УДК 519.71

ОБ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ В СЛОЖНОСТИ ОПЕРАТОРА СДВИГА*)

Д. Ю. ЧЕРУХИН

Показано, что сложность оператора сдвига в классе схем из функциональных элементов нелинейна тогда и только тогда, когда нелинейна сложность сети, в которую вписано семейство схем, реализующих каждый сдвиг по отдельности.

Одной из актуальных задач теории сложности является получение нелинейных нижних оценок сложности схем из функциональных элементов (СФЭ), реализующих явно заданные последовательности булевых функций (или операторов) [2, Гл. 8]. Получение нижних оценок реализаций некоторых операторов, в частности, оператора умножения чисел, представляет самостоятельный интерес. Известно, что нелинейность сложности оператора умножения следует из нелинейности сложности оператора сдвига [3, п. 3.1.1]. В настоящей заметке доказано, что сложность оператора сдвига нелинейна тогда и только тогда, когда нелинейна сложность сети, допускающей для каждой величины сдвига передачу информации от входов к соответствующим выходам, т. е. управление передачей информации в данной сети можно организовать без существенного увеличения сложности.

Пусть $n \in \mathbb{N}$, $r_n = \lceil \log_2 n \rceil$. *Оператором сдвига* (арифметическим, влево) называется оператор

$$\mathrm{SAL}_n : \{0,1\}^{n+r_n} \to \{0,1\}^{2n-1},$$

определённый следующим образом:

$$\mathrm{SAL}_n(x_{n-1}, \ldots, x_0,\ y_{r_n-1}, \ldots, y_0) = (x'_{2n-2-y}, \ldots, x'_{-y}), \tag{1}$$

где

$$y = \sum_{i=0}^{r_n-1} y_i 2^i, \qquad x'_i = \begin{cases} x_i, & \text{если } 0 \leqslant i < n, \\ 0 & \text{в противном случае.} \end{cases}$$

Переменные $x_{n-1}, \ldots, x_0$ в (1) называются *информационными*, а переменные $y_{r_n-1}, \ldots, y_0$ — *управляющими*. Результат настоящей заметки может быть легко перенесён на случай оператора циклического сдвига.

Будем рассматривать СФЭ, в которых элементами являются произвольные двуместные булевы функции. *Сетью* в данной заметке будем называть конечный ориентированный граф без ориентированных циклов, в котором входная степень каждой вершины равна 0 (в этом случае вершина называется *входом*) или 2; некоторые вершины отмечены и называются *выходами*. Другими словами, сетями являются каркасы рассматриваемых СФЭ и только они (*каркас*

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 02–01–00985), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.01) и программы "Университеты России" (проект УР 04.03.061).

схемы — сеть, полученная стиранием символов переменных у входов и символов функций у элементов). Сложностью сети называется сложность СФЭ (число элементов), каркасом которой сеть является.

Пусть C — СФЭ с входами $v_{n-1}, \dots, v_0$, реализующая на выходах $w_{n-1}, \dots, w_0$ тождественный (n,n)-оператор: функция, вычисляемая на выходе w_i $(0 \leqslant i < n)$, тождественно равна переменной, подаваемой на вход v_i. Тогда каркас схемы C назовём *информационной* сетью для входов $(v_{n-1}, \dots, v_0)$ и выходов $(w_{n-1}, \dots, w_0)$. Сеть S с входами $v_{n-1}, \dots, v_0$ и выходами $w_{2n-2}, \dots, w_0$ назовём *n-сдвиговой*, если для любого j, $0 \leqslant j < n$, сеть S является информационной для входов $(v_{n-1}, \dots, v_0)$ и выходов $(w_{n-1+j}, \dots, w_j)$. Наименьшую сложность n-сдвиговой сети обозначим через L_n. Через $L(C)$ будем обозначать сложность СФЭ C, а через $L(F)$ — сложность оператора F в классе СФЭ из двухвходовых элементов.

Теорема. *При любом n*

$$L_n \leqslant L(\mathrm{SAL}_n). \tag{2}$$

Если $n \to \infty$, $m < n^2/4$, то

$$L(\mathrm{SAL}_m) = \mathcal{O}(n \cdot L_n). \tag{3}$$

Следствие. *При $n \to \infty$*

$$L(\mathrm{SAL}_n) = \mathcal{O}(n) \iff L_n = \mathcal{O}(n).$$

Импликация слева направо следует из (2), справа налево — из (3).

Доказательство теоремы. Неравенство (2) очевидно: n-сдвиговую сеть можно получить из СФЭ, реализующей оператор SAL_n, удалением входов, соответствующих управляющим переменным, и всех вершин, недостижимых по ориентированным путям ни от одного из оставшихся входов. Докажем соотношение (3). Сначала докажем равенство (3) для $n = 2^k$ $(k \in \mathbb{N})$ и $m = n^2 - n$.

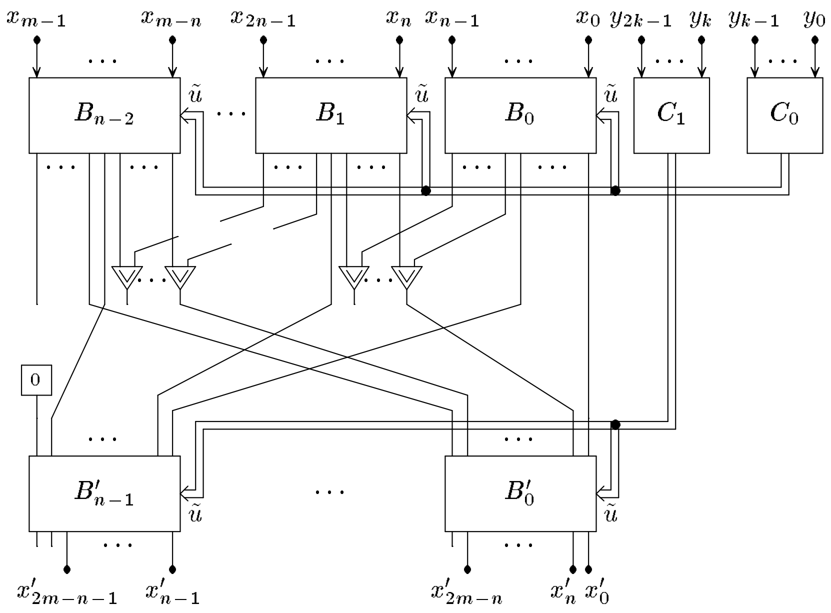
Пусть S — n-сдвиговая сеть наименьшей сложности, равной L_n. Рассмотрим какую-нибудь СФЭ A, реализующую универсальную функцию

$$U_2(z, t,\ u_{1,1}, \dots, u_{0,0}) = \bigvee_{(i,j)\in\{0,1\}^2} u_{i,j} z^i t^j$$

(здесь $x^1 = x$, $x^0 = \bar{x}$). Построим СФЭ B. Для этого в сети S каждую вершину v, отличную от входов, заменим своим экземпляром A_v схемы A, а рёбра, входящие в вершину v, подсоединим к входам z и t схемы A_v. Дополнительно вставим новый экземпляр A'_w схемы A после каждой схемы A_w, соответствующей выходу w сети S, подсоединив к входам z, t схемы A'_w выход схемы A_w. Входами схемы B объявим входы сети S и все входы $u_{i,j}$ схем A_v и A'_w; выходами схемы B — выходы подсхем A'_w. Имеем

$$L(B) = (L_n + 2n - 1) \cdot L(A) = \mathcal{O}(L_n + n). \tag{4}$$

Обозначим через $\tilde{u}$ набор, состоящий из тех входов схемы B, которые являются входами $u_{i,j}$ подсхем A_v и A'_w. Заметим, что при подаче на входы $\tilde{u}$ различных наборов констант схема B будет моделировать всевозможные схемы, каркасом которых является S. Более того, любая схема C', каркас которой может быть получен из S удалением некоторых выходов, моделируется схемой B в том смысле, что на отсутствующие в C' выходы подаются нули; в этом смысле моделируются схемы для тождественных операторов, фигурирующие в определении n-сдвиговой сети.



Подадим на входы из набора $\tilde{u}$ такие функции $(f_u)_{u\in\tilde{u}}$, зависящие от управляющих переменных $y_{k-1},\ldots,y_0$, что полученная схема будет вычислять оператор SAL_n. Обозначим через C схему минимальной сложности, вычисляющую функции $(f_u)_{u\in\tilde{u}}$ (можно взять конструктивно построенную СФЭ сложности, близкой к минимальной). Сложность одной функции от k переменных есть $\mathcal{O}(2^k/k)$ [1, ¡ 4], число входов в наборе $\tilde{u}$ равно $4(L_n+2n-1)$. Следовательно,

$$L(C) = 4(L_n+2n-1)\cdot\mathcal{O}\Big(\frac{2^k}{k}\Big) = \mathcal{O}\Big(\frac{n}{\log_2 n}\cdot(L_n+n)\Big). \tag{5}$$

Наконец, построим схему D, реализующую оператор SAL_{n^2-n} (схема изображена на рисунке). Сдвиг будем осуществлять как композицию двух сдвигов (подобно [3, п. 6.3.2]). Для этого управляющие переменные разобъём на две группы: старшие — $y_{2k-1},\ldots,y_k$ и младшие — $y_{k-1},\ldots,y_0$. Каждую из этих групп подадим на вход своего экземпляра схемы C (C_1 и C_0 соответственно). Младшие переменные определяют величину первого сдвига, сам сдвиг осуществляется $n-1$ экземплярами схемы B: $B_{n-2},\ldots,B_0$. Схемы $B_{n-2},\ldots,B_0$ функционируют синхронно. Поэтому для вычисления функций, управляющих их работой, достаточно одной схемы C_0. После первого сдвига производится учёт переносов; для этого используется $(n-1)(n-2)$ дизъюнкторов.

Далее производится второй сдвиг; его величина равна $y'n$, где y' — величина, определяемая старшими разрядами. Для этого все разряды группируются в зависимости от остатка при делении на n; разряды с остатком i ($0\leqslant i< n$) подаются на входы схемы B'_i (экземпляра схемы B). Схемы $B'_{n-1},\ldots,B'_0$ функционируют синхронно, поэтому для управления ими достаточно одного блока C_1. После выполнения сдвига восстанавливается естественный порядок следования разрядов.

Используя (4) и (5) получаем

$$L(D) = 2L(C) + (2n-1)L(B) + (n-1)(n-2) + O(1) = \\ = \mathcal{O}\Big(\frac{n}{\log_2 n}\cdot(L_n+n)\Big) + \mathcal{O}(n\cdot(L_n+n)) + \mathcal{O}(n^2).$$

Каждый выход n-сдвиговой сети должен быть соединён со всеми входами. Поэтому $L_n \geqslant n-1$. Следовательно,

$$L(D) = \mathcal{O}(n\cdot L_n). \tag{6}$$

Теперь рассмотрим произвольные n, m такие, что $m < n^2/4$. Пусть k таково, что $2^k \leqslant n < 2^{k+1}$. Тогда $2^k \geqslant (n+1)/2$. Следовательно,

$$2^k(2^k-1) \geqslant \frac{(n+1)}{2}\cdot\frac{(n-1)}{2} = \frac{n^2}{4} - \frac{1}{4} \geqslant m. \tag{7}$$

Заметим, что функции $L(\mathrm{SAL}_n)$ и L_n не убывают по n. Действительно, из СФЭ для оператора SAL_n подстановкой нулей вместо лишних переменных и удалением ненужных элементов и выходов можно получить СФЭ для $\mathrm{SAL}_{n'}$, $n' < n$; аналогичное верно и для сетей. Поэтому в силу (6) и (7) имеем

$$L(\mathrm{SAL}_m) \leqslant L(\mathrm{SAL}_{2^k(2^k-1)}) = \mathcal{O}(2^k\cdot L_{2^k}) \leqslant \mathcal{O}(n\cdot L_n).$$

Теорема доказана.

Литература

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Из-во МГУ, 1984.
2. Нигматуллин Р. Г. Сложность булевых функций. М.: Наука, 1991.
3. Сэвидж Дж. Э. Сложность вычислений. М.: Из-во "Факториал", 1998.

Адрес автора:
Каф. дискретной математики,
мех.-мат. факультет МГУ,
Москва, 119992, Россия

Статья поступила
21 сентября 2004 г.