Math-Net.Ru

Общероссийский математический портал

К. А. Зыков, О сравнении сложности двух способов реализации некоторых линейных булевых преобразований, *Дискрет. матем.*, 1996, том 8, выпуск 2, 151–159

DOI: <https://doi.org/10.4213/dm527>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.64.247

26 апреля 2023 г., 16:42:03

О сравнении сложности двух способов реализации некоторых линейных булевых преобразований

© 1996 г. К. А. Зыков

В работе изучается сложность реализации систем линейных булевых функций схемами в базисе из элементов двоичного сложения. Рассматриваются системы функций, задаваемые матрицами без прямоугольников. Такие матрицы часто возникают в различных областях математики.

1. Постановка задачи

Булева матрица A с элементами a_{ij} , $i = 1, \dots, n$, $j = 1, \dots, m$, задает систему m булевых функций

$$f_j = \sum_{i=1}^n a_{ij} x_i,$$

где сложение осуществляется по модулю 2. Система функций, задаваемая матрицей A , реализуется схемами в базисе из элементов двоичного сложения с двумя входами и произвольным количеством выходов (определение схем из функциональных элементов см. в [1]).

Сложностью схемы считается количество входящих в нее элементов. Сложность схемы S будем обозначать через $L(S)$.

Сложностью матрицы A будем называть величину $\min_S L(S)$, где минимум берется по всем схемам S , реализующим эту систему функций. Сложность матрицы A будем обозначать через $L(A)$.

Очевидно, что систему функций, задаваемую матрицей A , можно реализовать, строя для каждой функции системы отдельную схему. Такую реализацию будем называть тривиальной, а ее сложность обозначать через $L_T(A)$. Легко видеть, что если в матрице A нет нулевых столбцов, то

$$L_T(A) = E(A) - m,$$

где $E(A)$ — число входящих в матрицу A единиц, а m — число столбцов этой матрицы.

Тривиальная реализация не всегда является наилучшей. Очевидно, что если в матрице D существуют хотя бы 2 столбца, содержащие 1 хотя бы в двух одинаковых строках, то сумма этих переменных может быть реализована одновременно для двух функций рассматриваемой системы, и, следовательно, в этом случае $L(D) < L_T(D)$.

Определение 1. Булеву матрицу A с элементами a_{ij} , $i = 1, \dots, n$, $j = 1, \dots, m$, называют матрицей без прямоугольников, если для любых k, l, g, h таких, что $1 \leq k, l \leq n$, $1 \leq g, h \leq m$, $k \neq l$, $g \neq h$, элементы a_{kg} , a_{kh} , a_{lg} , a_{lh} не все равны 1.

Э. И. Нечипорук в работе [2] доказал, что для схем из функциональных элементов в базисе $\{\vee, \&\}$ при реализации системы функций

$$g_j = \bigvee_{i=1}^n a_{ij} x_i,$$

задаваемой матрицей без прямоугольников, невозможна реализация со сложностью меньшей, чем сложность тривиальной реализации. Там же был установлен аналогичный результат относительно реализации матриц без прямоугольников в классе вентильных схем. Следующий пример показывает, что для рассматриваемых нами схем из функциональных элементов в базисе $\{\oplus\}$ аналогичное утверждение неверно. Схема S_{B_1} (см. рис. 1) реализует матрицу без прямоугольников B_1 (см. рис. 2). При этом $L(S_{B_1}) = 6$, в то время, как $L_T(B_1) = 7$.

Следующие два утверждения показывают, что матрица B_1 является в некотором смысле простейшей матрицей без прямоугольников, дающей экономию сложности по сравнению с тривиальной реализацией.

Предложение 1. Пусть B — матрица без прямоугольников и $L(B) < L_T(B)$. Тогда $L_T(B) \geq 7$.

Предложение 2. Пусть B — матрица без прямоугольников и $L(B) < L_T(B)$. Тогда B содержит не менее пяти строк, т.е. система функций, задаваемая матрицей B , существенно зависит не менее, чем от пяти переменных.

Доказательства предложений 1 и 2 могут быть проведены, например, перебором и здесь не приводятся.

Возникает вопрос, насколько велико может быть отношение $L_T(A)/L(A)$ для матриц без прямоугольников. В работе построено двухпараметрическое семейство матриц без прямоугольников F_p^n , $n = 1, 2, \dots$, $p = 2, 3, 5, \dots$ (простое число), для которого $L_T(F_p^n)/L(F_p^n) \gtrsim 2$, когда $p, n \rightarrow \infty$, и $p = o(n)$.

2. Построение семейства матриц F_p^n

2.1. Разбиение переменных на группы

Пусть p — простое число. Из p^2 переменных $x_1, \dots, x_{p^2}$ составим $(p+1)$ семейство так, чтобы выполнялись следующие условия: в каждом семействе содержится p групп по p переменных в каждой; все переменные в семействе различны; любые две группы содержат не более одной общей переменной. Докажем, что это возможно.

Рис. 1.

x_1	1	0	0	1	0
x_2	1	1	0	0	1
x_3	0	0	0	1	1
x_4	0	1	1	1	0
x_5	0	0	1	0	1
	f_1	f_2	f_3	f_4	f_5

Рис. 2.

$$\left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{array} \right)$$

Рис. 3.

Семейство с номером 0 состоит из следующих групп: $(x_1, \dots, x_p)$, $(x_{p+1}, \dots, x_{2p}), \dots, (x_{p^2-p+1}, \dots, x_{p^2})$. В семействе с номером k , $k = 1, \dots, p$, группа с номером i , $i = 1, \dots, p$, состоит из переменных $x_{\alpha p + 1 + \text{res}_p(k\alpha - \alpha - 1 + i)}$, где $\alpha = 0, \dots, p-1$, а через $\text{res}_p(a)$ обозначается неотрицательный остаток от деления числа a на число p .

Булева матрица N размера $p^2 \times p^2$, рассмотренная в [2], совпадает с матрицей, полученной следующим образом. Пусть строкам матрицы соответствуют переменные, а столбцам — группы переменных из семейств с номерами $1, \dots, p$. При этом столбцам $1, \dots, p$ соответствуют группы $1, \dots, p$ из первого семейства, столбцам $p+1, \dots, 2p$ — группы из второго семейства и т. д. Элемент n_{ij} матрицы N равен 1 тогда и только тогда, когда x_i входит в соответствующую j -му столбцу группу переменных. В [2] показано, что данная матрица является матрицей без прямоугольников. Пример матрицы N для случая $p = 3$ показан на рис. 3.

Рассмотрим теперь матрицу N' , полученную из матрицы N , добавлением к ней слева p столбцов, соответствующих группам из нулевого семейства. Очевидно, матрица N' также будет матрицей без прямоугольников. Таким образом показано, что любые две группы имеют не более одной общей переменной.

2.2. Построение элементарной схемы

Отметим в матрице N' по одному (произвольному) столбцу для каждого из семейств переменных за исключением нулевого. Матрицу N' без отмеченных столбцов обозначим N'' . Добавим к матрице N'' еще $p(p-1)$ строк, соответствующих новым переменным $x_{p^2+1}, \dots, x_{2p^2-p}$, следующим образом. К первым p столбцам добавляется матрица, состоящая из одних нулей, а к остальным — единичная матрица. Полученную матрицу обозначим N^* (см. рис. 4).

Систему функций, задаваемую матрицей N^* , обозначим через $g_1, \dots, g_{p^2}$, а схему, реализующую ее тривиальным образом, через V_p^1 . Легко видеть, что

$$L(V_p^1) = p^2(p-1) + p(p-1) = p(p^2-1).$$

Функции $g_1, \dots, g_{p^2}$, вычисляемые схемой V_p^1 , подадим на входы схемы V_p^2 , имеющей следующий вид. Тривиальным образом вычисляются суммы по модулю

p		$p^2 - p$		
				$\left. \begin{array}{c} \\ \end{array} \right\} p^2 - p$
		1	0	$\left. \begin{array}{c} \\ \end{array} \right\} p^2 - p$
0		$\ddots$		
		0	1	

Рис. 4.

два

$$s_0 = \sum_{i=1}^p g_i,$$

$$s_j = \sum_{i=1}^{p-1} g_{p+(j-1)(p-1)+i}, \quad j = 1, \dots, p.$$

С использованием этих функций вычисляются функции

$$v_j = s_0 \oplus s_j, \quad j = 1, \dots, p.$$

Таким образом соединенные схемы V_p^1 и V_p^2 образуют схему H_p . Пример схемы H_p для $p = 3$ показан на рис. 5.

Легко видеть, что для функций v_j , $j = 1, \dots, p$, реализуемых схемой H_p , выполняются равенства

$$v_j = s_0 \oplus s_j = h_{j-1} \oplus \sum_{i=1}^{p-1} x_{p^2+(p-1)(j-1)+i},$$

где функции h_{j-1} задаются отмеченными столбцами матрицы N' . Учитывая то, что матрица N' является матрицей без прямоугольников, можно утверждать, что схема H_p обладает следующими двумя свойствами. Во-первых, системе функций v_j , $j = 1, \dots, p$, реализуемой схемой H_p , соответствует матрица без прямоугольников. Будем обозначать ее F_p . Во-вторых, произвольная функция v_j имеет не более одной общей существенной переменной с произвольной функцией g_i , $i = 1, \dots, p^2$, реализуемой схемой V_p^1 , подсхемой схемы H_p .

Отметим, что

$$L(V_p^2) = (p-1) + (p-1)p = p^2 - 1,$$

$$L_T(F_p) = p(2p-1-1) = 2p(p-1).$$

2.3. Общее использование групп

Функцию, реализуемую элементом α схемы S , будем обозначать $\alpha(\tilde{x})$.

Рис. 5.

Лемма 1. Пусть схема G^0 реализует матрицу без прямоугольников D_0 , а элементы $\alpha_1, \dots, \alpha_d$ этой схемы реализуют линейные функции $\alpha_1(\tilde{x}), \dots, \alpha_d(\tilde{x})$ соответственно. Пусть, кроме того, любая из функций $\alpha_i(\tilde{x})$, $i = 1, \dots, d$, имеет не более одной общей существенной переменной с функцией, реализуемой любым выходом схемы G^0 . Тогда существует последовательность схем G_n , реализующих матрицы без прямоугольников D_n , такая, что при $n \rightarrow \infty$

$$\frac{L_T(D_n)}{L(G_n)} \sim \frac{L_T(D_0)}{L(G^0) - d}.$$

Доказательство. Построим схему G_n следующим образом. Пусть число переменных, подаваемых на входы схемы G^0 равно γ . Построим n схем G^0 , причем на все входы всех схем G^0 будем подавать различные переменные. Набор переменных, подаваемый на входы схемы с номером β_0 , $\beta_0 = 1, \dots, n$, обозначим $x_1^{\beta_0}, \dots, x_\gamma^{\beta_0}$. Иначе говоря, у переменной $x_j^{\beta_0}$, $j = 1, \dots, \gamma$, $\beta_0 = 1, \dots, n$, нижний индекс определяет место переменной в схеме G^0 , а верхний — номер схемы G^0 . отождествим во всех этих схемах переменные с одинаковыми нижними индексами, если функция $\alpha_1(\tilde{x})$ зависит от переменной с этим индексом. Теперь элементы α_1 во всех схемах G^0 реализуют одинаковые функции. Поэтому мы можем удалить элементы α_1 из всех схем G^0 кроме первой, а элемент из первой схемы использовать сразу для всех. Полученную таким образом схему обозначим G^1 . Верхний индекс у отождествленных переменных считаем равным 1.

Построим n схем G^1 с различными переменными. При этом переменные получают второй верхний индекс $\beta_1 = 1, \dots, n$, соответствующий номеру схемы G^1 . отождествим переменные с одинаковыми β_0 и нижними индексами, если в исходной схеме G^0 функция $\alpha_2(\tilde{x})$ зависит от переменной с этим нижним индексом. Элементы α_2 удаляются из всех схем G^1 кроме одной (т.е. удаляется $n(n-1)$ элементов). Каждый из n сохраненных элементов α_2 используется вместо $(n-1)$ -го удаленного элемента. Полученную схему обозначим через G^2 . Далее аналогично получим схемы G^i , $i = 3, \dots, d$. Положим $G_n = G^d$.

Допустим, что схема G^i реализует матрицу без прямоугольников, элементы $\alpha_1, \dots, \alpha_d$ во всех схемах G^0 реализуют суммы переменных, имеющие не более одной общей существенной переменной с функцией, реализуемой любым выходом схемы G^i . Докажем, что этими же свойствами будет обладать схема G^{i+1} , $i = 0, \dots, d-1$.

Покажем сначала, что функция, реализуемая произвольным выходом схемы G^{i+1} , имеет не более одной общей существенной переменной с функцией, реализуемой произвольным элементом α_k , $k = 1, \dots, d$. Действительно, внутри каждой схемы G^i утверждение выполняется по предположению индукции (при построении G^{i+1} переменные внутри G^i , т.е. имеющие одинаковые индексы β_i , не отождествляются). С другой стороны, в различных G^i могут совпадать лишь переменные с одинаковыми нижними индексами, а таких для функций, реализуемых произвольным выходом схемы и произвольным элементом α_k , не более одной. Утверждение доказано.

Покажем теперь, что схема G^{i+1} реализует матрицу без прямоугольников. Действительно, внутри одной схемы G^i функции, реализуемые различными выходами, имеют не более одной общей существенной переменной по предположению индукции. С другой стороны, в различных G^i совпадают лишь переменные

с нижними индексами, такими, что функция, реализуемая элементом α_{i+1} в исходной схеме G^0 , зависит от переменной с этим индексом. А таких переменных в каждом выходе схемы не более одной. Утверждение доказано.

Таким образом, схема G_n реализует некоторую матрицу без прямоугольников, обозначаемую далее D_n , и при этом

$$\begin{aligned} L_T(D_n) &= n^d L_T(D_0), \\ L(G_n) &= n^d (L(G^0) - d) + n^{d-1} d \end{aligned}$$

(число элементов α_i , $i = 1, \dots, d$, не увеличивалось при переходе от схемы G^{i-1} к схеме G^i). Следовательно,

$$\begin{aligned} \frac{L_T(D_n)}{L(G_n)} &= \frac{n^d L_T(D_0)}{n^d L(G^0) - n^d d + n^{d-1} d} = \frac{L_T(D_0)}{L(G^0) - d + d/n} \\ &\sim \frac{L_T(D_0)}{L(G^0) - d} \end{aligned}$$

при $n \rightarrow \infty$. Лемма 1 доказана.

2.4. Построение семейства матриц F_p^n

Заметим, что схема H_p и элементы, реализующие выходы подсхемы V_p^1 , удовлетворяют условию леммы 1. Построим схему H_p^n по способу леммы 1. Из рассмотрения схемы H_p видно, что ориентированный граф, соответствующий ее подсхеме V_p^1 (определение см. в [1]), состоит из нескольких бинарных деревьев. Поэтому при построении схемы H_p^n вместе с элементом, реализующим выход схемы V_p^1 , можно отбросить всю подсхему (бинарное дерево), реализующую этот выход. Следовательно,

$$\begin{aligned} L(H_p^n) &= L(V_p^2) n^{p^2} + L(V_p^1) n^{p^2-1} \\ &= (p^2 - 1) n^{p^2} + (p - 1) p (p + 1) n^{p^2-1}. \end{aligned}$$

Матрицу, реализуемую схемой H_p^n , будем обозначать F_p^n ;

$$L_T(F_p^n) = n^{p^2} L_T(F_p) = n^{p^2} 2p(p - 1).$$

Пусть $p \rightarrow \infty$ и $p/n \rightarrow 0$. Тогда

$$\begin{aligned} \frac{L_T(F_p^n)}{L(H_p^n)} &= \frac{n^{p^2} 2p(p - 1)}{(p^2 - 1) n^{p^2} + (p - 1) p (p + 1) n^{p^2-1}} = \frac{2p^2 n - 2pn}{p^2 n - n + p^3 - p} \\ &\sim \frac{2p^2 n}{p^2 n + p^3} \sim 2. \end{aligned}$$

Таким образом, при $p \rightarrow \infty$, $p/n \rightarrow 0$, для последовательности матриц F_p^n справедливо соотношение

$$\frac{L_T(F_p^n)}{L(F_p^n)} \gtrsim 2.$$

В заключение автор пользуется возможностью выразить признательность О. Б. Лупанову за постановку задачи и внимание к работе, а также О. М. Касим-Заде за полезные замечания.

Список литературы

1. Лупанов О. Б. *Асимптотические оценки сложности управляющих систем*. Изд-во МГУ, Москва, 1984.
2. Нечипорук Э. И. Об одной булевой матрице. *Пробл. киберн.* (1969) **21**, 237–240.

Статья поступила 25.02.94.