

Иркутский государственный университет

Приближенный алгоритм вычисления сложности обратимых реализаций полиномов булевых функций

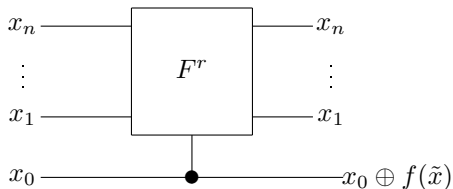
Винокуров Сергей Федорович,
Францева Анастасия Сергеевна

Монголия – 2019

Обратимое представление булевой функции

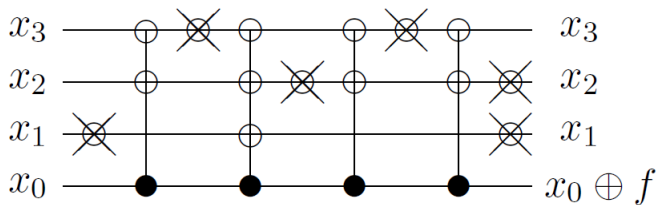
$$F(x_0, x_1, x_2) : (x_0, x_1, x_2) \rightarrow (x_0 \oplus x_1 \cdot x_2, x_1, x_2)$$

x_0	x_1	x_2	$x_0 \oplus x_1 \cdot x_2$	x_1	x_2
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

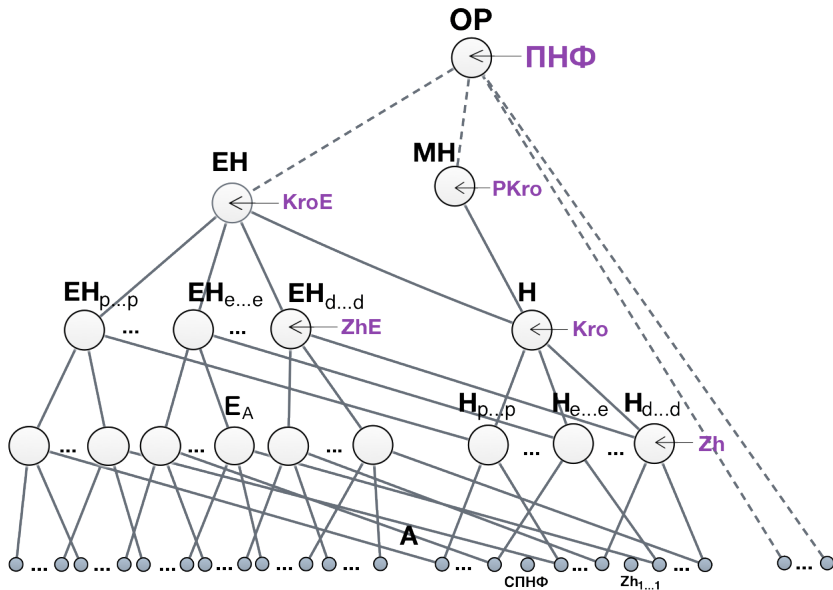


Обратимая схема из элементов Тоффоли

$$f(x_1, x_2, x_3) = x_2x_3 \oplus \bar{x}_1x_2\bar{x}_3 \oplus \bar{x}_2\bar{x}_3 \oplus \bar{x}_2x_3$$



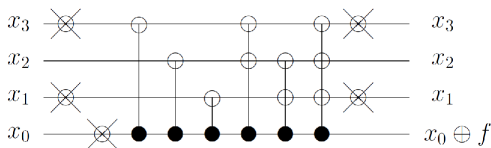
Классы полиномов



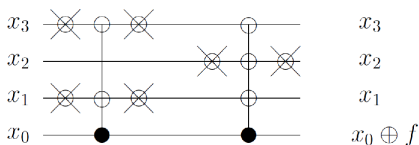
Пример обратимой реализации *ZhE*-полиномов булевых функций

$$f(x_1, x_2, x_3) = (10100100)$$

$$f(x_1, x_2, x_3) = 1 \oplus \bar{x}_3 \oplus x_2 \oplus \bar{x}_1 \oplus x_2\bar{x}_3 \oplus \bar{x}_1x_2 \oplus \bar{x}_1x_2\bar{x}_3$$



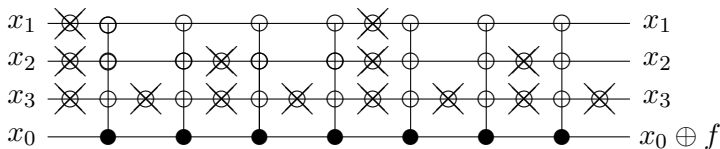
$$f(x_1, x_2, x_3) = \bar{x}_1\bar{x}_3 \oplus x_1\bar{x}_2x_3;$$



Пример обратимой реализации полинома булевой функции

$$f(x_1, x_2, x_3) =$$

$$= \bar{x}_1\bar{x}_2\bar{x}_3 \oplus \bar{x}_1\bar{x}_2x_3 \oplus \bar{x}_1x_2\bar{x}_3 \oplus \bar{x}_1x_2x_3 \oplus x_1\bar{x}_2\bar{x}_3 \oplus x_1\bar{x}_2x_3 \oplus x_1x_2\bar{x}_3$$



7+14

Точный алгоритм вычисления сложности обратимой схемы, реализующей полином булевой функции

Для каждого полинома булевой функции:

- ▶ перестановка s слагаемых;
- ▶ перестановка переменных $x_1, \dots, x_n$

$n!s!$

$n = 3, n = 4$

Приближенный алгоритм вычисления сложности обратимой схемы, реализующей полином

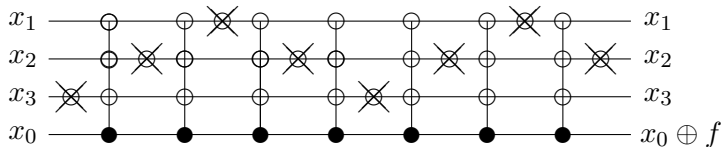
Рефлексивный порядок при $n = 3$:

000	011
001	001
010	000
011	010
100	110
101	100
110	101
111	111

Приближенный алгоритм вычисления сложности обратимой схемы, реализующей полином

$$f(x_1, x_2, x_3) =$$

$$= \bar{x}_1 x_2 x_3 \oplus \bar{x}_1 \bar{x}_2 x_3 \oplus \bar{x}_1 \bar{x}_2 \bar{x}_3 \oplus \bar{x}_1 x_2 \bar{x}_3 \oplus x_1 x_2 \bar{x}_3 \oplus x_1 \bar{x}_2 \bar{x}_3 \oplus x_1 \bar{x}_2 \bar{x}_3$$



7+8

Приближенный алгоритм вычисления сложности обратимой схемы, реализующей полином

Для каждого полинома:

- ▶ Упорядочить слагаемые по рефлексивному порядку $(0 - \bar{x}, 1 - x, \langle - \rangle)$.
- ▶ Вставить отсутствующие переменные с отрицанием или без (заменить $\langle - \rangle$ на x или $\bar{x}$).
- ▶ Подбор ближайшего следующего слагаемого, отличающегося в наименьшем числе отрицаний.

Пример

$$f(x_1, x_2, x_3) = (01110111)$$

$$x_2\bar{x}_3 \oplus \bar{x}_2x_3 \oplus \bar{x}_1x_2x_3 \oplus \bar{x}_1\bar{x}_2\bar{x}_3$$

$x_2\bar{x}_3$	$\bar{x}_1x_2x_3$	$\bar{x}_1x_2x_3$	$\bar{x}_1x_2x_3$	1
$\bar{x}_2x_3$	$\bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{x}_1x_2\bar{x}_3$	1
$\bar{x}_1x_2x_3$	$x_2\bar{x}_3$	$\bar{x}_1x_2\bar{x}_3$	$\bar{x}_1\bar{x}_2\bar{x}_3$	1
$\bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{x}_2x_3$	$\bar{x}_1\bar{x}_2x_3$	$\bar{x}_1\bar{x}_2x_3$	1+2

Результаты

Расширенные кронекеровы формы

$n = 3$	$n = 4$	$n = 5$
6	11	21

Banchmarks-функции	Значение сложности		
	$n = 6$	$n = 7$	$n = 8$
«сложные» в классах H_b, H	34	57	102
«сложные» в классах EH_b	31	56	99
«сложные» в классе EH	32	63	122