Представление многовыходных булевых функций обратимыми схемами в базисе Тоффоли

С. Ф. Винокуров[1], А. С. Казимиров[2], А. С. Францева[3]
ФГБОУ ВО Иркутский государственный университет
[1]servin38@gmail.com, [2]A.kazimirov@gmail.com, [3]a.s.frantseva@gmail.com

***Аннотация.* В работе рассматривается задача представления булевых функций обратимыми схемами, построенными из элементов Тоффоли. Поскольку обратимые схемы реализуют в общем случае обратимые функции, в исследовании использован метод Тоффоли-Фредкина для представления булевых функций обратимыми многовыходным булевыми функциями. Исследования касаются непосредственно представления многовыходных булевых функций схемами из указанных элементов. В работе приводится оценка сложности схемных представлений. Указанная сложность зависит от выбора класса полиномов булевых функций, в котором функция представлена. Поэтому в работе рассматриваются минимальные полиномиальные представления булевых функций и построены последовательности множеств самых сложных булевых функций в классах расширенных полиномов.**

Ключевые слова: булевы функции; полиномиальные нормальные формы; функции Тоффоли; обратимые схемы

I. Введение

В работе продолжаются исследования задачи построения минимальных представлений многовыходных булевых функций в классе обратимых схем, построенных из элементов Тоффоли. По методу Тоффоли-Фредкина [7] каждая булева функция имеет представление в виде обратимой функции, которая реализуется обратимой схемой. Схемы строятся в базисе Тоффоли [8].

Количество элементов в обратимой схеме зависит от полиномиального представления булевой функции. Поэтому актуальной является задача построения минимального полинома булевой функции. Например, найдено значение сложности для полиномиальной нормальной формы булевой функции от 7 переменных, оно равно 24. Вопрос существования полиномов сложности 25, 26 остается открытым [2]. Однако сложность обратимой схемы, реализующей соответствующую обратимую функцию, будет заведомо больше, поскольку требуется учесть, что отрицания над переменными в полиноме булевой функции реализуются отдельными элементами в схеме и значения входных переменных в схеме должны быть восстановлены. Таким образом, обратимая схема, реализующая данный полином, будет состоять из 24 элементов Тоффоли, реализующих каждое слагаемое полинома и из не более чем 62 элементов Тоффоли, реализующих отрицания над переменными и восстанавливающих значения переменных.

В работе рассматриваются классы расширенных поляризованных полиномов Жегалкина *ZhE* и расширенных кронекеровых форм *KroE*, построены последовательности множеств M_n и V_n самых сложных булевых функций в этих классах и приведены оценки их сложности в классе обратимых схем *RS*. Построенные ранее [3] самые сложные функции для классов поляризованных полиномов Жегалкина *Zh* и кронекеровых форм *Kro* не являются сложными в рассматриваемых классах расширенных полиномов.

Для описания классов полиномиальных нормальных форм булевых функций используется операторный подход [3].

Для построения последовательности множеств M_n и V_n использовались алгоритмы минимизации, основой для их разработки является алгоритм минимизации булевых функций в классе кронекеровых форм, разработанный в [5].

II. Классы полиномов булевых функций

В работе будут использоваться следующие соглашения и обозначения:

1) аргументы и значения функции алгебры логики выбираются из множества $\{0,1\}$;

2) $-x$ – функция отрицания;

3) $x \cdot y$ – функция произведения или конъюнкция;

4) $x \oplus y$ – функция сложение по модулю 2.

Под многовыходной булевой (n,k)*-функцией* f *будем называть отображение из множества* $\{0,1\}^n$ *в множество* $\{0,1\}^k$.

В этой терминологии $(n,1)$-функция соответствует булевой функции в традиционном употреблении терминов [6].

Класс расширенных поляризованных полиномов Жегалкина *ZhE* описан в [1]. Класс расширенных кронекеровых форм *KroE* вводится аналогично следующим образом.

Возьмем оператор $b = b_1 \ldots b_n$, где $b_j \in \{e, p, d\}$, построим класс K_b однородных операторных пучков $A_i = (a^{0,i}, \ldots, a^{N,i})$ $(N = 2^n - 1)$ по всем i от 0 до $2^n - 1$ таких, что $b = a^{0,i}$. Классу кронекеровых форм *Kro* соответствует объединение классов K_b по всем операторам b по базисной функции конъюнкции

$$g(x_1,\dots, x_n) = x_1 \cdot \dots \cdot x_n.$$

Составим оператор c^i как сумму операторов пучка A_i, взятого из K_b [3]. Обозначим через Kro_iE класс таких операторных пучков $C \subset A_i \cup \{c^i\}$, что мощность каждого равна 2^n и назовем его *i-ым классом расширенных кронекеровых форм*. Объединение классов Kro_iE составляет класс *KroE расширенных кронекеровых форм.*

Класс *ZhE* содержит класс поляризованных полиномов Жегалкина *Zh*, класс кронекеровых форм Kro содержит класс Zh, класс *KroE* содержит класс *Kro* и класс *ZhE*.

Пусть $(n,1)$-функция f имеет операторную форму в однородном операторном пучке A_i:

$$O^i(f)=a^{1,i}(x_1 \cdot\ldots\cdot x_n)\oplus \ldots \oplus a^{s,i}(x_1 \cdot\ldots\cdot x_n),$$

где $a^{k,i}$ из A_i и пусть K – множество операторов $a^{k,i}$, входящих в $OF(f)$. Тогда по пучку $C\in Kro_iE$ операторная форма $O^i_+(f)$ совпадает с $O^i(f)$, если оператор c^i в пучке C подставлен вместо оператора $a^{j,i}$, не входящего в $O^i(f)$; в противном случае

$$O^i_+(f)=c^i(x_1 \cdot\ldots\cdot x_n) \oplus a^{1,i}(x_1 \cdot\ldots\cdot x_n)\oplus \ldots \oplus a^{l,i}(x_1 \cdot\ldots\cdot x_n),$$

где $a^{j,i}$ принадлежат A_i и не принадлежат K.

Пример 1. При $n = 3$ рассмотрим однородный операторный пучок $A_3 = (ddd, ddp, ded, dep, pdd, pdp, ped, pep)$ из класса K_{ddd}, который соответствует Zh_3. Оператор суммы будет следующим:

$$c^3 = ddd\oplus ddp\oplus ded\oplus dep\oplus pdd\oplus pdp\oplus ped\oplus pep = \mathbf{epe}.$$

Расширенный операторный пучок:

$$C = (ddd, \mathbf{epe}, ded, dep, pdd, pdp, ped, pep).$$

Рассмотрим функцию $f(x_1, x_2, x_3) = 10100100$.

$$O^i(f) = 1\oplus -x_3 \oplus x_2\oplus -x_1 \oplus x_2 (-x_3) \oplus(- x_1)\, x_2\oplus(- x_1)x_2(-x_3);$$

$$O^i_+(f) =(- x_1)(-x_3) \oplus x_1(-x_2)x_3.$$

Пусть $L(O^i)$ – число слагаемых в операторной форме O^i. Тогда сложность представления булевой функции f в классе полиномов Q определяется так: $L_Q(f) = min_{O^i}L(O^i)$ по всем O^i составленным по пучкам класса Q.

III. Класс обратимых схем RS

Любая булева функция $f(x_1,\ldots,x_n)$ может быть представлена обратимой $(n+1,n+1)$-функцией $F(x_0, x_1, \ldots, x_n)$, задающей однозначное отображение множества $\{(a_0,a_1,\ldots,a_n)\}$ на множество $\{(a_0\oplus f(a_1,\ldots,a_n), a_1,\ldots,a_n)\}$.

Будем рассматривать множество $\boldsymbol{T}$ (называемое базисом Тоффоли) обратимых функций (называемых функциями Тоффоли [8]) следующего вида:

1) $T_0^{n+1}(x_i)$ задают отображение

$$(x_0, x_1, \ldots, x_i \ldots, x_n) \to (x_0, x_1, \ldots, -x_i \ldots, x_n),\ i\in\{0,\ldots,n\};$$

2) $T_k^{n+1}(x_{i1},\ldots,x_{ik}, x_0)$ задают отображение

$$(x_0, x_1, \ldots, x_n) \to (x_0 \oplus x_{i1} \cdot\ldots\cdot x_{ik}, x_1,\ldots, x_n),$$
$$k > 0,\ \{i1,\ldots, ik\} \subseteq \{1,\ldots,n\}.$$

Множество всех функций вида F включено в замыкание множества функций T по операции суперпозиции обратимых функций [1].

Структурное описание обратимых схем и их функционирование описано в [6]. В общем виде обратимая схема, реализующая функцию $F(x_0, x_1, \ldots, x_n)$ выглядит так, как показано на рис. 1. В качестве элементов в схеме используются функции множества T, в этом случае их называют элементами Тоффоли.

Обратимая функция $F(x_0, x_1, \ldots, x_n)$ реализуется обратимой схемой в зависимости от вида операторной формы функции $f(x_1, \ldots, x_n)$.

Пример 2. Для функции $f(x_1, x_2, x_3) = 10100100$ из примера 1 обратимые схемы, реализующие обратимую функцию $F(x_0, x_1, x_2, x_3)$ имеют вид, изображенный на рис. 2 и 3 в соответствии с операторными формами функции.

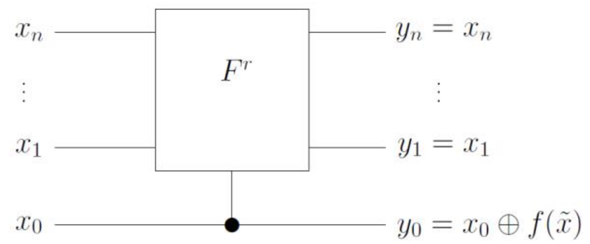

Рис. 1. Обратимая схема, реализующая обратимую функцию *F*.

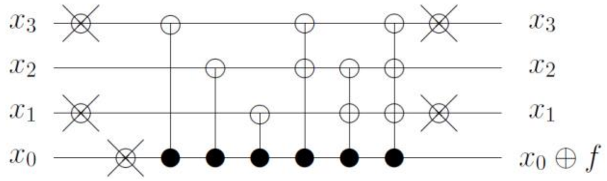

Рис. 2. Обратимая схема, реализующая булеву функцию $f(x_1, x_2, x_3) = 10100100$, представленную операторной формой O^i

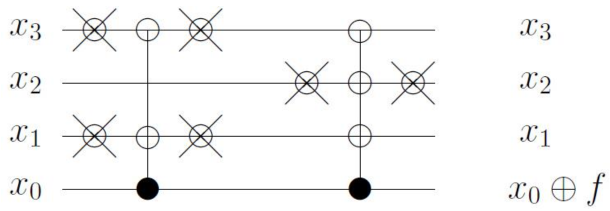

Рис. 3. Обратимые схемы, реализующие булеву функцию $f(x_1, x_2, x_3) = 10100100$, представленную операторной формой O_+^i

Пусть *RS* – класс обратимых схем на элементах Тоффоли, реализующих функции вида *F*.

IV. Алгоритмы

Более подробное описание алгоритма минимизации многовыходных булевых функций в классе *RS* предложено в [1]. Этот алгоритм включает в себя алгоритм минимизации булевых функций в классах полиномов *ZhE, KroE*. Поэтому далее шаги этих алгоритмов представлены в сокращенном виде.

A. Алгоритм минимизации булевых функций в классах полиномов ZhE, KroE

1. Предварительно построить бинарную матрицу B, содержащую информацию о классе *Zh* или *Kro*.
2. Булева функция f представлена совершенной полиномиальной нормальной формой. Построить специальную операторную форму функции, $SOF(f)$.
3. По матрице B и $SOF(f)$ вычислить сложности $L(O^i)$ представлений функции в операторных пучках выбранного класса полиномов.
4. По значениям $L(O^i)$ вычислить сложности $L(O_+^i)$ представлений функции в операторных пучках класса *ZhE* или *KroE*.
5. Вычислить сложность $L(f)$.

B. Алгоритм минимизации булевых функций в классе обратимых схем RS

1. Выполнить шаги 1–4 предыдущего алгоритма.
2. Построить обратимые схемы для операторных форм O^i и O_+^i функции f.
3. Выбрать схему с минимальным количеством элементов в ней [4].

V. Результаты алгоритмов

Алгоритм *A.* позволил построить последовательность множеств M_n самых сложных функций в классе *ZhE* и последовательность множеств V_n – в классе *KroE*.

Класс ZhE.

$M_n = \{p_n(x_1,..., x_n), q_n(x_1,..., x_n), t_n(x_1,..., x_n)\}$ $(n > 2)$, которые определим индуктивно следующим образом:

1) $p_3(x_1, x_2, x_3) = (00011011)$, $q_3(x_1, x_2, x_3) = (11010001)$, $t_3(x_1, x_2, x_3) = (11001010)$,
2) $p_n(x_1,..., x_n) = x_nq_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_np_{n-1}(x_1,..., x_{n-1})$,
$q_n(x_1,..., x_n)= x_nt_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_nq_{n-1}(x_1,..., x_{n-1})$,
$t_n(x_1,..., x_n) = x_n p_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_nt_{n-1}(x_1,..., x_{n-1})$.

Класс KroE.

$V_n = \{p_n(x_1,..., x_n), q_n(x_1,..., x_n), t_n(x_1,..., x_n)\}$ $(n > 3)$, которые определим индуктивно следующим образом:

$p_4(x_1, x_2, x_3, x_4) = (0001011001101001)$,
$q_4(x_1, x_2, x_3, x_4) = (1110100010000001)$,
$t_4(x_1, x_2, x_3, x_4) = (1111111011101000)$,

2) $p_n(x_1,..., x_n) = x_nq_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_np_{n-1}(x_1,..., x_{n-1})$,
$q_n(x_1,..., x_n) = x_nt_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_nq_{n-1}(x_1,..., x_{n-1})$,
$t_n(x_1,..., x_n) = x_n p_{n-1}(x_1,..., x_{n-1}) \oplus \neg x_nt_{n-1}(x_1,..., x_{n-1})$.

Для удобства представления данных функций используется обозначение: $f_i = f(x_1,..., x_i)$. Функции множеств M_n и V_n обладают следующими свойствами:

1) $p_n \oplus q_n \oplus p_n = 0$
2) $p_n = x_nq_{n-1} \oplus \neg x_np_{n-1} = x_nt_{n-1} \oplus p_{n-1} = \neg x_nt_{n-1} \oplus q_{n-1}$,
3) $q_n = x_nt_{n-1} \oplus \neg x_nq_{n-1} = x_np_{n-1} \oplus q_{n-1} = \neg x_np_{n-1} \oplus t_{n-1}$,
4) $t_n = x_np_{n-1} \oplus \neg x_nt_{n-1} = x_nq_{n-1} \oplus t_{n-1} = \neg x_nq_{n-1} \oplus p_{n-1}$.

Теорема 1 [6]**.** Для любой функции f_i из множества M_n сложность представлений функций в классе *ZhE* равна:

$$L_{ZhE}(f_i) = 2^{n-1}.$$

Теорема 2 [6]**.** Обратимые схемы, реализующие обратимые представления функций множества M_n, состоят из 2^{n-1} элементов Тоффоли T_k, $k > 0$, и не более $2n$ элементов T_0.

Теорема 3. Обратимые схемы, реализующие обратимые представления функций множества V_n, состоят из $\lfloor 5/12 \rfloor \cdot 2^{n-1}$ элементов Тоффоли T_k, $k > 0$, и не более 2^{n-1} элементов T_0.

Список литературы

[1] Алгоритм построения минимального представления многовыходных функций алгебры логики в классе обратимых схем вычислениях / С.Ф. Винокуров, Л.В. Рябец, С.И. Тодиков, А.С. Францева // Материалы XX Международной конференции по мягким вычислениям и измерениям SCM'2017., Санкт-Петербург, 24-26 мая 2017 / СПбГЭТУ «ЛЭТИ», С.-Петербург 2017. С. 175-178.

[2] Винокуров С.Ф., Казимиров А.С. О сложности одного класса булевых функций // Известия Иркутского государственного университета. Серия: Математика. 2010. Том 3. № 4. С. 2-6.

[3] Избранные вопросы теории булевых функций: Моногр. / Под ред. С.Ф. Винокурова и Н.А. Перязева. М. :ФИЗМАТЛИТ, 2001. 192 с.

[4] Пат. РФ № 2017619310 / С.Ф. Винокуров, Л.В. Рябец, А.С. Францева. Программа построения минимального представления многовыходных булевых функций в классе обратимых схем; Опубл. 22.08.17. Бюл. № 9.

[5] Рябец Л.В., Винокуров С.Ф. Алгоритм точной минимизации булевых функций в классе кронекеровых форм // Алгебра и теория моделей 4. 2003. С. 148-159.

[6] Схемная сложность представлений многовыходных функций алгебры логики в обратимых вычислениях / С.Ф. Винокуров, А.С. Францева // Материалы XIX Международной конференции по мягким вычислениям и измерениям SCM'2016., Санкт-Петербург, 25-27 мая 2016 / СПбГЭТУ «ЛЭТИ», С.-Петербург 2016. С. 130-133.

[7] Fredkin E., Toffoli T. Conservative Logic // International Journal of Theoretical Physics. 1982. Vol. 21, Iss. 3. P. 219-253.

[8] Toffoli T. Reversible Computing // Automata, Languages and Programming (Series: Lecture Notes in Computer Science). 1980. Vol. 85. P. 632-644.