

УДК 519.6

О СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ В ТРЕХ КЛАССАХ СХЕМ В БАЗИСЕ, СОСТОЯЩЕМ ИЗ ВСЕХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ*)

М. И. Гринчук

Рассматривается реализация булевых функций схемами в бесконечном базисе, состоящем из всех симметрических функций, причем за вес (стоимость) элемента принимается число его входов. В этом базисе для трех классов схем — схем общего вида, схем без ветвления выходов (т. е. формул) и схем, каждая из которых состоит из одного элемента, получены асимптотически точные оценки функции Шеннона. Для одноэлементных схем приведен пример булевой функции, имеющей максимальную по порядку сложность.

Введение

Рассмотрим бесконечный базис $B = B_{\text{симм}}$, состоящий из элементов, реализующих всевозможные симметрические булевы функции; в качестве веса (стоимости) элемента берется число его входов.

Сложность схемы Σ , построенной из таких функциональных элементов, будем понимать как сумму весов всех составляющих ее элементов и обозначать $L(\Sigma)$.

В настоящей работе рассматриваются три класса схем (в базисе B):

- (1) схемы без ограничений;
- (2) схемы без ветвления выходов (формулы);
- (3) одноэлементные схемы.

Лемма 1. Любую булеву функцию f можно реализовать в базисе B схемами любого из указанных трех классов.

ДОКАЗАТЕЛЬСТВО. Базис B является полным — он содержит дизъюнкцию, конъюнкцию и отрицание. Поэтому в нем можно реализовать произвольную булеву функцию как схемами, так и формулами.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-01-01527), а также программы «Университеты России».

Известно, что любую булеву функцию можно получить отождествлением переменных из подходящей симметрической функции: для получения n -местной функции f достаточно использовать симметрическую функцию F от $2^n - 1$ переменных с характеристической последовательностью $\pi_0, \dots, \pi_{2^n-1}$, где π_i есть значение функции f на наборе, совпадающем с двоичной записью индекса i :

$$f(x_1, \dots, x_n) = F(\underbrace{x_1, \dots, x_1}_{2^{n-1}}, \underbrace{x_2, \dots, x_2}_{2^{n-2}}, \dots, \underbrace{x_{n-2}, x_{n-2}, x_{n-2}, x_{n-2}}_{2^2}, \underbrace{x_{n-1}, x_{n-1}}_{2^1}, \underbrace{x_n}_{2^0})$$

(в частности, подобное представление, но для вдвое большего числа аргументов функции F , описано в [1]). Лемма 1 доказана.

В силу леммы 1 для каждой булевой функции f определены (и конечны) величины

$$\begin{aligned} L(f) &= \min_{\Sigma \text{ реализует } f} L(\Sigma), \\ L_\Phi(f) &= \min_{\substack{\Sigma \text{ реализует } f; \\ \Sigma \text{ — формула}}} L(\Sigma), \\ L_\Sigma(f) &= \min_{\substack{\Sigma \text{ реализует } f; \\ \Sigma \text{ состоит из одного элемента}}} L(\Sigma) \end{aligned}$$

(заметим, что величина $L_\Sigma(f)$ — это минимально возможное число аргументов симметрической функции, из которой отождествлением переменных можно получить f).

Далее определены соответствующие функции Шеннона:

$$\begin{aligned} L(n) &= \max L(f), \\ L_\Phi(n) &= \max L_\Phi(f), \\ L_\Sigma(n) &= \max L_\Sigma(f), \end{aligned}$$

где максимумы берутся по всем n -местным булевым функциям f .

§ 1. Схемы и формулы

Теорема 1. При $n \rightarrow \infty$ справедливо соотношение $L(n) \sim 2^n/n$.

Доказательство. Верхняя оценка сложности следует из результата О. Б. Лупанова [2, теорема 11]:

$$L(n) < \frac{k}{k-1} \frac{2^n}{n} (1 + o(1)),$$

поскольку приведенный вес конечного базиса из всех симметрических функций от k переменных (этот базис является подмножеством базиса Б) есть $k/(k-1)$.

Устремляя k к $+\infty$, получаем

$$L(n) < \frac{2^n}{n}(1 + o(1)).$$

Нижняя оценка, как обычно, получается из мощностных соображений: если число $N(n, l)$ различных схем с n входами и сложности не выше l таково, что $N(n, l) < 2^{2^n}$, то $L(n) > l$.

Подсчет числа различных схем можно проводить непосредственно, однако можно также свести схемы в бесконечном базисе B к некоторым другим схемам, которые «комбинаторно эквивалентны» схемам из функциональных элементов в конечном базисе. Эта конструкция, возможно, представляет самостоятельный интерес, поэтому именно ею мы и воспользуемся.

Введем понятие F -схем, которые эквивалентны (по функционированию) схемам из симметрических элементов, имеют такую же сложность, но содержат лишь одно- и двухвыходовые элементы.

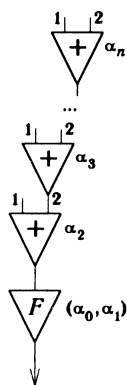
Пусть по определению F -схема состоит из следующих элементов:

— двухвыходовых $((+)$ -элементов), у которых входы различаются (будем говорить о первом и втором входах $(+)$ -элементов); $(+)$ -элементу приписывается число α , равное 0 или 1;

— одновыходовых (F -элементов), которым приписываются пары чисел вида (α_0, α_1) , где $\alpha_i \in \{0, 1\}$. Вес каждого элемента F -схемы положим равным 1.

На соединение элементов накладываются следующие ограничения:

- выходом схемы не может быть выход $(+)$ -элемента;
- выходы $(+)$ -элементов не ветвятся;
- выход $(+)$ -элемента не может подаваться на первый вход $(+)$ -элемента.



Очевидно, что любая F -схема, не содержащая «очевидно излишних» $(+)$ -элементов, т. е. элементов, выходы которых ни к чему не подключены, может быть представлена в виде объединения не содержащих общих элементов подсхем, каждая из которых представляет собой цепочку из одного F -элемента и, возможно, одного или нескольких $(+)$ -элементов (см. рисунок, изображающий цепочку из элементов, реализующую n -местную функцию $F : \{0, 1, \dots, n\} \rightarrow \{0, 1\}$, где

$F(i) = \alpha_i$). Далее всюду будут рассматриваться только схемы без «излишних» элементов.

Функционирование такой цепочки F -схемы отражает тот факт, что вычисление симметрической булевой функции $f(x_1, \dots, x_n)$ эквивалентно вычислению $F(x_1 + \dots + x_n)$, где знак «+» означает обычное сложение, а функция F задает отображение вида $\{0, 1, \dots, n\} \rightarrow \{0, 1\}$; (+)-элементы осуществляют сложение, а F -элементы — вычисление функции F . Конкретная функция F , вычисляемая тем или иным F -элементом, определяется пометками, приписанными элементам цепочки: последовательность значений $\{F(0), F(1), \dots, F(n)\}$ начинается парой чисел, приписанных F -элементу, а далее почленно «рассредоточена» по (+)-элементам. При этом цепочка из n элементов имеет n внешних входов и содержит $n + 1$ бит приписанной информации, что необходимо и достаточно для однозначного задания n -местной симметрической булевой функции f .

Тем самым указанная цепочка моделирует n -входовый симметрический элемент и имеет такую же (равную n) сложность. Поэтому между схемами в базисе B и $F@$ -схемами существует очевидное соответствие, сохраняющее сложность.

Но F -схемы являются схемами (с ограничениями) в конечном базисе, содержащем 2 вида двухвходовых элементов и 4 вида одновходовых. Поэтому для числа F -схем заданной сложности справедливы верхние оценки, установленные для схем в конечных базисах (см., например, [2, лемма 15]). Следствием этого является такая же, как для схем в базисах с приведенным весом 1, нижняя оценка функции Шеннона:

$$L(n) > \frac{2^n}{n}(1 - o(1)).$$

Теорема 1 доказана.

Для случая формул аналогично доказательству теоремы 1 устанавливается

Теорема 2. При $n \rightarrow \infty$ справедливо соотношение $L_\Phi(n) \sim 2^n / \log_2 n$.

§ 2. Схемы, состоящие из единственного элемента

Теорема 3. При любом $n \geq 1$ справедливо соотношение $2^n - n^2 \leq L_3(n) \leq 2^n - 1$.

Доказательство. Верхняя оценка была установлена в ходе доказательства леммы 1.

Нижняя оценка, как и в предыдущих случаях, будет получена из мощностных соображений. Предварительно отметим лишь то, что при $n < 5$ она тривиальна.

Пусть n -местная булева функция f получена из m -местной симметрической функции F :

$$f(x_1, \dots, x_n) = F(\underbrace{x_1, \dots, x_1}_{k_1}, \dots, \underbrace{x_n, \dots, x_n}_{k_n}), \quad (1)$$

где целые неотрицательные числа k_1, \dots, k_n связаны соотношением $k_1 + \dots + k_n \leq m$.

Известно, что неравенство $k_1 + \dots + k_n \leq m$ имеет $\binom{n+m}{n}$ решений в целых неотрицательных числах. Далее, на множестве $\{0, 1, \dots, m\}$ можно задать 2^{m+1} различных функций F . Поэтому число различных правых частей в (1) не превосходит

$$2^{m+1} \binom{n+m}{n}.$$

Для того чтобы со сложностью не выше m можно было реализовать все 2^{2^n} булевых функций от n аргументов, должно выполняться неравенство

$$2^{m+1} \binom{n+m}{n} \geq 2^{2^n},$$

которое не выполнено при $m < 2^n - n^2$ (в этом случае $\binom{n+m}{n} \leq (n+m)^n/n! \leq 2^{n^2}/n!$, т. е. при $n \geq 5$ получаем $2^{m+1} \binom{n+m}{n} < 2^{2^n}$). Тем самым теорема 3 доказана.

ЗАМЕЧАНИЕ 1. В работе [1] было отмечено, что $L_3(n) \leq 2^{n+1}$, и показано, что для функции

$$g_n = (x_1 \oplus x_2)(x_3 \oplus x_4) \dots (x_{n-1} \oplus x_n)$$

выполнена оценка $L_3(g_n) \geq 2^{n/2}$.

ЗАМЕЧАНИЕ 2. Нетрудно убедиться, что во всех трех рассмотренных классах схем наблюдается так называемый эффект Шеннона — почти все функции имеют асимптотически максимальную сложность.

§ 3. Пример почти самой сложной функции

Приведем, наконец, пример n -местной булевой функции f_n , для которой величина $L_3(f_n)$ по порядку совпадает с $L_3(n)$. Пусть

$$f_n(x_1, \dots, x_n) = x_1 x_2 \vee \bar{x}_1 x_2 x_3 \vee \bar{x}_1 \bar{x}_2 x_3 x_4 \vee \dots \vee \bar{x}_1 \bar{x}_2 \dots \bar{x}_{n-2} x_{n-1} x_n$$

(значением функции f_n на наборе $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ является тот элемент этого набора, который стоит сразу после первой единицы).

Пусть функция f_n реализована одним симметрическим элементом веса l , т. е. представлена в виде

$$f_n(x_1, \dots, x_n) = F(\lambda_1 x_1 + \dots + \lambda_n x_n),$$

где λ_i — неотрицательные целые числа, причем $\lambda_1 + \dots + \lambda_n = l$, а F — функция вида $\{0, 1, \dots, l\} \rightarrow \{0, 1\}$; далее сумму $\lambda_1 x_1 + \dots + \lambda_n x_n$ будем обозначать $\Lambda \tilde{x}$.

Будем говорить, что булевы наборы $\tilde{\alpha}$ и $\tilde{\beta}$ склеиваются, если $\Lambda \tilde{\alpha} = \Lambda \tilde{\beta}$. Очевидно, необходимым условием для этого является $f_n(\tilde{\alpha}) = f_n(\tilde{\beta})$.

Лемма 2. Булевы наборы вида $(0, \alpha_2, \alpha_3, \dots, \alpha_n)$ попарно не склеиваются.

ПОКАЗАТЕЛЬСТВО. Предположим, что наборы $\tilde{\alpha} = (0, \alpha_2, \alpha_3, \dots, \alpha_n)$ и $\tilde{\beta} = (0, \beta_2, \beta_3, \dots, \beta_n)$ склеиваются. Пусть эти наборы совпадают в первых $i-1$ разрядах ($1 \leq i \leq n$), и пусть, без уменьшения общности, $\alpha_i = 0$, $\beta_i = 1$.

Тогда должны склеиваться наборы $\tilde{\alpha}' = (0, \dots, 0, 1, 0, \alpha_{i+1}, \alpha_{i+2}, \dots, \alpha_n)$ и $\tilde{\beta}' = (0, \dots, 0, 1, 1, \beta_{i+1}, \beta_{i+2}, \dots, \beta_n)$, поскольку $\Lambda \tilde{\alpha} - \Lambda \tilde{\alpha}' = \Lambda \tilde{\beta} - \Lambda \tilde{\beta}'$. Но $f(\tilde{\alpha}') = 0 \neq 1 = f(\tilde{\beta}')$. Полученное противоречие доказывает лемму 2.

Лемма 3. Если имеется m попарно не склеивающихся наборов, то $l \geq m - 1$.

ПОКАЗАТЕЛЬСТВО. Достаточно заметить, что значения суммы $\Lambda \tilde{\alpha}$ — различные неотрицательные целые числа, не превосходящие l .

Из этих двух лемм сразу же вытекает

Теорема 4. При любом $n \geq 1$ выполнено неравенство $L_3(f_n) \geq (1/2)2^n - 1$.

ЗАМЕЧАНИЕ 3. Более тонкие рассуждения позволяют усилить эту оценку до $L_3(f_n) \geq (5/8)2^n - 1$, однако существеннее приблизить ее к 2^n не удастся: можно склеить наборы $(0, 1, 0, \alpha_4, \dots, \alpha_n)$ и $(1, 0, 1, \alpha_4, \dots, \alpha_n)$, выбрав коэффициенты $\lambda_1 = (1/4)2^n$, $\lambda_2 = (3/8)2^n$, $\lambda_k = 2^{n-k}$, $k = 3, \dots, n$, поэтому $L_3(f_n) \leq (7/8)2^n - 1$.

ЛИТЕРАТУРА

1. Smolensky R. On interpolation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates // Proc. 31st ann. sympos. on foundations of computer science. Los Alamitos: IEEE Comput. Soc. Press, 1990. V. 2. P. 628–631.
2. Лупанов О. Б. Асимптотические оценки сложности управляющих систем М.: Изд-во Моск. гос. ун-та, 1984.

Адрес автора:

Россия,
119899 Москва,
Воробьевы горы,
МГУ, мех.-мат. факультет

Статья поступила

20 ноября 1995 г.