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

ОБ ОДНОМ ПОДХОДЕ К ОЦЕНКЕ ПРОСТРАНСТВЕННОЙ СЛОЖНОСТИ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

С. А. ЛОЖКИН, А. И. РЫБКО, А. А. САПОЖЕНКО,
Ю. ХРОМКОВИЧ, Н. А. ШКАЛИКОВА

Московский государственный университет им. М. В. Ломоносова, Москва, СССР

The problem of the layout of Boolean circuits into the plane is investigated. A new general approach for proving lower bounds on layout area is given. Using this approach, the strongest lower bound $\Omega(n^2)$ on the layout area of any Boolean circuit computing a specific Boolean function g is obtained. Further, it is shown that the lower bound established is optimal, and that the three-dimensional layout of any Boolean circuit computing g requires at least $n^{4/3}$ amount of space. To relate these results to combinational complexity the boolean circuit of the size $O(n\log_2 n)$ computing g is constructed.

1. Введение

Наиболее распространенной моделью вычисления дискретных функций являются схемы из функциональных элементов, сложность которых, понимаемая как число элементов, рассматривалась во многих работах (см., например, [5]). Однако, при реализации функций интегральными схемами существенным параметром оказывается площадь, которую занимает схема. При этом величина площади зависит не только от числа элементов, но и от структуры связей между ними. Как следует из работы [1], размещение на плоскости схемы, оптимальной по числу элементов, требует, как правило, такой площади, которая существенно больше оптимальной.

В работах [2], [4], [8] была рассмотрена математическая модель схем из функциональных элементов, размещенных на плоскости, в которой критерием сложности схемы служила занимаемая ею площадь. В работе [4] был установлен порядок, а в работе [2] — доказано существование асимптотики для сложности самой сложной функции от n переменных. В работе [8] было показано, что сложность реализации всех элементарных конъюнкций от n переменных равна по порядку $n\cdot 2^n$, сложность реализации всех булевых функций от n переменных — $n\cdot 2^{2^n}$, сложность умножения двух n-разрядных двоичных чисел — n^2, сложность реализации произвольной заданной перестановки n заданных булевских переменных — $n^2\log n$. Что касается одной булевой функции $f\colon \{0, 1\}^n \to \{0, 1\}$, то в работе [8] было доказано, что сложность реализации некоторых симметрических функций равна по порядку $n\log n$, а в работе [9] была построена специальная булевская функция, сложность которой равна по порядку $n^{3/2}$. Тем самым, для сложности плоской реализации конкретных булевских функций были получены нелинейные нижние оценки.

Используя технику получения нижних оценок из [8], мы введем понятие коммуникативной сложности схем из функциональных элементов, с помощью которого сформулируем общий подход к доказательству нижних оценок сложности плоской реализации булевских функций. Применяя этот подход, получим квадратичную нижнюю оценку для сложности плоской реализации одной специальной булевской функции. С другой стороны, мы докажем, что эта оценка является точной по порядку. Будет доказана также нижняя оценка порядка $n^{4/3}$ для сложности объемной реализации этой функции и верхняя оценка порядка $n\log n$ для числа функциональных элементов.

2. Основные определения

Введем понятие коммуникативной сложности для схем из функциональных элементов. Отметим, что это понятие существенно отличается от понятия коммуникативной сложности из [3].

Пусть F — система булевских функций вида $\{0, 1\}^N \to \{0, 1\}^m$ от N переменных $X = \{x_1, x_2, \ldots, x_N\}$ и пусть $Y \subseteq X$. Рассмотрим произвольную схему S из функциональных элементов в каком-либо конечном базисе, которая реализует F. Пусть $\Pi_{Y,S}$ — множество всех разбиений π_Y вершин схемы S на два непересекающихся подмножества, каждое из которых содержит не менее $[|Y|/2]$ переменных из Y. Обозначим через $c(\pi_Y)$ число ребер, соединяющих вершины из различных подмножеств разбиения π_Y. Положим:

$$c_Y(S) = \min\{c(\pi_Y) |\ \pi_Y \in \Pi_{Y,S}\},$$

$$c_Y(F) = \min\{c_Y(S) |\ S \text{ реализует } F\},$$

$$c(F) = \max\{c_Y(F) |\ Y \subseteq X,\ |Y| \geqslant |X|/3\}.$$

Величину $c(F)$ будем называть *коммуникативной сложностью системы функций* F. Легко видеть [3], что для любой системы булевских функций F от N переменных $c(F) \leqslant N/2$.

Формальное определение математической модели схем из функциональных элементов, размещенных на плоскости, можно найти в [2], [4], [8]. Это определение основывается на понятии *схемы из клеточных элементов*, которая с содержательной точки зрения представляет собой плоскую прямоугольную решетку, в каждой клетке которой расположен либо функциональный, либо коммутационный элемент. На каждой стороне клетки расположено не более одного входа или выхода соответствующего элемента, с помощью которого этот элемент соединяется с соседним элементом. Входы и выходы всей схемы расположены (вообще говоря произвольно) по ее границе. Под *сложностью схемы* понимается число клеток прямоугольника, который она занимает, а под *сложностью $A(F)$ системы булевских функций F* — минимальная из площадей (сложностей) схем, ее реализующих.

3. Подход к получению нижних оценок

Основой предлагаемого подхода является следующая

Теорема. *Пусть F — система булевских функций вида $\{0, 1\}^N \to \{0, 1\}^m$. Тогда*

$$A(F) \geqslant \tfrac{1}{12}(N+m)c(F).$$

Доказательство. Пусть K — схема из клеточных элементов размеров a на b, реализующая систему F. Пусть $a \geqslant b$ и, следовательно, $a \geqslant (m+N)/4$. Возьмем произвольное подмножество Y множества переменных $X = \{x_1, \ldots, x_n\}$ системы F такое, что $|Y| \geqslant N/3$. Рассмотрим два случая в зависимости от того, существует или нет прямая l параллельная стороне длины b схемы K, которая разделяет входные переменные Y на две части, содержащие не менее чем $[|Y|/2]$ переменных. Если такой прямой не существует, то по крайней мере на одной из сторон длины b схемы K должно быть расположено не менее половины входов из Y. Следовательно,

$$b \geqslant N/6, \qquad ab \geqslant \frac{m+N}{4}\cdot\frac{N}{6}$$

и, так как $c_Y(F) \leqslant c(F) \leqslant N/2$, то

$$ab \geqslant \tfrac{1}{12}(m+N)c_Y(F).$$

Если такая прямая существует, она порождает некоторое разбиение π_Y обычной схемы из функциональных элементов S, соответствующей схеме K. Тем самым,

$$b \geqslant c(\pi_Y) \geqslant c_Y(F) \quad \text{и} \quad ab \geqslant \frac{m+N}{4}c_Y(F).$$

В любом из этих случаев для каждого $Y \subseteq X$ такого, что $|Y| \geqslant N/3$ получено неравенство

$$ab \geqslant \frac{m+N}{12} c_Y(F),$$

которое доказывает теорему.

Введенное выше понятие коммуникативной сложности булевских функций имеет общие черты с понятием коммуникативной сложности VLSI-схем, предложенной в [7]. Коммуникативная сложность схем из функциональных элементов, реализующих F, позволяет получать нижние оценки для $A(F)$, в то время как коммуникативная сложность VLSI-схем помогает получать нижние оценки только для пространственно-временного параметра AT^2. Это связано с тем, что соответствующие модели вычисления имеют следующие основные отличия:

1. все процессоры в VLSI-схеме работают синхронно в каждый из дискретных моментов времени $t = 0, 1, \ldots$ пока продолжается вычисление, тогда как каждый клеточный элемент срабатывает в течение вычисления только один раз;

2. в схеме из клеточных элементов каждая входная переменная имеет свой вход, в то время, как в VLSI-схеме через один и тот же вход в разные моменты времени могут поступать разные переменные.

Обозначим через $\mathrm{COMM}(f)$ коммуникативную сложность булевской функции f в VLSI-модели [6]. Легко показать, что

$$\mathrm{COMM}(f) \leqslant c(f).$$

Так как для почти всех булевских функций от N переменных $\mathrm{COMM}(f) \geqslant [N/2]$ (см. [6]), то для почти всех функций от N переменных будет иметь место равенство $c(f) = [N/2]$.

4. Квадратичная оценка площади для одной булевской функции

Получим квадратичную нижнюю и квадратичную верхнюю оценки величины $A(g_n)$ для булевской функции g_n от переменных $\tilde{x} = (x_1, x_2, \ldots, x_{2n})$, $\tilde{y} = (y_1, y_2, \ldots, y_{2n})$, $\tilde{u} = (u_1, \ldots, u_{2n})$, $\tilde{v} = (v_1, \ldots, v_{2n})$ определенной следующим образом:

$$g_n(\tilde{u}, \tilde{v}, \tilde{x}, \tilde{y}) = \mathop{\&}_{i=1}^{s} (x_{h_k(\tilde{u})} \sim y_{h_k(\tilde{v})}), \tag{1}$$

где

$$s = s(\tilde{u}, \tilde{v}) = \min\Big\{ \sum_{i=1}^{2n} u_i, \sum_{j=1}^{2n} v_j \Big\},$$

а $h_k(\tilde{z})$ — номер той координаты набора значений переменных $\tilde{z}$, в которой находится k-я (считая слева направо) единица. Функция g_n равна 1 тогда и только тогда, когда поднаборы наборов значений переменных $\tilde{x}$ и $\tilde{y}$, выделяемые единицами наборов значений переменных $\tilde{u}$ и $\tilde{v}$ соответственно, совпадают в первых $s(\tilde{u}, \tilde{v})$ координатах.

Лемма 1. $c(g_n) \geqslant n$.

Доказательство. Обозначим через W множество всех переменных функции g_n. Рассмотрим подмножество Z множества W, состоящее из переменных наборов $\tilde{x}$ и $\tilde{y}$. Нам достаточно доказать, что $c_Z(g_n) \geqslant n$.

Предположим, что это не так, то есть, существует схема из функциональных элементов S, реализующая g_n, и ее разбиение π_Z, для которого $c(\pi_Z) \leqslant n-1$. Пусть $\tilde{q} = (q_1, \ldots, q_r)$ — набор тех вершин схемы S, которые соответствуют выходам элементов или входам S, переходящим из одной части разбиения π_Z в другую. Очевидно, что $r \leqslant c(\pi_Z) \leqslant (n-1)$. Для каждого набора $\tilde{\delta}$ значений входных переменных обозначим через $\tilde{\eta}(\tilde{\delta})$ набор значений булевских функций, реализуемых в вершинах $q_1, q_2, \ldots, q_r$.

Пусть в одной части разбиения π_Z оказалось p переменных из набора $\tilde{x}$ и m переменных из набора $\tilde{y}$, где $p+m = 2n$. Без ограничения общности можно считать, что $m \geqslant p$ и поэтому $m \geqslant n$, и что в первой части разбиения π_Z находятся переменные $X' = \{x_{i_1}, \ldots, x_{i_n}\}$, а во второй части — переменные $Y' = \{y_{j_1}, \ldots, y_{j_n}\}$. Выберем значения $\tilde{\alpha}$ и $\tilde{\beta}$ переменных $\tilde{u}$ и $\tilde{v}$ так чтобы, для всех $k = 1, 2, \ldots, n$, $h_k(\tilde{\alpha}) = i_k, h_k(\tilde{\beta}) = j_k$, а число 1 в каждом из наборов $\tilde{\alpha}$ и $\tilde{\beta}$ было равно n.

Рассмотрим множество M всех таких наборов $\tilde{\delta}$ значений переменных из W, для которых $\tilde{u} = \tilde{\alpha}$, $\tilde{v} = \tilde{\beta}$, переменные x_i и y_j, не входящие, соответственно, в X' и Y', равны 1, и, кроме того, $g_n(\tilde{\delta}) = 1$. Очевидно, что $|M| = 2^n$. Так как $r \leqslant c(\pi_Z) \leqslant (n-1)$, то найдутся два различных набора $\tilde{\delta}'$ и $\tilde{\delta}''$ из M, для которых $\tilde{\eta}(\tilde{\delta}') = \tilde{\eta}(\tilde{\delta}'')$. Обозначим через $\tilde{\gamma}'$ набор, который получается заменой в наборе $\tilde{\delta}'$ координат, связанных с множеством переменных X', на соответствующие координаты набора $\tilde{\delta}''$, а через $\tilde{\gamma}''$ — набор, который получается заменой в наборе $\tilde{\delta}''$ координат, связанных с множеством переменных Y', на соответствующие координаты набора $\tilde{\delta}'$. Очевидно, что $g_n(\tilde{\gamma}') = g_n(\tilde{\gamma}'') = 0$.

Предположим, что выход схемы находится в первой части разбиения π_Z и придем к противоречию, показав, что на наборе $\tilde{\gamma}''$ на выходе схемы должна появиться 1. Рассмотрим первую часть схемы S как самостоятельную схему S_1, входами которой являются те входы S, которые в нее попали, и часть вершин $q_1, q_2, \ldots, q_r$, а выходом — выход схемы S. На наборах $\tilde{\delta}''$и $\tilde{\gamma}''$ значения всех входов схемы S_1 одинаковы и, следовательно, на наборе $\tilde{\gamma}''$ на выходе схемы S_1, а значит и на выходе S должна появиться 1. Если выход схемы S расположен во второй половине разбиения π_2, то аналогичные рассуждения будут справедливы для наборов $\tilde{\gamma}'$ и $\tilde{\delta}'$. Полученное противоречие доказывает лемму.

Следствие. $A(g_n) \geqslant \frac{3}{4}n^2$.

Доказательство следует из теоремы и леммы 1.

Лемма 2. $A(g_n) \leqslant dn^2$, *где* d *— некоторая константа, зависящая от базиса.*

Доказательство. Построим такую схему K из клеточных элементов, которая реализует функцию g_n и имеет площадь, равную по порядку n^2. Схема K включает в себя прямоугольную решетку, составленную из одинаковых по размерам, ориентации и функционированию прямоугольных блоков (схем) $K_{i,j}$, $i, j = 1, 2, \ldots, 2n$. Каждый такой блок имеет 7 входов и 7 выходов, пронумерованных числами $1, 2, \ldots, 7$ (см. рис. 1). Входы и выходы блоков, имеющие один и тот же номер, будем называть *соответствующими.* Функционирование одного блока $K_{i,j}$ может быть описано следующим образом: значения на выходах 1, 2, 6, 7 всегда равны значениям на соответствущих входах; значения на выходах 3–5 могут отличаться от значений соответствующих входов только тогда, на всех входах 2–6 имеются единичные значения; в этом случае значения на выходах 3, 4 равны нулю, а на выходе 5 реализуется функция совпадения входов 1 и 7, то есть функция $x_i \sim y_j$.

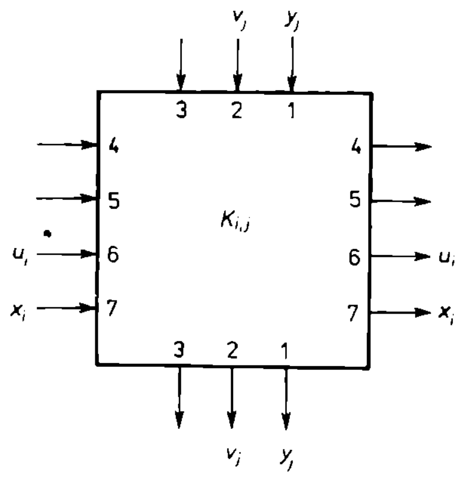

Рис. 1

В схеме K на входы 1, 2 и 3 каждого блока $K_{i,j}$ при $i > 1$ подаются соответствующие выходы блока $K_{i-1,j}$, а при $i = 1$ — переменные y_j, v_j и константа 1; аналогично организовано соединение входов и выходов соседних блоков $K_{i,j-1}$, $K_{i,j}$, $i, j = 1, \ldots, 2n$, причем на входы 4, 5 блока $K_{i,1}$ подается константа 1, а на входы 6, 7 этого блока — переменные u_i, x_i (см. рис. 2). Выход 5 каждого блока $K_{i,2n}$, $i = 1, \ldots, 2n$, подается на 1-й вход блока D_i, реализующего конъюнкцию. На 2-й вход блока D_i при

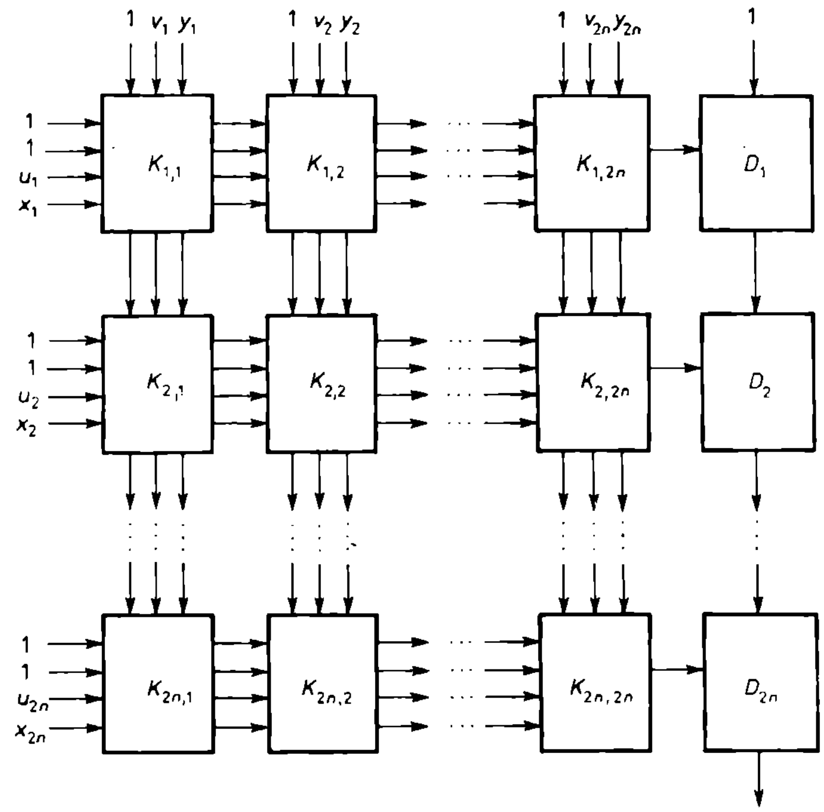

Рис. 2

$i > 1$ подается выход блока D_{i-1}, а при $i = 1$ — константа 1. Выходом схемы является выход блока D_{2n}.

Нетрудно убедиться в том, что при любом наборе значений переменных $\tilde{u}$ и $\tilde{v}$ все блоки $K_{i,j}$, $i, j = 1, \ldots, 2n$, для которых сомножитель $(x_i \sim y_j)$ не входит в конъюнкцию (1), работают как коммутационные элементы, передающие значения входов на соответствующие выходы. Сомножители конъюнкции (1), реализованные при этом на выходах остальных блоков $K_{i,j}$, проходят на входы блоков D_i и на выходе схемы возникает значение функции g_n.

Очевидно, что каждый из описанных выше блоков может быть реализован с константной сложностью в произвольном полном базисе из функциональных и коммутационных элементов, и поэтому для некоторой константы d, зависящей от базиса,

$$A(g_n) \leqslant dn^2.$$

Лемма доказана.

В работе [9] рассматривалось размещение схем из функциональных элементов не только в двумерном, но и в трехмерном пространстве, причем мерой сложности трехмерной схемы служил занимаемый ею объем. Там было доказано, что для каждой трехмерной схемы объема V можно построить эквивалентную ей плоскую схему, площадь которой по порядку не больше чем $V^{3/2}$. В силу доказанных выше теоремы и леммы 1, отсюда следует, что сложность объемной реализации функции g_n по порядку не меньше чем $n^{4/3}$.

В дальнейшем через $L(F)$ будем обозначать минимальное число функциональных элементов из какого-либо конечного полного базиса, достаточное для построения схемы, реализующей систему булевских функций F. Для булевского набора $\tilde\sigma = \tilde\sigma^r = (\sigma_1, \ldots, \sigma_r)$ введем также обозначения: $\|\tilde\sigma\| = \sum\limits_{i=1}^{r} \sigma_i$ и $|\tilde\sigma| = \sum\limits_{i=1}^{r} \sigma_i 2^{i-1}$.

Лемма 3. *Для некоторой константы d_1, зависящей от базиса, справедливо неравенство $L(g_n) \leqslant d_1 n \log n$.*

Доказательство. Для $q = 2^{p-1}$, $p = 2, 3, \ldots$ рассмотрим систему булевских функций R_q вида $\{0, 1\}^{2q+p} \to \{0, 1\}^{2q}$, которая переводит набор значений входных переменных $\tilde x^q, \tilde u^q, \tilde s^p$ в набор значений выходных переменных $\tilde w^{2q}$ так, что при $\tilde u = \tilde 0^q$ $\tilde w = \tilde 0^{2q}$, а при $\tilde u \neq \tilde 0^q$ для всех $k = 1, 2, \ldots, \|\tilde u\|$, $w_{|\tilde s|+k} = x_{h_k(\tilde u)}$, тогда как все остальные переменные w_j равны 0. Покажем, что

$$L(R_{2q}) \leqslant 2L(R_q) + d_2 q, \tag{2}$$

где d_2 — некоторая константа, зависящая от базиса. Схема, которая реализует R_{2q}, показана на рис. 3, где $\tilde x'$, $\tilde x''$, $\tilde u'$, $\tilde u''$, $\tilde s'$ и $\tilde s''$ — наборы переменных $(x_1, \ldots, x_q)$, $(x_{q+1}, \ldots, x_{2q})$, $(u_1, \ldots, u_q)$, $(u_{q+1}, \ldots, u_{2q})$, $(s_1, \ldots, s_{p-1})$ и (s_p, s_{p+1}) соответственно. Блок M вычисляет набор $\tilde\tau = (\tau_1, \ldots, \tau_{p+1})$, для которого $|\tilde\tau| = \|\tilde u'\|$. Блок Σ вычисляет набор $\tilde\sigma = (\tilde\sigma', \tilde\sigma'')$, где $\tilde\sigma' = (\sigma_1, \ldots, \sigma_{p-1})$, $\tilde\sigma'' = (\sigma_p, \sigma_{p+1}, \sigma_{p+2})$, для которого

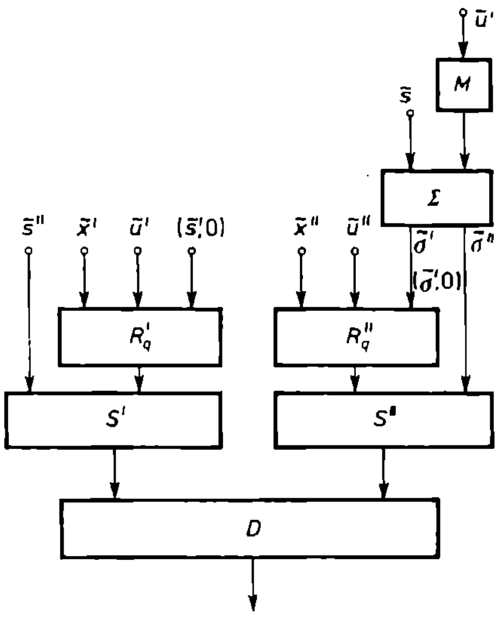

Рис. 3

$|\tilde{\sigma}| = |\tilde{s}| + |\tilde{\tau}|$, а блоки R'_q и R''_q реализуют системы функций R_q от переменных $(\tilde{x}', \tilde{u}', (\tilde{s}', 0))$ и $(\tilde{x}'', \tilde{u}'', (\tilde{\sigma}', 0))$ соответственно. Блок S' (соответственно S'') имеет $4q$ выходов и сдвигает выходы блока R'_q (соответственно R''_q) на $q|\tilde{s}''|$ (соответственно $q|\tilde{\sigma}''|$), разрядов вправо, присваивая нулевые значения „свободным" выходным переменным. Блок D выполняет поразрядную дизъюнкцию выходов блоков S' и S''. Неравенство (2) следует из того, что блоки M, Σ, S', S'' и D можно реализовать с линейной относительно числа их входов сложностью. С помощью (2) легко показать, что для некоторой константы d_3, зависящей от базиса, и любого $p = 1, 2, \ldots$

$$L(R_{2^p}) \leqslant d_3 p \cdot 2^p.$$

Схему, которая реализует функцию g_n и имеет сложность, удовлетворяющую требованиям леммы, можно построить из двух схем R_q, где $q = 2^{p-1}$, а $p =]\log_2 2n[+1$, и схемы сравнения двух q-разрядных наборов. На входы первой схемы R_q подаются наборы $(\tilde{x}^{2n}, \tilde{O}^{q-2n})$, $(\tilde{u}^{2n}, \tilde{O}^{q-2n})$ и набор $\tilde{\alpha}$, для которого $|\tilde{\alpha}| = q - \min\{\|\tilde{u}\|, \|\tilde{v}\|\}$, а на входы второй схемы R_q — наборы $(\tilde{y}^{2n}, \tilde{O}^{q-2n})$, $(\tilde{v}^{2n}, \tilde{O}^{q-2n})$ и $\tilde{\alpha}$. Схема сравнения сравнивает первые q выходов указанных схем R_q. Так как сложность схемы, вычисляющей набор $\tilde{\alpha}$, и сложность схемы сравнения линейны относительно q, сложность всей схемы, реализующей функцию g_n, определяется сложностью схем R_q и имеет порядок $n\log n$.

Результаты данной статьи были получены при обсуждении проблемы на одном из семинаров в международном математическом центре им. С. Банаха.

Литература

[1] A. Albrecht, *Komplexitatstheoretische Aspecte des Antwurfs von* VLSI-*Systemen*, Prepr. Humboldt-Univ. Berlin, Sect. Math. 28 (1982), 36.

[2] —, *О схемах из клеточных элементов*, Проблемы кибернетики, вып. 33, М., Наука (1978), 209–214.

[3] J. Hromkovic, *Linear lower bounds on unbounded fan-in Boolean circuits*, Information Processing Letters 21 (2), 71–75.

[4] С. С. Кравцов, *О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов*, Проблемы кибернетики, вып. 19, М., Наука (1967), 274–284.

[5] О. Б. Лупанов, *О синтезе некоторых классов управляющих систем*, Проблемы кибернетики, вып. 10, М., Физматгиз 1963, 63–97.

[6] C. H. Papadimitriou, M. Sipser, *Communication complexity*, J. of Computer and System Sciences 28 (2) (1984), 261–269.

[7] C. D. Thompson, *A complexity theory for* VLSI, Ph. D. dissertation, Dept. Comput. Sci., Carnegie-Mellon Univ., Pittsburgh, PA, August 1980.

[8] Н. А. Шкаликова, *О сложности реализации некоторых функций клеточными схемами*, Сборник работ по математической кибернетике, вып. 1, М., ВЦ АН СССР (1976), 102–115.

[9] —, *О соотношении сложностей плоских и объемных схем из функциональных элементов*, Методы дискретного анализа в оценках сложности управляющих систем, вып. 38, Новосибирск (1982), 87 107.

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