ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2006. Серия 1. Том 13, № 4. 89–92

УДК 519.7

О СЛОЖНОСТИ ЦИКЛИЧЕСКОГО СДВИГА НАБОРА ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ*)

А. В. Чашкин

Показано, что сложность реализации циклического сдвига набора действительных чисел длины 2^n схемами из функциональных элементов, базис которых содержит трёхместную функцию выбора и все двухместные булевы функции, равна $2^n n$.

Определим оператор циклического сдвига и функцию выбора следующим образом. Пусть $\boldsymbol{x} = (x_0, \ldots, x_{2^n-1})$ и $\boldsymbol{y} = (y_0, \ldots, y_{2^n-1})$ — наборы действительных чисел, $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ — булев набор. Положим $|\boldsymbol{\alpha}| = \sum\limits_{i=0}^{n-1} \alpha_i 2^i$. Оператор $F(\boldsymbol{x}, \boldsymbol{\alpha}) = \boldsymbol{y}$ называется *оператором циклического сдвига* набора $\boldsymbol{x}$, если $y_j = x_i$, где $j = i - |\boldsymbol{\alpha}| \pmod{2^n}$ для каждого $j = 0, \ldots, 2^n - 1$. Пусть, далее, $x, y \in \mathbb{R}$, $\alpha \in \{0, 1\}$. Функцией выбора назовём функцию

$$\varphi(x, y, \alpha) = \begin{cases} x, & \text{если } \alpha = 1, \\ y, & \text{если } \alpha = 0. \end{cases}$$

В статье исследуется сложность реализации оператора циклического сдвига набора действительных чисел схемами из функциональных элементов. Базис рассматриваемых схем состоит из всех двухместных булевых функций и функции выбора. Определение схемы из функциональных элементов и другие необходимые определения можно найти в [3]. *Сложностью* $L(S)$ схемы S называется число функциональных элементов этой схемы. Схема S называется *минимальной* схемой оператора F, если S реализует F, и сложность этой схемы не больше сложности любой другой схемы, реализующей F. *Сложностью* $L(F)$ *оператора* F называется сложность минимальной схемы, реализующей F.

Рассматриваемая в работе задача внешне похожа на задачу о сложности логического оператора циклического сдвига, в которой циклический

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–5400.2006.1).

сдвиг выполняется над булевым набором посредством булевых схем в полном базисе. Существенное отличие последней задачи от рассматриваемой заключается в том, что циклический сдвиг набора действительных чисел реализуется схемами, которые по своим свойствам и выразительным возможностям близки к монотонным булевым схемам. Различные результаты о сложности логического оператора циклического сдвига можно найти в [4].

Основным результатом настоящей работы является следующее утверждение.

Теорема. *Если* $\boldsymbol{x} \in \mathbb{R}^{2^n}$ *и* $\boldsymbol{\alpha} \in \{0,1\}^n$, *то* $L(F(\boldsymbol{x}, \boldsymbol{\alpha})) = n2^n$.

Схемы, реализующие циклический сдвиг наборов длины 2^n, неоднократно рассматривались различными авторами. По-видимому, одним из первых был О. Б. Лупанов. Им в [2] была приведена конструкция схемы, которая реализует циклический сдвиг булевых векторов в двухместном булевом базисе. Конструкция из [2] (аналогичная конструкция описана в [4]) может быть легко адаптирована для построения схемы, реализующей циклический сдвиг наборов действительных чисел длины 2^n так, что построенная схема будет состоять из $n2^n$ элементов, каждый из которых реализует функцию выбора, т. е. булевы элементы не используются, а управление элементами выбора осуществляется непосредственно разрядами булева набора $\boldsymbol{\alpha}$. Поэтому далее ограничимся получением только нижней оценки сложности. Для этого потребуется вспомогательное утверждение о сумме высот листьев в корневом бинарном дереве. *Высотой* $h(v)$ листа v в корневом дереве G называется число внутренних вершин дерева, лежащих между листом и корнем. Различные варианты приводимого ниже утверждения можно найти в литературе, посвящённой нижним оценкам сложности (см., например, [1]).

Лемма. *Для любого бинарного дерева* G *с* n *листьями*

$$\sum_{v \in G} h(v) \geqslant n \log_2 n.$$

Доказательство проведём индукцией по числу листьев. В основание индукции положим очевидный случай $n = 2$. Допустим, что для любого $n \leqslant m-1$ лемма справедлива. В дереве G с m листьями рассмотрим два поддерева G_1 и G_2, корнями которых являются вершины, смежные с корнем. По предположению индукции для этих поддеревьев справедливы неравенства $\sum\limits_{v \in G_1} h_1(v) \geqslant m_1 \log_2 m_1$, $\sum\limits_{v \in G_2} h_2(v) \geqslant m_2 \log_2 m_2$, где $m_1 + m_2 = m$, а h_1 и h_2 — высоты листьев в поддеревьях G_1 и G_2. В этом

случае для дерева G справедлива следующая оценка:

$$\begin{aligned}\sum_{v\in G} h(v) &= \sum_{v\in G_1} h(v) + \sum_{v\in G_2} h(v) = \sum_{v\in G_1} (h_1(v)+1) + \sum_{v\in G_2} (h_2(v)+1)\\ &= m_1\log_2 m_1 + m_1 + m_2\log_2 m_2 + m_2\\ &= \frac{1}{2}(2m_1\log_2 2m_1 + 2m_2\log_2 2m_2)\\ &\geqslant \frac{2m_1+2m_2}{2}\log_2\frac{2m_1+2m_2}{2} = m\log_2 m.\end{aligned}$$

Лемма доказана.

Доказательство теоремы. Пусть S — схема, реализующая оператор циклического сдвига набора длины 2^n. Входы схемы, на которые подаются элементы сдвигаемого набора, назовём основными, а входы, на которые подаются элементы булевого набора $\boldsymbol{\alpha}$, назовём управляющими. Введём функцию $\chi(i,j,v,\boldsymbol{\alpha})$. Эта функция равна единице, если при поданном на управляющие входы схемы S наборе $\boldsymbol{\alpha}$ поданное на её i-й основной вход число проходит через элемент v и попадает на j-й выход. Во всех остальных случаях эта функция равна нулю. При фиксированном наборе $\boldsymbol{\alpha}$, входе i и выходе j таких, что $j = i - |\boldsymbol{\alpha}| \pmod{2^n}$, функцию χ можно рассматривать как индикатор цепи, по которой в схеме S поданное на i-й вход число проходит до j-го выхода. Зафиксируем j, объединим все цепи с данным j и в получившемся объединении выделим остовное дерево с корнем в j-м выходе. Применив к этому дереву лемму, получим, что при каждом j имеет место неравенство

$$\sum_{i=1}^{2^n}\sum_{\boldsymbol{\alpha}\in\{0,1\}^n}\sum_{v\in S}\chi(i,j,v,\boldsymbol{\alpha}) \geqslant 2^n n,$$

и, таким образом,

$$\sum_{j=1}^{2^n}\sum_{i=1}^{2^n}\sum_{\boldsymbol{\alpha}\in\{0,1\}^n}\sum_{v\in S}\chi(i,j,v,\boldsymbol{\alpha}) \geqslant 2^n 2^n n. \tag{1}$$

Из определения функции χ следует, что при фиксированном элементе v и фиксированном наборе $\boldsymbol{\alpha}$ существует не более одного входа i и не более одного выхода j таких, что $\chi(i,j,v,\boldsymbol{\alpha}) = 1$. Поэтому для любых v и $\boldsymbol{\alpha}$

$$\sum_{j=1}^{2^n}\sum_{i=1}^{2^n}\chi(i,j,v,\boldsymbol{\alpha}) \leqslant 1.$$

Следовательно, для любого элемента v

$$\sum_{j=1}^{2^n}\sum_{i=1}^{2^n}\sum_{\alpha\in\{0,1\}^n}\chi(i,j,v,\boldsymbol{\alpha})\leqslant 2^n. \tag{2}$$

Теперь дополним неравенство (1) оценкой сверху. Для этого изменим порядок суммирования, сделав суммирование по элементам схемы внешним. Внутренние суммы по i,j и $\boldsymbol{\alpha}$ оценим при помощи неравенства (2). В результате получаем

$$2^n 2^n n\leqslant\sum_{v\in S}\Bigl(\sum_{j=1}^{2^n}\sum_{i=1}^{2^n}\sum_{\boldsymbol{\alpha}\in\{0,1\}^n}\chi(i,j,v,\boldsymbol{\alpha})\Bigr)\leqslant\sum_{v\in S}2^n=L(S)2^n. \tag{3}$$

Из этого неравенства следует, что схема S состоит не менее чем из $2^n n$ элементов. Теорема доказана.

ЛИТЕРАТУРА

1. **Григорьев Д. Ю.** О нелинейной нижней оценке сложности схем для систем дизъюнкций в монотонном булевом базисе // Записки научн. семинаров ЛОМИ. 1977. Т. 68. С. 19–25.
2. **Лупанов О. Б.** Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып 14. М.: Наука, 1965. С. 31–110.
3. **Нигматуллин Р. Г.** Сложность булевых функций. М.: Наука, 1991.
4. **Savage J. E.** Models of computation: exploring the power of computing. Reading, MA: Addison Wesley Longman, 1998.

Адрес автора:

МГУ, мех.-мат. факультет,
Ленинские горы,
119992 Москва, Россия.
E-mail: chash@online.ru

Статья поступила
7 марта 2006 г.