемы, имеющая выходную степень не менее двух. Как видно из утверждения 3 наличие таких вершин повышает сложность схемы. Поскольку реально не удается доказать существование в схеме вершин с выходной степенью более двух, то мы сформулируем частный случай утверждения 3:

Утверждение 5. *Если схема S имеет n полюсов, p расщеплений и одну выходную вершину, то*

$$L(S) \geqslant n + p - 1. \tag{4}$$

Частично учет расщеплений проводился уже в предыдущем параграфе. В этом параграфе мы используем этот прием в полной мере. Он был разработан Паулем в [7].

Внимательный читатель мог заметить, что при оценке сложности парно-разделимых функций в параграфе 4 условия леммы 2 были выполнены с трудом. Поэтому, если потребовать от парно-разделимой функции „немного" дополнительных свойств, условия леммы 2 перестанут выполняться и в схеме появится много новых расщеплений. Мы потребуем от парно-разделимой функции, чтобы она была надфункцией множества функций $\mathscr{F}$ из (1).

Следующее утверждение является переформулировкой леммы из [7].

Лемма 3. *В минимальной схеме для универсальной функции множества $\mathscr{F}$ из* (1) *каждой паре полюсов $x_i, x_j \in X$ соответствуют такие пути $(x_i \Rightarrow t)$ и $(x_j \Rightarrow t)$, что до их первого пересечения хотя бы один из них разветвляется.*

Доказательство от противного. Пусть пути $(x_i \Rightarrow t)$ и $(x_j \Rightarrow t)$ впервые встречаются в вершине a и до этого они не разветвляются. Тогда при произвольной подстановке констант на места переменных, отличных от x_i и x_j, тип функции $\varphi(x_i, x_j)$, вычисляемой в вершине a, совпадает с типом вершины a либо функция $\varphi(x_i, x_j)$ не зависит хотя бы от одной из переменных x_i, x_j. Поэтому такая схема не может вычислять нашу функцию.

Сформулируем теперь теорему из [7] в удобных для нас терминах:

ТЕОРЕМА 4. *Для универсальной функции f множества функций $\mathscr{F}$ из* (1)

$$L(f) \geqslant 2n-2$$

в базисе B_2.

Доказательство. В произвольной минимальной схеме для функции f имеется $n-1$ таких полюсов $x_i \in X$, что путь $(x_i \Rightarrow t)$ разветвляется. В противном случае для некоторых x_{i_0}, $x_{j_0} \in X$ существовало бы только по одному пути $(x_{i_0} \Rightarrow t)$ и $(x_{j_0} \Rightarrow t)$, что противоречит лемме 3. Возьмем в каждом из $n-1$ путей $(x_i \Rightarrow t)$ первую вершину с выходной степенью не менее двух. Эти вершины попарно различны в силу леммы 3. Применение утверждения 5 дает оценку $2n-2$.

6. Техника доказательств: присвоение функций

Мы рассматривали выше прием, который заключается в присвоении некоторой переменной некоторой булевой константы. В этом параграфе этот прием обобщается до присвоения произвольной булевой функции некоторой переменной. Этот прием был предложен Паулем [7]. Мы продемонстрируем его на примере оценки сложности универсальной функции множества

$$\mathscr{F} = \{x_1, \ldots, x_n\}. \tag{5}$$

ТЕОРЕМА 5. *Для универсальной функции U множества $\mathscr{F} = \{x_1, \ldots, x_n\}$ в базисе B_2 справедлива нижняя оценка*

$$L(U(\mathscr{F})) \geqslant 2n-2. \tag{6}$$

Доказательство почти дословно повторяет доказательство из [7]. При $n = 1$ утверждение очевидно. Пусть теперь $n \geqslant 2$. Возможны три случая.

Случай 1. Существует $x_i \in \mathscr{F}$ такое, что выходная степень полюса x_i не меньше 2. Положив $x_i = 0$ (или 1), можно удалить из схемы по крайней мере два элемента. Полученная схема реализует универсальную функцию множества $\mathscr{F} \setminus \{x_i\}$ и к ней применимо предположение индукции. Поэтому $L(U(\mathscr{F} \setminus \{x_i\})) \geqslant 2(n-1)-2$ и (6) доказано.

Случай 2. Существует $x_i \in \mathscr{F}$ такое, что выходная степень полюса x_i равна 1 и единственное ребро, выходящее из x_i, идет в вершину типа $\wedge$. Обозначим эту вершину v. Она не может быть выходной, поскольку при забивающем значении x_i функция, вычисляемая в этой вершине, не зависит от остальных переменных из X вопреки определению универсальной функции $U(\mathscr{F})$. Положив x_i равным забивающему значению, можно удалить элемент v и следующий за ним.

Случай 3. Существует $x_i \in \mathscr{F}$ такое, что выходная степень полюса x_i равна 1 и единственное ребро, выходящее из x_i, идет в вершину типа $\oplus$. Обозначим эту вершину v. Она не может быть выходной. Действительно, выберем значения дополнительных переменных так, чтобы $U = x_j$ $(j \neq i)$. Но при этом функция, вычисляемая в вершине v, зависит от x_i. Следовательно, вершина v не выходная.

Пусть на второй вход вершины v подается некоторая функция y. Положим $x_i := y$ (это и есть новый прием). Тогда в вершине v реализуется константа и из схемы можно удалить элемент v и следующий за ним элемент. Полученная схема реализует универсальную функцию $U(\mathscr{F} \setminus \{x_i\})$. Остается воспользоваться предположением индукции.

В каждом из рассмотренных выше доказательств НОСЛ как правило использовался лишь один из описанных приемов (не считая подстановок констант). Комбинирование различных приемов (и особенно, учет взаимного расположения вершин) позволяет доказать следующее утверждение:

Теорема 6. *Для универсальной функции множества*

$$\mathscr{F} = \{x_i \wedge x_j,\ x_i \oplus x_j \mid\ 1 \leqslant i \leqslant j \leqslant n\}$$

имеет место следующая нижняя оценка в базисе B_2

$$L(U(\mathscr{F})) \geqslant 3n-3.$$

Доказательство следует доказательствам работ [1], [7]. Здесь оно не приводится, поскольку требует нескольких страниц текста, а необходимая техника уже описана выше.

7. Математические модели нижних оценок сложности

Проблема нижних оценок сложности принадлежит к числу очень трудных математических проблем. Видимо, не достигнуто еще и хорошее понимание этой проблемы. Об этом косвенным образом свидетельствует то, что еще не сформирована отточенная формулировка проблемы, позволяющая отсекать неудовлетворительные решения этой проблемы (в частности, решения, поучаемые мощностным методом Шеннона или подобным ему методом). Об этом же говорит же и разнообразие методов доказательств НОСЛ, которые трудно поддаются классификации.

В данном параграфе излагается предложенный автором в [5], [6] подход, позволяющий описать доказательства НОСЛ с единых позиций. Он основан на представлении доказательств НОСЛ в виде доказательств НОСЛ для подходящих надфункций или, в более общем случае, для надсхем. Тем самым доказательства НОСЛ для надфункций и надсхем можно рассматривать как модели нижних оценок сложности.

В основе предлагаемой модели лежит тезис о том, что доказатель-

ства НОСЛ по своей природе близки к доказательствам НОСЛ в задаче на покрытие. В задаче на покрытие, как известно, множество считается покрытым, если покрыт каждый его элемент. Наш тезис состоит в том, что при доказательствах НОСЛ функция, сложность которой оценивается снизу, распадается на множество подфункций и нижняя оценка сложности доказывается для произвольной надфункции этого множества функций. Поскольку множество подфункций может иметь различные надфункции (что было хорошо видно на примере парно-разделимых функций в параграфе 4), то нижняя оценка доказывается, вообще говоря, не для индивидуальной функции, а для множества функций. При этом величина нижней оценки мажорируется сложностью самой простой из этих функций. Поскольку этих функций может быть много, то среди них могут найтись и простые функции. Это делает невозможным доказательство высокой НОСЛ для исходной функции. В этом заключается, повидимому, главная трудность доказательства высоких НОСЛ.

Покажем теперь, что доказательства НОСЛ, описанные в параграфах 3–6, действительно можно представить как доказательства НОСЛ для подходящих надфункций.

Для произвольного набора $\tilde{a} \in B^n$ положим

$$\varphi_{\tilde{a}}(\tilde{x}) = \begin{cases} 1, & \text{если } \tilde{x} = \tilde{a}, \\ 0, & \text{если } \varrho(\tilde{x}, \tilde{a}) = 1, \\ \Delta & \text{в остальных случаях.} \end{cases}$$

Полагая $\bar{\Delta} = \Delta$, можно считать определенной функцию $\bar{\varphi}_{\tilde{a}}(\tilde{x})$.

Рассмотрим множество $\mathscr{F}$ ч.б.ф., которое для каждого набора $\tilde{a} \in B^n$ содержит либо функцию $\varphi_{\tilde{a}}(\tilde{x})$, либо $\bar{\varphi}_{\tilde{a}}(\tilde{x})$. Очевидно, множества $\mathscr{F}$ такого типа допускают лишь две надфункции, а именно, линейные функции $l_n = x_1 \oplus \ldots \oplus x_n$ и $\bar{l}_n$. Анализ доказательства леммы 1 и теоремы 1 показывает, что оно сохраняет силу для произвольной надфункции множества $\mathscr{F}$ (что, впрочем, не удивительно, поскольку линейные функции l_n и $\bar{l}_n$ являются единственными надфункциями множества $\mathscr{F}$).

Перейдем теперь к парно-разделимым функциям. В их определении не содержится явного указания множества подфункций, однако примеры парно-разделимых функций показывают, что в качестве множества подфункций достаточно взять множество $\mathscr{F}$ из (1). То же множество годится для доказательства теоремы 4. В теореме 3 в качестве множества ч.б.ф. можно взять модифицированное очевидным образом множество (1).

В теоремах 5 и 6 множества подфункций явным образом указаны.

Таким образом, для всех доказательств НОСЛ из параграфов 3–6 нам удалось указать такие множества подфункций $\mathscr{F}$, что доказательство НОСЛ можно преобразовать в доказательство НОСЛ для надфункции множества $\mathscr{F}$. Это получилось с легкостью благодаря тому, что необходимые подмножества $\mathscr{F}$ уже были выделены при доказательстве НОСЛ.

В общем случае при доказательстве НОСЛ эти подмножества явным образом не фигурируют, и их приходится „выуживать" из доказательства.

Целый ряд описанных в работе доказательств (см. теоремы 2, 4–6) допускает перенос не только на надфункции, но и на универсальные функции. Мы обращаем на это внимание, поскольку использование дополнительных переменных универсальной функции предоставляет широкие возможности для построения таких функций, причем с малой сложностью. Это позволяет ограничить сверху величины нижних оценок сложности.

Литература

[1] N. Blum, *A Boolean function requiring 3n network size*, Theoret. Comput. Sci. 28, No. 3 (1984), 337–345.

[2] Б. М. Клосс, В. А. Малышев, *Оценки сложности некоторых классов функций*, Вестник Моск. ун.-та сер. матем. мех. №4 (1965), 44–51.

[3] О. Б. Лупанов, *О методах получения оценок сложности и вычисления индивидуальных функций*, Сб. Дискретный анализ, вып. 25. Новосибирск 1974, 3–18.

[4] Р. Г. Нигматуллин, *Сложность булевых функций*, Казань, изд-во Каз. ун-та, 1983.

[5] —, *Сложность универсальных функций и нижние оценки сложности*, Известия вузов. Мат.-ка, №11, Казань 1984, 10–20.

[6] —, *Are lower bounds on the complexity lower bounds for universal circuits?* Lecture Notes in Computer science, 199, Proc. FCT'85 Conf. Springer, 1985, 331–340.

[7] W. J. Paul, *A 2.5n-lower bound on the combinational complexity of Boolean functions*, SIAM J. Comput. 6, No. 3 (1977), 427–443.

[8] Н. П. Редькин, *Доказательство минимальности некоторых схем из функциональных элементов*, Сб. Проблемы кибернетики, вып. 23. — М., Наука (1970), 83–101.

[9] J. E. Savage, *The complexity of computing*, N. Y., Wiley-Interscience, 1976.

[10] В. М. Храпченко, *Нижние оценки сложности схем из функциональных элементов* (обзор), Сб. Кибернетически сборник, вып. 21. — М., Мир (1984), 3–54.

Presented to the semester
Mathematical Problems in Computation Theory
September 16–December 14, 1985