

УДК 519.673

Приближенный алгоритм нахождения сложности обратимых реализаций расширенных кронекеровых форм булевых функций

Винокуров Сергей Федорович, Францева Анастасия Сергеевна

Иркутский государственный университет, e-mail: servin38@gmail.com, a.s.frantseva@gmail.com

В работе продолжается исследование задачи обратимых реализаций полиномиальных нормальных представлений булевых функций и приводится реализация алгоритма нахождения сложности обратимых реализаций расширенных кронекеровых форм булевых функций. Данные исследования представляют также теоретический интерес и могут быть использованы для нахождения неизвестной пока оценки значения функции Шеннона сложности представлений булевых функций в соответствующем классе обратимых реализаций.

Ключевые слова: функция Тоффоли, обратимые схемы, булевы функции, кронекерова форма.

Обратимым представлением булевой функции $f(x_1, \dots, x_n)$ называется обратимая функция следующего вида:

$$F(x_0, x_1, \dots, x_n) = (f_0(x_1, \dots, x_n), f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)),$$

где

$$f_0(x_1, \dots, x_n) = x_0 \oplus f(x_1, \dots, x_n),$$

$$f_i(x_1, \dots, x_n) = x_i \text{ по всем } 1 \leq i \leq n;$$

т.е. функция $F^r(x_0, x_1, \dots, x_n)$ осуществляет следующее отображение:

$$(x_0, x_1, \dots, x_n) \mapsto (x_0 \oplus f(x_1, \dots, x_n), x_1, \dots, x_n).$$

В работе рассматриваются следующие обратимые функции (функции Тоффоли):

$$\begin{aligned} T_0^{n+1}(x_i) &: (x_0, x_1, \dots, x_i, \dots, x_n) \rightarrow (x_0, x_1, \dots, \bar{x}_i, \dots, x_n); \\ T_k^{n+1}(x_{i_1}, \dots, x_{i_k}, x_0) &: (x_0, x_1, \dots, x_n) \rightarrow (x_0 \oplus x_{i_1} \cdot \dots \cdot x_{i_k}, x_1, \dots, x_n), \\ &k \leq n, \{i_1, \dots, i_k\} \subset \{1, \dots, n\}. \end{aligned}$$

Любая обратимая функция $F(x_0, x_1, \dots, x_n)$ представляется в виде суперпозиции функций Тоффоли [5].

Более подробно остальные определения, а также описание построения обратимых схем, реализующих обратимые функции указанного вида, можно прочесть, например в [3]. Вид обратной схемы (выбранная последовательность элементов функций Тоффоли) зависит от вида полиномиального представления булевой функции. В [3] рассматриваются обратимые реализации

расширенных поляризованных полиномов Жегалкина (или ZhE -полиномов) булевой функции.

В данной работе рассматриваются расширенные кронекеровы формы булевых функций (класс EH), построение которых подробно описано с использованием операторного подхода и введением класса двупорожденных операторных пучков в [2; 4]. Класс EH включает в себя известный класс H кронекеровых форм.

Схематически обратимая схема, реализующая полином булевой функции, выглядит так, как показано на рисунке 1. Внутри блока F располагаются элементы функций Тоффли T_0 и T_k . Элементы T_0 реализуют отрицания над переменными, элементы T_k — слагаемые полинома. Одним из условий построения обратимой схемы является условие совпадения значений на выходах y_i в схеме со значениями на входах x_i . Тогда с учетом вида EH -полинома булевой функции, для его обратимой реализации требуется, в отличие от обратимой реализации ZhE -полиномов, реализовывать отрицания каждого слагаемого EH -полинома.

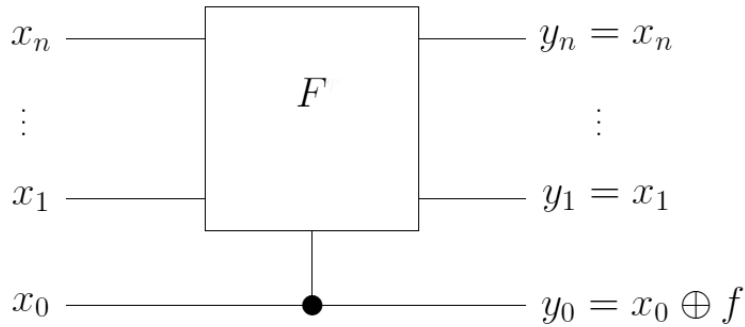


Рис. 1: Обратимая схема, реализующая булеву функцию $f(x_1, \dots, x_n)$

Пусть S — обратимая схема, реализующая EH -полином P функции f . Схема S построена в соответствии с вышеприведенными рассуждениями. В ходе выполнения алгоритма в схеме S переставляются те ее части, что реализуют слагаемые EH -полинома. $l(S)$ — количество элементов функций Тоффли T_0 и T_k , составляющих схему. Тогда под сложностью обратимой реализации EH -полиномов булевой функции будем понимать $\min_P l(S)$ по всем полиномам P класса EH , представляющим булеву функцию.

В соответствии с определением класса EH расширенных кронекеровых форм EH -полином P предполагает две формы: кронекерову и расширенную.

На шаге 1 и 2 алгоритма используется модифицированная версия алгоритма точной минимизации булевых функций в классе кронекеровых форм [1].

Алгоритм нахождения сложности обратимых реализаций EH -полиномов булевых функций

Входные данные: вектор булевой функции f

Выходные данные: минимальное значение $Cost$ сложности обратимых реализаций всех EH -полиномов функции f .

По всем базисам класса кронекеровых форм H :

1. Строится кронекерова форма Fh функции f и вычисляется количество слагаемых t .
2. Строится расширенная кронекерова форма Fe функции f и вычисляется количество слагаемых s .
3. Упорядочиваются в рефлексивном порядке слагаемые формы Fh .
4. В первом слагаемом вставляется отсутствующая (-ие) переменная (-ые) с отрицанием или без в соответствии с ближайшим следующим слагаемым, в котором эта переменная присутствует; в следующем слагаемом (и по всем остальным) вставляются переменные в соответствии с предыдущим слагаемым.
5. Вычисляется количество $n1$ элементов T_0 (отрицаний), необходимое для обратимой реализации каждого слагаемого полинома Fh .
6. Для каждого слагаемого, по порядку, подбирается из оставшихся слагаемых ближайшее следующее слагаемое, отличающееся в наименьшем количестве отрицаний, необходимых для его реализации.
7. Повторяется шаг 5 и вычисляется $n2$.
8. Из значений $n1$ и $n2$ выбирается меньшее n .
9. Выполняются шаги 3 - 8 для формы Fe и вычисляется количество отрицаний m .
10. Если $t + n < s + m$, и $t + n < Cost$, то $Cost = t + n$. Иначе если $s + m < Cost$, то $Cost = s + m$.

Время работы текущей реализации алгоритма для одной функции при $n = 8$ равно примерно 5 секунд.

Результаты алгоритма представлены в таблицах 1–4.

В таблице 4 приведены значения сложности обратимых реализаций EH -полиномов булевых функций, которые являются сложными в классах кронекеровых форм, расширенных кронекеровых форм.

Текущая реализация алгоритма тестировалась на булевых функциях при $n \leq 8$. Алгоритм предполагается использовать при n не более 16.

Таблица 1: Значения сложности функций при $n = 3$

Сложность	Количество функций
1	8
2	28
3	56
4	70
5	68
6	25

Таблица 2: Значения сложности функций при $n = 4$

Сложность	Количество функций
1	16
2	120
3	560
4	1820
5	4592
6	10052
7	15080
8	16251
9	12736
10	3876
11	432

Таблица 3: Значения сложности функций при $n = 5$ (представители классов эквивалентности по группе Джевонса)

Сложность	Количество функций	Сложность	Количество функций
1	6	12	186495
2	13	13	243675
3	66	14	201856
4	189	15	169425
5	818	16	78262
6	2378	17	35027
7	7815	18	5762
8	18457	19	623
9	45083	20	26
10	81304	21	3
11	150874		

Таблица 4: Значения сложности Banchmarks-функций

Banchmarks-функции	Сложность		
	$n = 6$	$n = 7$	$n = 8$
«сложные» в классах H_b, H [2]	34	57	102
«сложные» в классах EH_b [4]	31	56	99
«сложные» в классе EH [4]	32	63	122

Список литературы

- [1] Винокуров С. Ф., Рябец Л. В. Алгоритм точной минимизации булевых функций в классе кронекеровых форм // Алгебра и теория моделей 4. Новосибирск, 2003. С. 148–159.
- [2] Избранные вопросы теории булевых функций / А. С. Балюк, С. Ф. Винокуров, А. И. Гайдуков, О. В. Зубков, К. Д. Кириченко, В. И. Пантелеев, Н. А. Перязев, Ю. В. Перязева ; под ред. С. Ф. Винокурова, Н. А. Перязева. М. : Физматлит, 2001. 192 с.
- [3] Францева А. С. Алгоритм минимизации функций алгебры логики в классе обратимых схем Тоффоли // Известия Иркутского государственного университета. Серия Математика. 2018. Т. 25. С. 144–158. <https://doi.org/10.26516/1997-7670.2018.25.144>
- [4] Францева А. С. Сложность представлений булевых функций в классах расширенных двупорожденных операторных форм // Сибирские электронные математические известия : электронное периодическое издание. 2019. Т. 16. С. 523–541. <https://doi.org/10.33048/semi.2019.16.034>
- [5] Toffoli T. Reversible Computing // Automata Languages and Programming (Series: Lecture Notes in Computer Science). 1980. Vol. 85. P. 632–644. https://doi.org/10.1007/3-540-10003-2_104

An Approximate Algorithm for Finding the Complexity of Reversible Implementations Boolean Functions' Extended Kronecker Forms

Vinokurov Sergey Fedorovich, Frantseva Anastasiya Sergeevna

Irkutsk State University, e-mail: servin38@gmail.com, a.s.frantseva@gmail.com

In this paper, the research of the problem of reversible implementations of Boolean functions' polynomial normal representations (exclusive-or sum-of-products expressions) continues. An implementation of the algorithm for finding the complexity of reversible implementations Boolean functions' extended Kronecker forms is given. These researches are also theoretical interest and can be used to find an unknown estimate of the Shannon function's value of the complexity of Boolean functions' representations in the corresponding class of reversible implementations.

Keywords: Toffoli function, reversible circuits, Boolean functions, Kronecker form.