ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь – март 1995. Том 2, № 1, 7–20

УДК 519.6

О СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ СХЕМАМИ В ОДНОМ БЕСКОНЕЧНОМ БАЗИСЕ *)

О. М. Касим-Заде

Изучается сложность реализации булевых функций схемами из функциональных элементов в бесконечном базисе AC, состоящем из всевозможных антицепных булевых функций, т. е. функций, принимающих значение единица лишь на попарно несравнимых наборах. Показано, что при $n \to \infty$ порядок роста сложности реализации линейной функции от n переменных схемами в базисе AC не меньше $(n/\ln n)^{1/2}$. Установлено, что наибольшая сложность булевых функций n переменных при реализации схемами в базисе AC по порядку роста заключена между $(n/\ln n)^{1/2}$ и n.

Булева функция, принимающая значение единица лишь на попарно несравнимых наборах, называется *антицепной*. Обозначим через AC множество антицепных функций. Нетрудно убедиться, что AC является функционально полным и замкнутым относительно операций подстановки констант и отождествления переменных.

Рассмотрим реализацию булевых функций схемами из функциональных элементов в бесконечном базисе AC. Под *сложностью схемы* понимаем число входящих в нее элементов. Введем обозначения:

$L(S)$ — сложность схемы S,

$L(f)$ — наименьшая сложность реализации функции f схемами в базисе AC,

$L(n)$ — наибольшая сложность реализации функций n переменных.

В [1] получены оценки

$$n^{1/3} \preccurlyeq L(n) \leqslant n + 1, \qquad n \to \infty.$$

Нижняя оценка вытекает из установленной в [1] нижней оценки $L(l_n) \succcurlyeq n^{1/3}$ сложности реализации линейной функции $l_n = x_1 \oplus \ldots \oplus x_n$ от n переменных.

В данной работе получена более точная нижняя оценка сложности реализации линейных функций схемами в базисе AC.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-01-01527).

Теорема А. *При $n \to \infty$ имеет место оценка*

$$L(l_n) > (n/\ln n)^{1/2}.$$

Соединяя нижнюю оценку из теоремы А с верхней оценкой из [1], приходим к следующей теореме.

Теорема В. *При $n \to \infty$ имеют место оценки*

$$(n/\ln n)^{1/2} \preccurlyeq L(n) \leqslant n + 1.$$

Цель данной работы — доказательство теоремы А. Мы применим вариант известного метода подстановки констант, обычно используемого для вывода нижних оценок в конечных базисах. Рассматривая схему S в бесконечном базисе AC, реализующую линейную функцию l_n, зададимся некоторым натуральным числом s, $s \leqslant n$, и осуществим следующую процедуру.

Если в схеме S имеется элемент, у которого число входов, присоединенных к входам схемы, меньше s, то замещаем такие входы константой 0; при этом число входов схемы уменьшится на величину, не превосходящую $s - 1$. В результате получаем новую схему S_1, которая реализует линейную функцию от $n_1 > n - s + 1$ переменных.

По построению в схеме S_1 число элементов, имеющих входы, присоединенные к входам схемы, по меньшей мере на единицу меньше, чем в исходной схеме S.

Применим описанную процедуру к полученной схеме S_1 и т. д. до тех пор, пока это возможно. Если удалось применить описанную процедуру k раз, то $L(S) \geqslant k$. Если k велико, то для сложности исходной схемы S получается достаточно высокая нижняя оценка. Если k мало, то построенная на k-м шаге схема S_k реализует линейную функцию от $m \geqslant n - k(s-1)$ переменных, причем в этом случае m оказывается достаточно большим. Кроме того, схема S_k будет s-регулярной (см. определение ниже).

Для оценки сложности s-регулярных схем применяется другой метод. Считаем, что схема, реализующая функцию f, одновременно реализует и всякую частичную функцию, совпадающую на своей области определения с функцией f. Если дана s-регулярная схема, реализующая линейную функцию от m переменных, то по отношению к этой схеме осуществляется определение частичных функций, реализуемых этой схемой. При этом каждое последующее уменьшение осуществляется так, что по меньшей мере один из элементов схемы, реализовавших в предыдущей области частичную функцию, отличную от констант, в

новой области реализует функцию, равную константе. Ввиду специфики базиса AC и s-регулярности схемы число таких шагов велико по отношению к m. Следовательно, сложность рассматриваемой схемы достаточно велика.

Доказательство разбито на три части:

— описывается используемый вариант метода подстановки констант,

— доказываются комбинаторные леммы и вспомогательные утверждения о булевых функциях, используемых при рассмотрении s-регулярных схем,

— изучаются s-регулярные схемы и доказывается основной результат.

§ 1. Схемы в базисе AC и подстановка констант

Схема S называется *приведенной*, если на выходе каждого ее элемента реализуется функция, отличная от константы, а различные входы присоединены к различным вершинам схемы.

Через $P(S)$ обозначим число элементов схемы S, у которых по меньшей мере один из входов присоединен к входам схемы. Очевидно, что $L(S) \geqslant P(S)$ для любой схемы S.

Ввиду замкнутости базиса AC относительно операций подстановки констант и отождествления переменных справедлива

Лемма 1.1. *Для любой схемы S в базисе AC, реализующей отличную от константы функцию f, существует приведенная схема S' в базисе AC, реализующая функцию f и такая, что $L(S') \leqslant L(S)$ и $P(S') \leqslant P(S)$.*

Пусть $s \in \mathbf{N}$. Приведенную схему S будем называть *s-регулярной*, если для любого элемента e из схемы S число входов этой схемы, к которым присоединены входы элемента e, либо равно нулю, либо не меньше s.

Лемма 1.2. *Пусть n и s целые, $n \geqslant 2$, $s \geqslant 2$, и пусть приведенная схема S в базисе AC реализует линейную функцию l_n от n переменных и не является s-регулярной. Тогда существуют целое неотрицательное число n_1, $n - (s-1) \leqslant n_1 \leqslant n$, и приведенная схема S_1 в базисе AC, реализующая линейную функцию l_{n_1} и такая, что $L(S_1) \geqslant L(S)$, $P(S_1) \leqslant P(S) - 1$.*

Доказательство. Так как схема S не является s-регулярной и $n \geqslant 2$, имеется элемент e схемы S, входы которого присоединены менее чем к s входам схемы S. Пусть r — число указанных входов схемы, $1 \leqslant r \leqslant s-1$, и $x_{i_1}, \ldots, x_{i_r}$ — переменные, приписанные этим входам. Осуществим подстановку констант $x_{i_r} = \ldots = x_{i_r} = 0$ в функцию l_n, а в схеме S входы переменных $x_{i_1}, \ldots, x_{i_r}$ заменим константой 0. При этом функция l_n перейдет в функцию l_{n_1} от оставшихся $n_1 = n - r$

переменных, где $n_1 > n-(s-1)$, а схема S перейдет в некоторую схему S', реализующую функцию l_{n_1}. Поскольку элемент e уже не имеет входов, присоединенных к входам схемы S', получаем $P(S') < P(S)-1$.

Заметим, что схема S не является приведенной. Используя лемму 1.1, перейдем от схемы S' к соответствующей приведенной схеме S_1, реализующей ту же функцию l_{n_1}. Легко видеть, что $L(S_1) \leqslant L(S)$ и $P(S_1) \leqslant P(S') \leqslant P(S) - 1$. Лемма 1.2 доказана.

Лемма 1.3. *Пусть n, n_0, s целые, $n \geqslant 2$, $n > n_0 \geqslant 1$, $s \geqslant 2$. Тогда справедливо неравенство $L(l_n) \geqslant (n-n_0)/(s-1)$ или для некоторого m, $n_0 < m \leqslant n$, существует s-регулярная схема S_0, реализующая функцию l_m и такая, что $L(l_n) \geqslant L(S_0)$.*

Доказательство. Пусть S — минимальная по числу элементов приведенная схема, реализующая функцию l_n. В силу леммы 1.1 имеем $L(S) = L(l_n)$. Если схема S является s-регулярной, полагаем $m = n$, $S_0 = S$, и лемма 1.3 доказана.

Если схема S не является s-регулярной, в соответствии с леммой 1.2 построим приведенную схему S_1, реализующую функцию l_{n_1} от $n_1 \geqslant n-(s-1)$ переменных и такую, что $L(S_1) \leqslant L(S)$, $P(S_1) \leqslant P(S)-1$.

Если $n_1 \leqslant 1$ или схема S_1 является s-регулярной, построение закончено.

Если $n_1 \geqslant 2$ и схема S_1 не является s-регулярной, в соответствии с леммой 1.2 построим приведенную схему S_2, реализующую функцию l_{n_2} от $n_2 \geqslant n_1 - (s-1) \geqslant n - 2(s-1)$ переменных и такую, что $L(S_2) \leqslant L(S_1) \leqslant L(S)$, $P(S_2) \leqslant P(S_1) - 1 \leqslant P(S) - 2$ и т. д.

В результате после k шагов будет построена приведенная схема S_k, реализующая функцию l_{n_k} от $n_k \geqslant n-k(s-1)$ переменных и такая, что $L(S_k) \leqslant L(S)$, $P(S_k) \leqslant P(S)-k$, причем $n_k \leqslant 1$ либо схема S_k является s-регулярной.

Если $n_k \leqslant n_0$, то $L(l_n) = L(S) \geqslant P(S) \geqslant P(S_k)+k \geqslant k$, а поскольку $n_k > n - k(s-1)$, имеем $k > (n-n_0)/(s-1)$. Поэтому $L(l_n) \geqslant (n-n_0)/(s-1)$.

Если $n_k > n_0$, то $n_k \geqslant 2$, и схема S_k является s-регулярной. Полагая $m = n_k$ и $S_0 = S_k$, получаем $L(l_n) = L(S) \geqslant L(S_k) = L(S_0)$. Лемма 1.3 доказана.

§ 2. Комбинаторные леммы

Двоичным n-мерным кубом B_2^n называется множество всевозможных наборов длины n из нулей и единиц.

Цепью в кубе B_2^n называется подмножество C, $C \subseteq B_2^n$, в котором любые два набора сравнимы.

Длиной цепи называется число наборов, входящих в цепь.

Всякая цепь C содержит

— *наименьший набор,* т. е. набор $\widetilde{\alpha} \in C$ такой, что $\widetilde{\alpha} \leqslant \widetilde{\beta}$ для всех $\widetilde{\beta} \in C$,

— *наибольший набор,* т. е. набор $\widetilde{\gamma} \in C$ такой, что $\widetilde{\beta} \leqslant \widetilde{\gamma}$ для всех $\widetilde{\beta} \in C$.

Наименьший и наибольший наборы цепи C будем обозначать через $m(C)$ и $M(C)$ соответственно.

Цепь назовем *плотной*, если в ней любые два набора, непосредственно следующие друг за другом (при естественном упорядочении по возрастанию), различаются ровно в одной компоненте.

Двоичный набор длины n, состоящий только из нулей, обозначим через $\widetilde{0}^n$, а набор, состоящий только из единиц, — через $\widetilde{1}^n$. Плотная цепь, содержащая наборы $\widetilde{0}^n$ и $\widetilde{1}^n$, называется *максимальной.* Всякая максимальная цепь в кубе B_2^n имеет длину $n+1$. Число различных максимальных цепей в кубе B_2^n равно $n!$.

Весом набора $\widetilde{\alpha}$ называется число его единичных компонент (обозначается через $\|\widetilde{\alpha}\|$).

Пусть $\widetilde{\alpha}$ и $\widetilde{\beta}$ — два набора из куба B_2^n такие, что $\widetilde{\alpha} \leqslant \widetilde{\beta}$. Множество наборов $\widetilde{\gamma}$, $\widetilde{\gamma} \in B_2^n$, удовлетворяющих неравенствам $\widetilde{\alpha} \leqslant \widetilde{\gamma} \leqslant \widetilde{\beta}$, называется *интервалом куба* B_2^n. *Рангом интервала* называется число совпадающих компонент наборов $\widetilde{\alpha}$ и $\widetilde{\beta}$, определяющих этот интервал. Под *весом интервала* понимается вес набора $\widetilde{\alpha}$. Очевидно, что вес любого интервала не превосходит его ранга.

Как известно, имеется взаимно однозначное соответствие между интервалами куба B_2^n и элементарными конъюнкциями от переменных $x_1, \ldots, x_n$: каждому интервалу I куба B_2^n ранга r соответствует некоторая элементарная конъюнкция вида $x_{i_1}^{\sigma_1} \ldots x_{i_r}^{\sigma_r}$, где $1 \leqslant i_1 < \ldots < i_r \leqslant n$, $\sigma_1, \ldots, \sigma_r \in \{0,1\}$. Эта конъюнкция принимает значение 1 на тех и только тех наборах из куба B_2^n, которые принадлежат интервалу I. Легко видеть, что при этом вес интервала I равен весу набора $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_r)$.

Нам понадобятся некоторые утверждения о числе максимальных цепей, имеющих заданные размеры пересечения с заданным интервалом n-мерного куба.

Лемма 2.1. *Пусть n, r, k, a целые, $0 \leqslant k \leqslant r \leqslant n$, $0 \leqslant a \leqslant n-r$, и пусть I — интервал куба B_2^n ранга r и веса k. Тогда число максимальных цепей в кубе B_2^n, имеющих с интервалом I в точности $a+1$ общих вершин, равно величине*

$$\binom{n-a-1}{r-1}\binom{r}{k}^{-1}\binom{n}{r}^{-1} n!. \tag{2.1}$$

Доказательство. Пусть C — максимальная цепь, имеющая с интервалом I ровно $a+1$ общих вершин. Ясно, что пересечение $C \cap I$ является плотной цепью длины $a+1$. Пусть $\widetilde{\alpha} = m(C \cap I)$ — наименьший и $\widetilde{\beta} = M(C \cap I)$ — наибольший наборы этой цепи. Тогда $\widetilde{\alpha}$ и $\widetilde{\beta}$ удовлетворяют следующим условиям:

$$\widetilde{\alpha}, \widetilde{\beta} \in I, \quad \widetilde{\alpha} \leqslant \widetilde{\beta}, \quad \|\widetilde{\beta}\| = \|\widetilde{\beta}\| + a. \tag{2.2}$$

Цепь C представим в виде объединения $C = C_1 \cup C_2 \cup C_3$ трех плотных цепей C_1, C_2, C_3 таких, что

$$m(C_1) = \widetilde{0}^n, \quad M(C_1) = \widetilde{\alpha}, \quad C_1 \cap I = \{\widetilde{\alpha}\}, \tag{2.3}$$

$$m(C_2) = \widetilde{\alpha}, \quad M(C_2) = \widetilde{\beta}, \tag{2.4}$$

$$m(C_3) = \widetilde{\beta}, \quad M(C_3) = \widetilde{1}^n, \quad C_3 \cap I = \{\widetilde{\beta}\}. \tag{2.5}$$

Очевидно, что $C_2 = C \cap I$. Легко видеть, что всякой максимальной цепи C в кубе B_2^n такой, что $|C \cap I| = a+1$, однозначно соответствует набор $(\widetilde{\alpha}, \widetilde{\beta}, C_1, C_2, C_3)$, удовлетворяющий условиям (2.2)–(2.5). С другой стороны, всякому такому набору однозначно соответствует некоторая максимальная цепь, имеющая с интервалом I ровно $a+1$ общих вершин. Таким образом, искомое число максимальных цепей равно числу наборов $(\widetilde{\alpha}, \widetilde{\beta}, C_1, C_2, C_3)$, удовлетворяющих условиям (2.2)–(2.5).

Введем дополнительный числовой параметр $t = \|\widetilde{\alpha}\| - k$. Нетрудно убедиться, что для всякого набора $\widetilde{\alpha}$, удовлетворяющего условиям (2.2), выполняются неравенства $k \leqslant \|\widetilde{\alpha}\| \leqslant n-r-a+k$. Следовательно, параметр t принимает значения в интервале $[0, n-r-a]$. Фиксируем произвольное значение t из этого интервала и подсчитаем число наборов $(\widetilde{\alpha}, \widetilde{\beta}, C_1, C_2, C_3)$, удовлетворяющих условиям (2.2)–(2.5) и дополнительному условию

$$\|\widetilde{\alpha}\| = k + t. \tag{2.6}$$

Легко видеть, что число пар наборов $\widetilde{\alpha}$, $\widetilde{\beta}$, удовлетворяющих условиям (2.2) и (2.6), равно величине

$$\binom{n-r}{t}\binom{n-r-t}{a}.$$

Известно [2], что для любых двух наборов $\widetilde{\gamma}, \widetilde{\delta} \in B_2^n$, удовлетворяющих условиям $\widetilde{\gamma} \leqslant \widetilde{\delta}$, $\|\widetilde{\delta}\| - \|\widetilde{\gamma}\| = s$, число плотных цепей с наименьшим набором $\widetilde{\gamma}$ и наибольшим набором $\widetilde{\delta}$ равно $s!$. Используя этот факт, нетрудно убедиться в следующем:

число цепей C_1 с условиями (2.3) равно $(k+t-1)!k$,

число цепей C_2 с условиями (2.4) равно $a!$,
число цепей C_3 с условиями (2.5) равно $(n-k-a-t-1)!(r-k)$.

Следовательно, число наборов $(\widetilde{\alpha}, \widetilde{\beta}, C_1, C_2, C_3)$, удовлетворяющих условиям (2.2)–(2.6), равно величине

$$\binom{n-r}{t}\binom{n-r-t}{a}(k+t-1)!ka!(n-k-a-t-1)!(r-k)$$

$$= \frac{(n-r)!(k+t-1)!(n-k-a-t-1)!k(r-k)}{t!(n-r-t-a)!}.$$

Последнее равенство умножим и поделим на $(k-1)!(r-k-1)!r!n!$. Сгруппировав полученные сомножители, получаем выражение

$$\frac{(k-1+t)!}{t!(k-1)!}\frac{(n-k-a-1-t)!}{(n-r-a-t)!(r-k-1)!}\frac{k!(r-k)!}{r!}\frac{(n-r)!r!}{n!}n!$$

$$= \binom{k-1+t}{k-1}\binom{n-k-a-1-t}{r-k-1}\binom{r}{k}^{-1}\binom{n}{r}^{-1}n!. \qquad (2.7)$$

Теперь остается просуммировать (2.7) по всем t из интервала $[0, n-r-a]$ и привести полученную сумму к виду (2.1). Для этого воспользуемся известным комбинаторным равенством

$$\sum_{t=0}^{s}\binom{p+t}{p}\binom{q+s-t}{q} = \binom{p+q+s+1}{p+q+1},$$

которое справедливо при любых целых неотрицательных p, q, s (см. [3, с. 268, задача 2.13(3)]). Полагая в равенстве $p = k-1$, $q = r-k-1$, $s = n-r-a$, находим

$$\sum_{t=0}^{n-r-a}\binom{k-1+t}{k-1}\binom{n-k-a-1-t}{r-k-1} = \binom{n-a-1}{r-1}.$$

Следовательно, рассматриваемая сумма выражений (2.7) равна выражению (2.1). Лемма 2.1 доказана.

Лемма 2.2. *В условиях леммы* 2.1 *число максимальных цепей в кубе* B_2^n, *имеющих с интервалом* I *не менее* $a+1$ *общих вершин, равно величине*

$$\binom{n-a}{r}\binom{r}{k}^{-1}\binom{n}{r}^{-1}n!. \qquad (2.8)$$

Доказательство. В известном комбинаторном тождестве

$$\sum_{t=p}^{s}\binom{t}{p}\equiv\binom{s+1}{p+1},$$

которое справедливо при любых целых неотрицательных s, p, $s\geqslant p$ (см. [3, с. 253, задача 1.15(8)]), положим $s=n-a-1$, $p=r-1$ и найдем сумму

$$\sum_{b=a}^{n-r}\binom{n-b-1}{r-1}=\sum_{i=r-1}^{n-a-1}\binom{i}{r-1}=\binom{n-a}{r}.$$

Учитывая, что в силу леммы 2.1 число максимальных цепей в кубе B_2^n, имеющих с интервалом I в точности $b+1$ общих вершин, равно величине

$$\binom{n-b-1}{r-1}\binom{r}{k}^{-1}\binom{n}{r}^{-1}n!,$$

получаем искомое выражение (2.8). Лемма 2.2 доказана.

Лемма 2.3. *Пусть n, r, k, a целые, $1\leqslant r\leqslant n$, $0\leqslant k\leqslant r$, $a\geqslant 0$, и пусть I — интервал куба B_2^n ранга r и веса k. Тогда число максимальных цепей в кубе B_2^n, имеющих с интервалом I не менее $a+1$ общих вершин, не превосходит величины*

$$\binom{r}{k}^{-1}e^{-ar/n}n!. \tag{2.9}$$

Доказательство. Если $a\leqslant n-r$, то в соответствии с леммой 2.2 число максимальных цепей в кубе B_2^n, имеющих с интервалом I не менее $a+1$ общих вершин, дается выражением (2.8). Чтобы убедиться, что выражение (2.9) действительно является верхней оценкой выражения (2.8), достаточно воспользоваться известным неравенством

$$\binom{n-a}{r}\binom{n}{r}^{-1}\leqslant e^{-ar/n},$$

которое справедливо при любых целых неотрицательных n, a, r, $r\leqslant n-a$ (см. [3, с. 277, задача 4.11(3)]). Остается заметить, что любая цепь в кубе B_2^n имеет с интервалом I не более $n-r+1$ общих вершин и, следовательно, если $a>n-r$, то число максимальных цепей в кубе B_2^n, имеющих с интервалом I не менее $a+1$ общих вершин, равно нулю, тогда как величина, определяемая выражением (2.9), положительна. Лемма 2.3 доказана.

§ 3. Некоторые свойства булевых функций

Все $n!$ различных максимальных цепей в кубе B_2^n занумеруем произвольным образом числами от 1 до $n!$. Цепь с номером i, $1 \leqslant i \leqslant n!$, обозначим через D_i. Нумерацию цепей будем считать фиксированной до конца статьи. Пусть $R_n = \{1, \ldots, n!\}$. Для любой булевой функции f от n переменных через N_f обозначим множество вершин куба B_2^n, на которых функция f принимает значение единица.

Лемма 3.1. *Пусть n, r и a целые, $a \geqslant 0$, $1 \leqslant r \leqslant n$. Предположим, что $g'(x_{i_1}, \ldots, x_{i_r})$ — функция из AC, существенно зависящая от r переменных, причем $1 \leqslant i_1 \leqslant \ldots \leqslant i_r \leqslant n$, и функция $g(x_1, \ldots, x_n)$ отличается от $g'(x_1, \ldots, x_n)$ лишь наличием $n - r$ несущественных переменных. Тогда верна оценка*

$$|K| \leqslant e^{-ar/n} n!,$$

где K — множество номеров i, $i \in R_n$, цепей D_i в кубе B_2^n таких, что $|D_i \cap N_g| \geqslant a + 1$.

Доказательство. Рассмотрим представление функции g' в виде совершенной дизъюнктивной нормальной формы (ДНФ):

$$g'(y_1, \ldots, y_r) = \bigcup_{j=1}^{M} y_1^{\sigma_{j1}} \ldots y_r^{\sigma_{jr}},$$

где $M = |N_{g'}|$. Тогда $N_{g'} = \{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_M\}$, где

$$\tilde{\sigma}_1 = (\tilde{\sigma}_{11}, \ldots, \tilde{\sigma}_{1r}), \ldots, \tilde{\sigma}_M = (\sigma_{M1}, \ldots, \sigma_{Mr}).$$

Для каждого j, $1 \leqslant j \leqslant M$, положим $k_j = \|\tilde{\sigma}_j\|$. Поскольку $g' \in AC$, наборы $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_M$ попарно несравнимы, и в соответствии с известным неравенством Любеля [2] выполняется соотношение

$$\sum_{j=1}^{M} \binom{r}{k_j}^{-1} \leqslant 1.$$

Функция $g(x_1, \ldots, x_n)$ допускает представление в виде ДНФ:

$$g(x_1, \ldots, x_n) = \bigcup_{j=1}^{M} x_{i_1}^{\sigma_{j1}} \ldots x_{i_r}^{\sigma_{jr}}.$$

Для каждого j, $1 \leqslant j \leqslant M$, конъюнкция $x_{i_1}^{\sigma_{j1}} \ldots x_{i_r}^{\sigma_{jr}}$, отвечающая набору $\tilde{\sigma}_j = (\tilde{\sigma}_{j1}, \ldots, \tilde{\sigma}_{jr})$, определяет в кубе B_2^n некоторый интервал I_j.

Поскольку наборы $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_M$ попарно несравнимы, наборы из различных интервалов $I_1, \ldots, I_M$ также несравнимы. Следовательно, каждая из цепей $D_1, \ldots, D_{n!}$ может иметь общие вершины лишь с одним из указанных интервалов. Поэтому для всякой цепи D_i такой, что пересечение $D_i \cap N_g$ непусто, существует единственный интервал I_j такой, что $D_i \cap N_g = D_i \cap I_j$. Обозначим через K_j множество номеров цепей D_i таких, что $|D_i \cap I_j| \geqslant a+1$. Из сказанного выше следует, что K есть объединение множеств $K_1, \ldots, K_M$. В соответствии с леммой 2.3 для каждого j имеем

$$|K_j| \leqslant \binom{r}{k_j}^{-1} e^{-ar/n} n!.$$

Таким образом, верно соотношение

$$|K| \leqslant \sum_{j=1}^{M} \binom{r}{k_j}^{-1} e^{-ar/n} n!,$$

из которого с учетом неравенства Любеля получаем

$$|K| \leqslant e^{-ar/n} n!.$$

Лемма 3.1 доказана.

Ниже используются частичные булевы функции. Пусть A — произвольное подмножество вершин куба B_2^n. *Частичной булевой функцией f от n переменных с областью определения A* называется отображение $f : A \to \{0,1\}$; вне множества A функция f не определена. Множество всех частичных булевых функций от n переменных с областью определения A обозначим через $P_2^n(A)$. Если $A \subseteq B$ и $f \in P_2^n(B)$, то функция $g \in P_2^n(A)$, совпадающая с f на всех наборах из множества A, называется *сужением функции f на множество A* и обозначается через $f|_A$. Сужения на множество A функций, равных константам 0 и 1, обозначаем через $0|_A$ и $1|_A$, а сужение функции, равной переменной x_i, — через $x_i|_A$. Положим

$$C^n(A) = \{0|_A, 1|_A\}, \quad U^n(A) = \{0|_A, 1|_A, x_1|_A, \ldots, x_n|_A\}.$$

Будем рассматривать сужения линейных функций на множества, представляющие собой цепи в кубах соответствующей размерности. В дальнейшем потребуется простое свойство таких сужений, сформулированное в следующей лемме.

Лемма 3.2. *Если C — произвольная (не обязательно плотная) цепь в кубе B_2^n, длина которой больше $(n+3)/2$, то $l_n|_C \notin U^n(C)$.*

При доказательстве леммы 3.2 используется следующая очевидная

Лемма 3.3. *Если C — плотная цепь в кубе B_2^n, то линейная функция l_n принимает каждое из двух значений 0 и 1 не более чем на $(|C|+1)/2$ наборах цепи C.*

§ 4. Оценка сложности s-регулярных схем

Пусть схема S в базисе AC имеет n входов, которым приписаны переменные $x_1, \ldots, x_n$, и реализует всюду определенную функцию $g(x_1, \ldots, x_n)$. Пусть A — произвольное подмножество вершин куба B_2^n и f — частичная функция от n переменных с областью определения A такая, что $g|_A = f$. В этом случае будем говорить, что *схема S реализует на множестве A частичную функцию f*.

Для любого элемента e схемы S обозначим через $g_e(x_1, \ldots, x_n)$ функцию от входных переменных $x_1, \ldots, x_n$, реализуемую на выходе элемента e. Для любого множества $A \subseteq B_2^n$ обозначим через $Q(S, A)$ множество элементов e схемы S таких, что $g_e|_A \in C^n(A)$. Число элементов в $Q(S, A)$ будем обозначать через $q(S, A)$.

Лемма 4.1. *Пусть n, s, p, a целые, $1 \leqslant s \leqslant n$, $p \geqslant 1$, $a \geqslant 0$, A — непустое подмножество вершин куба B_2^n. Предположим, что схема S в базисе AC имеет n входов, является s-регулярной и реализует на множестве A частичную функцию f такую, что $f \notin U^n(A)$. Пусть J — непустое подмножество множества R_n такое, что $|D_j \cap A| \geqslant p$ для каждого $j \in J$. Тогда существуют непустое подмножество $A' \subseteq A$ и подмножество $J' \subseteq J$ такие, что*

$$q(S, A') \geqslant q(S, A) + 1,$$

$$|D_j \cap A'| \geqslant p - a \quad \textit{при каждом } j \in J',$$

$$|J'| \geqslant |J| - e^{-as/n} n!.$$

Доказательство. Поскольку $f \notin U^n(A)$, в схеме S имеются элементы, не входящие в множество $Q(S, A)$. Среди них найдется хотя бы один элемент, каждый вход которого присоединен к выходу некоторого элемента из $Q(S, A)$ или к некоторому входу схемы S. При этом по меньшей мере один из его входов присоединен к входу схемы. Зафиксируем любой из таких элементов и обозначим его через e.

Пусть r — число входов схемы S, к которым присоединены входы элемента e. Поскольку по меньшей мере один из входов элемента e присоединен к входу схемы, а схема S является s-регулярной, выполняется неравенство $r \geqslant s$.

Пусть $x_{i_1}, \ldots, x_{i_r}$ — переменные, приписанные входам схемы S, к которым присоединены входы элемента e, $1 \leqslant i_1 < \ldots < i_r \leqslant n$. Рассмотрим функцию $g_e(x_1, \ldots, x_n)$, реализуемую на выходе элемента e. Заметим, что в соответствии с определением множества $Q(S, A)$ на входы элемента e, присоединенные к выходам элементов из этого множества, поступают функции, сужения которых на множество A равны

константам. Поэтому на множестве A функция $g_e(x_1,\dots,x_n)$ совпадает с некоторой функцией $\varphi(x_{i_1},\dots,x_{i_r})$, которая получается из базисной функции, приписанной элементу e, соответствующей подстановкой констант. Так как базисная функция, приписанная элементу e, принадлежит AC, а базис AC замкнут относительно операции подстановки констант, функция φ также принадлежит AC. Поскольку $e \notin Q(S,A)$, функция φ не равна константе и, следовательно, существенно зависит от всех переменных $x_{i_1},\dots,x_{i_r}$.

Обозначим через $g(x_1,\dots,x_n)$ функцию n переменных, отличающуюся от $\varphi(x_{i_1},\dots,x_{i_r})$ лишь наличием $n-r$ несущественных переменных. Очевидно, что $g|_A = g_e|_A$. Положим $A' = A \setminus N_g$. В силу соотношения $g_e|_A \notin C^n(A)$ множество A' непусто, а в силу включения $A' \subseteq A$ имеем $Q(S,A') \supseteq Q(S,A)$. Учитывая очевидные соотношения $g_e|_{A'} = g|_{A'} = 0|_{A'}$, получаем $Q(S,A') \setminus Q(S,A) \supseteq \{e\}$, откуда $q(S,A') \geqslant q(S,A)+1$.

Отметим, что

$$|D_j \cap A| = |D_j \cap A'| + |D_j \cap A \cap N_g| \leqslant |D_j \cap A'| + |D_j \cap N_g|$$

для каждого j, $j \in R_n$. Следовательно, $|D_j \cap A'| \geqslant p - |D_j \cap N_g|$ для каждого $j \in J$. Обозначим через K множество номеров j, $j \in R_n$, цепей D_j таких, что $|D_j \cap N_g| \geqslant a+1$, и положим $J' = J \setminus K$. Тогда $|D_j \cap A'| \geqslant p-a$ для каждого $j \in J'$. Учитывая оценку $|K| \leqslant e^{-ar/n}n!$ из леммы 3.1 и неравенство $r \geqslant s$, приходим к неравенству $|J'| \geqslant |J| - e^{-as/n}n!$. Лемма 4.1 доказана.

Лемма 4.2. *Пусть n, s, a натуральные, $s \leqslant n$, t целое такое, что $t \geqslant 0$, $t < (n-1)/(2a)$, $t < e^{as/n}$, и S — s-регулярная схема в базисе AC, реализующая функцию l_n. Тогда существуют непустые множества*

$$A_0, A_1, \dots, A_{t+1} \subseteq B_2^n, \qquad A_0 \supseteq A_1 \supseteq \dots \supseteq A_{t+1},$$

и множества

$$J_0, J_1, \dots, J_{t+1} \subseteq R_n, \quad J_0 \supseteq J_1 \supseteq \dots \supseteq J_{t+1},$$

среди которых $J_0, J_1, \dots, J_t$ непусты, такие, что для каждого i, $0 \leqslant i \leqslant t$, выполнены следующие условия:

1) $q(S,A_i) \geqslant i$,
2) $|D_i \cap A_i| \geqslant n+1-ia$ *для каждого* $j \in J_i$,
3) $|J_i| \geqslant (1-ie^{-as/n})n!$.

Доказательство. Пусть $A_0 = B_2^n$, $J_0 = R_n$. Тогда условия 1–3 выполнены при $i=0$. Предположим, что для некоторого i, $0 \leqslant i \leqslant t$,

множества A_i, J_i, удовлетворяющие условиям 1–3, построены, причем A_i непусто.

Опишем построение множеств A_{i+1}, J_{i+1}. Ввиду неравенств

$$|J_i| \geqslant (1 - ie^{-as/n})n! \geqslant (1 - te^{-as/n})n! > 0$$

множество J_i непусто. Поэтому найдется число $k \in J_i$ такое, что

$$|D_k \cap A_i| \geqslant n + 1 - ia \geqslant n + 1 - ta > (n + 3)/2.$$

По лемме 3.2 имеем $l_n|_{D_k \cap A_i} \notin U^n(D_k \cap A_i)$, следовательно, $l_n|_{A_i} \notin U^n(A_i)$. Таким образом, на множестве A_i схема S реализует частичную функцию, не принадлежащую $U^n(A_i)$. По лемме 4.1 существуют непустое множество $A_{i+1} \subseteq A_i$ и множество $J_{i+1} \subseteq J_i$ такие, что

$$q(S, A_{i+1}) \geqslant q(S, A_i) + 1 \geqslant i + 1,$$

$$|D_j \cap A_{i+1}| \geqslant n + 1 - (i + 1)a \quad \text{для каждого } j \in J_{i+1},$$

$$|J_{i+1}| \geqslant (1 - (i + 1)e^{-as/n})n!\,.$$

Лемма 4.2 доказана.

Лемма 4.3. *Пусть n, s, a натуральные, $s \leqslant n$, и пусть s-регулярная схема S реализует функцию l_n. Тогда*

$$L(S) \geqslant \min(\lfloor (n - 1)/(2a) \rfloor, \lfloor e^{as/n} \rfloor).$$

Доказательство. Положим

$$t = \min(\lfloor (n - 1)/(2a) \rfloor, \lfloor e^{as/n} \rfloor) - 1.$$

Очевидно, что

$$t \leqslant (n - 1)/(2a) - 1 < (n - 1)/(2a), \quad t \leqslant e^{as/n} - 1 < e^{as/n}.$$

Если $t < 0$, то искомая нижняя оценка тривиальна. Если $t \geqslant 0$, то по лемме 4.2 существует непустое множество A_{t+1}, $A_{t+1} \subseteq B$, такое, что $q(S, A_{t+1}) \geqslant t + 1$. Остается заметить, что

$$L(S) \geqslant q(S, A_{t+1}) \geqslant t + 1.$$

Лемма 4.3 доказана.

§ 5. Завершение доказательства основного результата

Следующая лемма подводит итог предыдущим рассмотрениям.

Лемма 5.1. *Пусть n, n_0, s, a целые, $2 \leqslant s \leqslant n_0 < n$, $a \geqslant 0$. Тогда*

$$L(l_n) \geqslant \min((n - n_0)/(s-1), \lfloor n_0/(2a) \rfloor, \lfloor e^{as/n} \rfloor).$$

Доказательство. Согласно лемме 1.3 либо выполнено неравенство $L(l_n) \geqslant (n - n_0)/(s-1)$, либо для некоторого m, $n_0 < m \leqslant n$, существует s-регулярная схема S, реализующая функцию l_m и такая, что $L(l_m) \geqslant L(S_0)$. В последнем случае с учетом леммы 4.3 и неравенства $s \leqslant n_0 < m$ имеем

$$L(l_n) \geqslant L(S_0) \geqslant \min(\lfloor (m-1)/(2a) \rfloor, \lfloor e^{as/m} \rfloor) > \min(\lfloor n_0/(2a) \rfloor, \lfloor e^{as/n} \rfloor).$$

Объединяя обе оценки величины $L(l_n)$, получаем требуемое соотношение. Лемма 5.1 доказана.

Для завершения доказательства теоремы А положим в лемме 5.1 $n_0 = \lfloor n/2 \rfloor$, $s = \lceil (n \ln n)^{1/2} \rceil$, $a = \lceil (n \ln n)^{1/2} \rceil$. Очевидно, что при достаточно больших значениях n все условия леммы 5.1 выполнены. Остается заметить, что

$$(n - n_0)/(s-1) \asymp n_0/(2a) \asymp (n/\ln n)^{1/2}$$

при $n \to \infty$ и $as/n \geqslant (\ln n)/2$ при любом n, так что $e^{as/n} \geqslant n^{1/2}$. Применяя лемму 5.1, получаем искомую оценку. Теорема А доказана.

Автор выражает признательность О. Б. Лупанову за внимание к данной работе.

ЛИТЕРАТУРА

1. **Касим-Заде О. М.** О сложности схем в одном бесконечном базисе // Вестн. МГУ. Сер. 1. Математика, механика. 1994. № 6. С. 40–44.
2. **Айгнер М.** Комбинаторная теория. М.: Мир, 1982.
3. **Гаврилов Г. П., Сапоженко А. А.** Сборник задач по дискретной математике. М.: Наука, 1977.

Адрес автора:

РОССИЯ,
119899, Москва,
Воробьевы горы,
МГУ,
механико-матем. ф-т

Статья поступила

22 ноября 1994 г.