Серия «Математика»
2016. Т. 16. С. 30—42

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.673
MSC 94C10

Сложность представлений многовыходных функций алгебры логики *

С. Ф. Винокуров, А. С. Францева
Иркутский государственный университет

Аннотация. В работе исследуется вопрос сложности логических схем, реализующих функции алгебры логики. Реализация функций алгебры логики рассматривается в классе логических схем, называемых обратимыми. Для построения обратимых схем используются элементарные обратимые схемы, известные под названием элементов Тоффоли. За исключением двух функций одного аргумента, все функции алгебры логики не являются обратимыми. Однако их можно моделировать так называемыми многовыходными функциями, у которых число выходов совпадает с числом аргументов и которые являются перестановками на множестве наборов аргументов. В работе использовано представление функций алгебры логики многовыходными функциями. Многовыходные функции, в свою очередь, реализованы обратимыми схемами в базисе Тоффоли. Для функции схема, ее реализующая, не определена однозначно. Это позволяет определить сложность функции, как сложность минимальной схемы, реализующей эту функцию. В представленных результатах решена задача нахождения сложности самой сложной функции или функции Шеннона для класса всех функций алгебры логики в классе обратимых схем в подмножестве базиса Тоффоли. Решение этой задачи сведено к решению задачи нахождения функции Шеннона для класса булевых функций в классе полиномиальных форм, называемых расширенными полиномами Жегалкина. Для решения задачи нахождения функции Шеннона для класса булевых функций в классе расширенных полиномов Жегалкина построены последовательности множеств функций по количеству аргументов. Для функций в этих множествах найдена сложность их полиномиальных представлений и доказано, что эти функции имеют максимальную сложность среди всех функций в классе расширенных полиномов Жегалкина.

Ключевые слова: функции алгебры логики, многовыходные функции, обратимые функции, элементы Тоффоли, обратимые схемы, сложность, полином Жегалкина.

* Работа выполнена в рамках проекта 14.579.21.0092 ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технического комплекса России на 2014–2020 годы, № RFMEFI57914X0092.

1. Введение

Внимание к обратимым схемам связано с моделированием обратимых вычислений. Интерес к такого рода математическим моделям вычислений обусловлен, прежде всего, перспективными направлениями конструирования технических устройств, реализующих квантовые вычисления. Постулирование обратимости квантовых вычислений исходит из физических свойств квантового мира и привязано к затратам энергии на преобразование информации. Обратимые преобразования информации существенно эффективнее по энергозатратам по сравнению с традиционными — необратимыми [3; 4]. Для построения обратимых схем используются элементарные обратимые схемы, известные под названием элементов Тоффоли или базиса Тоффоли. В общем виде схема представляет собой последовательное соединение базисных элементов. Сложностью схемы считается количество элементов в этой схеме. Обратимые схемы реализуют взаимно однозначные или обратимые функции. Традиционные функции алгебры логики с числом аргументов больше одного не являются обратимыми. Однако, возможность их реализации обратимыми схемами определена их представлением многовыходными функциями. Для обратимости многовыходных функций необходимо выполнение условия равенства числа входов с числом выходов функции. В случае определения на конечных множествах обратимые функции являются просто перестановками элементов этих множеств. Более детально описание реализаций обратимых функций обратимыми схемами, а также алгоритмов вычисления их сложности можно найти, например, в [1; 2].

2. Основные определения и обозначения

Многовыходной $(n,k)-$функцией f будем называть отображение из множества наборов $\{0,1\}^n$ в множество $\{0,1\}^k$.

В этой терминологии понятию $(n,1)-$функции соответствует понятие функции алгебры логики или булевой функции в традиционном употреблении терминов. Многовыходную $(n,k)-$функцию $f(x_1,...,x_n)$ иногда удобно представлять набором из k функций алгебры логики

$$f(x_1,...,x_n) = (f_1(x_1,...,x_n),...,f_k(x_1,...,x_n)).$$

Под обратимой функцией $f(x_1,...,x_n)$ будем понимать такую многовыходную $(n,n)-$функцию $(f_1(x_1,...,x_n),...,\ f_n(x_1,...,x_n))$, что отображение

$$f : \{(\alpha_1,...,\alpha_n)\} \to \{(f_1(\alpha_1,...,\alpha_n),...,f_n(\alpha_1,...,\alpha_n))\}$$

является однозначным.

Для сокращения записи пусть $\tilde{x}_k^i = x_i, x_{i+1}, ..., x_k$, $\tilde{x} = x_1, ..., x_n$.

Любая многовыходная (n,k)-функция $f(\tilde{x}) = (f_1(\tilde{x}), ..., f_k(\tilde{x}))$ может быть представлена $(n+k, n+k)$-функцией

$$F(\tilde{c}_k^1, \tilde{x}) : (c_1, ..., c_k, x_1, ..., x_n) \ \mapsto \ (c_1 \oplus f_1(\tilde{x}), ..., c_k \oplus f_k(\tilde{x}), x_1, ..., x_n),$$

Легко заметить, что функция F является обратимой и первые k компонент вектора при всех $c_i = 0$ соответствуют исходной (n,k)-функции $f(\tilde{x})$.

В частности, $(n,1)$-функция $f(\tilde{x})$ представляется *обратимой функцией*

$$F(\tilde{x}_n^0) : \ (x_0, x_1, ..., x_n) \ \mapsto \ (x_0 \oplus f(\tilde{x}), x_1, ..., x_n).$$

В дальнейшем изложении используются только такие обратимые функции. Исключения будут специально оговариваться.

Пусть даны две обратимые функции $F(x_0,x_1, ..., x_n)$, $G(x_0, x_1, ..., x_n)$, которые представляют $(n,1)$-функции $f(\tilde{x})$ и $g(\tilde{x})$, соответственно. Тогда, по определению суперпозиции [1], функция

$$H(x_0, x_1, ..., x_n) = G(F(x_0, x_1, ..., x_n))$$

представляет $(n,1)$-функцию

$$h(x_1, ..., x_n) = f(x_1, ..., x_n) \oplus g(x_1, ..., x_n).$$

Через RF будем обозначать класс обратимых функций вида $F(\tilde{x}_n^0)$.

Рассмотрим класс T, содержащий следующие функции, определенные в [5]:

$$\begin{aligned} T_1^{n+1}(x_i) : \ & (x_0, x_1, ..., x_i, ..., x_n) \to (x_0, x_1, ..., \bar{x}_i, ..., x_n); \\ T_{k+1}^{n+1}(x_{i_1}, ..., x_{i_k}, x_0) : \ & (x_0, x_1, .., x_n) \to (x_0 \oplus x_{i_1} \cdot ... \cdot x_{i_k}, x_1, ..., x_n), \\ & k \le n, \ \{i_1, ..., i_k\} \subset \{1, ..., n\}. \end{aligned}$$

В [5] сформулирована и доказана следующая теорема:

Теорема 1. *Любая обратимая функция $F(x_0, x_1, ..., x_n)$, реализующая $(n,1)$-функцию алгебры логики $f(x_1, ..., x_n)$, может быть получена суперпозицией элементов класса T.*

Класс T получил название базиса Тоффоли, функции этого класса называются функциями Тоффоли.

В общем виде схема, реализующая обратимую функцию $F(\tilde{x}_n^0)$, показана на рис. 1. Входы и выходы схемы на рисунке изображены слева и справа, соответственно.

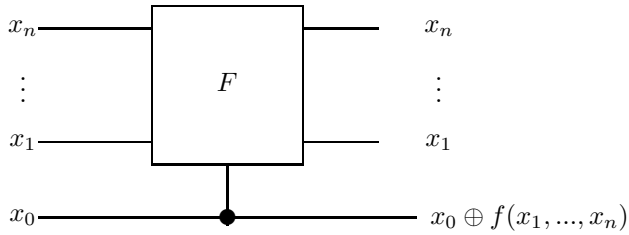

Рис. 1. Обратимая схема, реализующая функцию F.

В [4] обосновываются необходимость некоторых свойств технической реализации обратимых схем. В частности, обосновывается свойство, что значение выходов совпадает со значением входов. Это свойство позволяет суперпозицию функций F и G реализовать простым соединением выходов схемы функции F с соответствующими входами схемы функции G, как это показано на рис. 2.

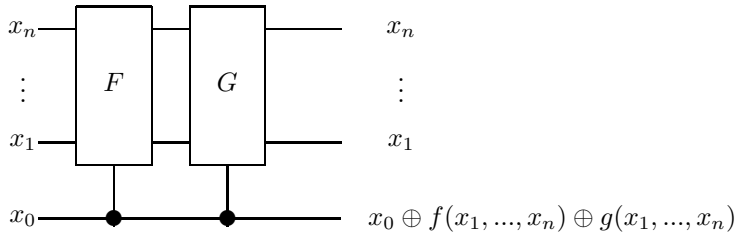

Рис. 2. Суперпозиция функций F и G.

Примеры элементарных схем, реализующих функции базиса T приведены на рис. 3.

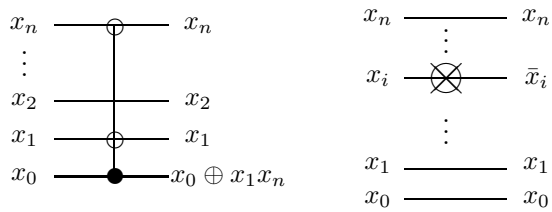

Рис. 3. Обратимые схемы, реализующие функции $T_3^{n+1}(x_1, x_n, x_0)$ и $T_1^{n+1}(x_i)$, соответственно.

Теорема 1 гарантирует, что для любой обратимой функции F, представляющей $(n, 1)$-функцию алгебры логики f, существует обратимая схема, построенная из схем, реализующих базисные функции класса

T. Поскольку функция может быть реализована разными схемами, с различным количеством элементов, интересен вопрос о существовании некоторой оптимальной схемы, например, с минимальным количеством элементов.

Схемы, реализующих базисные функции класса T, называют элементами Тоффоли. А множество таких элементарных схем — схемным базисом Тоффоли. Мы будем называть его просто базисом Тоффоли, как и функциональный базис, если из контекста ясно, о каких представлениях идет речь.

Пусть RS — класс обратимых схем в базисе T, реализующих обратимые функции вида $F(\tilde{x}_n^0)$.

Количество элементов в схеме S будет называться *сложностью схемы* и обозначаться $|S|$.

Сложность $L_{RS}(F)$ функции F, в классе обратимых схем RS определяется следующим образом:

$$L_{RS}(F) = \min_S |S|$$

по всем схемам S, реализующим F.

Функция сложности $L_{RS}(n)$ или функция Шеннона для класса всех $(n,1)$-функций определяется так:

$$L_{RS}(n) = \max_F(L_{RS}(F)).$$

Функция сложности $L_{RS}(M)$ для некоторого подмножества M множества всех $(n,1)$-функций определяется так:

$$L_{RS}(M) = \max_F(L_{RS}(F))$$

по всем функциям F, реализующим функции из множества M.

Пусть x^σ обозначает x, если $\sigma = 1$, и $\bar{x}$, если $\sigma = 0$.

Производная $f'_{x_i}(x_1, ..., x_n)$ по переменной x_i для функции алгебры логики $f(x_1, ..., x_n)$ определена стандартно:

$$f'_{x_i}(x_1, ..., x_n) = f(x_1, ..., x_{i-1}, 0, x_{i+1}, ..., x_n) \oplus f(x_1, ..., x_{i-1}, 1, x_{i+1}, ..., x_n).$$

При рассмотрении полиномиальных представлений удобно применять оператор производной: $d^0_{x_i}(f(\tilde{x})) = f'_{x_i}(\tilde{x})$, $d^1_{x_i}(f(\tilde{x})) = f(\tilde{x})$;

$$d^{\tau_1,...,\tau_n}_{x_1,...,x_n} f(x_1, ..., x_n) = d^{\tau_n}_{x_n}\left(d^{\tau_1,...,\tau_{n-1}}_{x_1,...,x_{n-1}} f(x_1, ..., x_n)\right).$$

Подробно операторы и их свойства изложены в [3].

Множество функций

$$Zh_{\tilde{\sigma}} = \{d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}),\ \tilde{\sigma} \in \{0,1\}^n\}$$

называют базисом поляризованного полинома Жегалкина поляризации $\tilde{\sigma}$.

Пусть $Zh = \bigcup_{\tilde{\sigma}\in\{0,1\}^n} Zh_{\tilde{\sigma}}$ обозначает класс поляризованных полиномов Жегалкина.

Поляризованный полином Жегалкина для функции $f(x_1, ..., x_n)$ имеет вид:

$$f(x_1, ..., x_n) = \sum_{\tilde{\tau}\in\{0,1\}^n} \alpha_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}) = P,$$

где $\tilde{\sigma} = (\sigma_1, ..., \sigma_n)$ – вектор поляризации, $\alpha_{\tilde{\tau}} \in \{0, 1\}$ — коэффициенты представления.

Сложностью $L_{Zh_{\tilde{\sigma}}}(P)$ полинома P будем называть число ненулевых коэффициентов $\alpha_{\tilde{\tau}}$:

$$L_{Zh_{\tilde{\sigma}}}(P) = \sum_{\tilde{\tau}\in\{0,1\}^n} \alpha_{\tilde{\tau}}.$$

Сложность $L_{Zh}(f)$ $(n, 1)$-функции $f(\tilde{x})$ в классе Zh определяется следующим образом:

$$L_{Zh}(f) = \min_{\tilde{\sigma}}(L_{Zh_{\tilde{\sigma}}}(P)).$$

Функция Шеннона $L_{Zh}(n)$ для класса всех функций алгебры логики определяется так:

$$L_{Zh}(n) = \max_{f}(L_{Zh}(f)).$$

Теорема 2. *Пусть* $V \subset Zh_{\tilde{\sigma}} \cup \{x_1^{\bar{\sigma}_1} \cdot ... \cdot x_n^{\bar{\sigma}_n}\}$ *и* $|V| = 2^n$. *Тогда любая функция алгебры логики* $f(x_1, ..., x_n)$ *имеет единственное представление следующего вида:*

$$f(x_1, ..., x_n) = \sum_{\tilde{\tau}\in\{0,1\}^n} \beta_{\tilde{\tau}} g^{\tilde{\tau}}(x_1, ..., x_n),$$

где $g^{\tilde{\tau}}(x_1, ..., x_n) \in V$, $\beta_{\tilde{\tau}} \in \{0, 1\}$.

Доказательство. Следует из теоремы о представлении произвольной функции алгебры логики $f(\tilde{x})$ в виде суммы образов базисной функции по пучку расширенных операторных форм [3]. Достаточно в качестве базисной функции взять произведение $x_1 \cdot ... \cdot x_n$, а базисный пучок, по которому составляется расширенная форма, имеет вид $(d...d, ..., a_1...a_n)$, где $a_i \in \{p, e\}$. □

Множество V будем называть базисом. Множество разложений по базисам из $Zh_{\tilde{\sigma}} \cup \{x_1^{\bar{\sigma}_1} \cdot ... \cdot x_n^{\bar{\sigma}_n}\}$будем называть классом расширенных полиномов поляризации $\tilde{\sigma}$ и обозначать через $Zh_{\tilde{\sigma}}E$.

Множество $ZhE = \bigcup_{\tilde{\sigma}\in\{0,1\}^n} Zh_{\tilde{\sigma}}E$ будем называть классом расширенных полиномов.

3. Сложность представления $(n,1)$-функций в классе расширенных полиномов

Введем последовательность $(n,1)$-функций, определяемых индуктивно:

$$p_3(x_1,x_2,x_3)=(00011011),\ q_3(x_1,x_2,x_3)=(11010001),$$
$$t_3(x_1,x_2,x_3)=(11001010);$$
$$p_n(x_1,...,x_n)=x_nq_{n-1}(x_1,...,x_{n-1})\oplus\bar{x}_np_{n-1}(x_1,...,x_{n-1}),$$
$$q_n(x_1,...,x_n)=x_nt_{n-1}(x_1,...,x_{n-1})\oplus\bar{x}_nq_{n-1}(x_1,...,x_{n-1}),$$
$$t_n(x_1,...,x_n)=x_np_{n-1}(x_1,...,x_{n-1})\oplus\bar{x}_nt_{n-1}(x_1,...,x_{n-1}).$$

Для удобства представления последовательности функций используется обозначение: $f_i=f(x_1,...,x_i)$.

Лемма 1. *Для функций из $M_n=\{p_n,\ q_n,\ t_n\}$ справедливы следующие равенства:*

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

Доказательство. Свойство 1) докажем индукций по числу переменных.

При $n=3$ равенство проверяется непосредственно.

Пусть $n>3$. Тогда по индукции

$$p_n\oplus q_n\oplus t_n=x_nq_{n-1}\oplus\bar{x}_np_{n-1}\oplus x_nt_{n-1}\oplus\bar{x}_nq_{n-1}\oplus x_np_{n-1}\oplus\bar{x}_nt_{n-1}=$$
$$=x_n(p_{n-1}\oplus q_{n-1}\oplus t_{n-1})\oplus\bar{x}_n(p_{n-1}\oplus q_{n-1}\oplus t_{n-1})=0.$$

Равенство 2) следует из свойства 1):

$$p_n=x_nq_{n-1}\oplus\bar{x}_np_{n-1}=x_nq_{n-1}\oplus x_np_{n-1}\oplus p_{n-1}=$$
$$=x_n(q_{n-1}\oplus p_{n-1})\oplus p_{n-1}=x_nt_{n-1}\oplus p_{n-1};$$

$$p_n=x_nq_{n-1}\oplus\bar{x}_np_{n-1}=x_nq_{n-1}\oplus\bar{x}_np_{n-1}\oplus q_{n-1}\oplus q_{n-1}=$$
$$=\bar{x}_n(q_{n-1}\oplus p_{n-1})\oplus q_{n-1}=\bar{x}_nt_{n-1}\oplus q_{n-1}.$$

Остальные равенства доказываются аналогично. □

Лемма 2. *Для любой функции $f(\tilde{x})\in M_n$*

$$L_{Zh}(f)\in\left\{\frac{1}{2}2^n-1,\ \frac{1}{2}2^n,\ \frac{1}{2}2^n+1\right\}.$$

Доказательство. Проводится индукцией по числу переменных n функции f.

При $n=3$ сложности представлений приведены в таблице 1.

Таблица 1.

Вектор поляризации	$L_{Zh_{\tilde{\sigma}}}(p_3)$	$L_{Zh_{\tilde{\sigma}}}(q_3)$	$L_{Zh_{\tilde{\sigma}}}(t_3)$
000	4	5	3
001	4	3	5
010	4	4	4
011	5	3	4
100	5	4	3
101	4	4	4
110	3	4	5
111	3	5	4

При $n > 3$ для любой поляризации $\tilde{\sigma} = \sigma_1, ..., \sigma_n$, согласно лемме 1, сложности функций p_n, q_n, t_n представлены в таблице 2.

Таблица 2.

σ_n	$L(p_n)$	$L(q_n)$	$L(t_n)$
0	$L(t_{n-1}) + L(q_{n-1})$	$L(p_{n-1}) + L(t_{n-1})$	$L(q_{n-1}) + L(p_{n-1})$
1	$L(t_{n-1}) + L(p_{n-1})$	$L(p_{n-1}) + L(q_{n-1})$	$L(q_{n-1}) + L(t_{n-1})$

Сложности $L(p_{n-1})$, $L(q_{n-1})$, $L(t_{n-1})$ принимают значения из множества $\left\{\frac{1}{2}2^{n-1} - 1,\ \frac{1}{2}2^{n-1},\ \frac{1}{2}2^{n-1} + 1\right\}$. Возможны следующие варианты для сложностей $L(p_n)$, $L(q_n)$, $L(t_n)$:

1) $L(p_{n-1}) = L(q_{n-1}) = L(t_{n-1}) = \frac{1}{2}2^{n-1}$;

2) сложности попарно различны.

В первом случае $L(p_n) = L(q_n) = L(t_n) = \frac{1}{2}2^{n-1} + \frac{1}{2}2^{n-1} = \frac{1}{2}2^n$; во втором — получаем три также попарно различные значения сложностей: $\left(\frac{1}{2}2^{n-1} - 1\right) + \left(\frac{1}{2}2^{n-1}\right) = \frac{1}{2}2^n - 1$, $\left(\frac{1}{2}2^{n-1}\right) + \left(\frac{1}{2}2^{n-1} + 1\right) = \frac{1}{2}2^n + 1$, $\left(\frac{1}{2}2^{n-1} - 1\right) + \left(\frac{1}{2}2^{n-1} + 1\right) = \frac{1}{2}2^n$. □

Теорема 3.

$$L_{ZhE}(n) = \frac{1}{2}2^n.$$

Доказательство. Докажем неравенство $L_{ZhE}(n) \leq \frac{1}{2}2^n$.

Пусть

$$f(x_1 ..., x_n) = \bigoplus_{\tilde{\tau} \in \{0,1\}^n} \alpha_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}) \text{ и } k = \sum_{\tilde{\tau} \in \{0,1\}^n} \alpha_{\tilde{\tau}}.$$

Тогда

$$f(x_1 ..., x_n) = \bigoplus_{\tilde{\tau}\in\{0,1\}^n} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}) \oplus \bigoplus_{\tilde{\tau}\in\{0,1\}^n} \bar{\alpha}_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}) =$$

$$= x_1^{\bar{\sigma_1}} \cdot ... \cdot x_n^{\bar{\sigma_n}} \oplus \bigoplus_{\tilde{\tau}\in\{0,1\}^n} \bar{\alpha}_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_1});$$

$$\sum_{\tilde{\tau}\in\{0,1\}^n} \bar{\alpha}_{\tilde{\tau}} = 2^n - k$$

и для сложности $L_{ZhE}(f)$ выполняется:

$$L_{ZhE}(f) = \min_k(k, 2^n - k + 1) \leq \frac{1}{2}2^n.$$

Поскольку это неравенство выполняется для любых функций f, получаем неравенство:

$$L_{ZhE}(n) \leq \frac{1}{2}2^n.$$

Для доказательства неравенства $L_{ZhE}(n) \geq \frac{1}{2}2^n$ рассмотрим множество функций M_n.

По лемме 2 выполняется равенство $L_{Zh}(M_n) = \frac{1}{2}2^n+1$. Пусть $f \in M_n$ и $L_{Zh}(f) = \frac{1}{2}2^n + 1$.

По предыдущим рассуждениям:

$$L_{ZhE}(f) = \min(\frac{1}{2}2^n + 1, 2^n - (\frac{1}{2}2^n + 1) + 1) = \frac{1}{2}2^n.$$

Таким образом, получаем второе неравенство:

$$L_{ZhE}(n) \geq L_{ZhE}(f) = \frac{1}{2}2^n.$$

□

Теорема 3 дает точное значение для функции Шеннона сложности $(n, 1)$-функций в классе расширенных полиномов Жегалкина. Однако из доказательства следует, что это значение также имеет место и для любого класса расширенных поляризованных полиномов любой поляризации.

4. Сложность представления $(n, 1)$-функций в классе обратимых схем

Полученные оценки $L_{Zh}(n)$ и $L_{ZhE}(n)$ позволяют получить верхнюю и нижнюю границы для сложности функций в классе обратимых схем.

Теорема 4.

$$L_{RS}(n) = \frac{1}{2}2^n + O(n),$$

где $1 \le O(n) \le 2n$.

Доказательство. Рассмотрим представления (*n*,1)-функций $f(x_1,...,x_n)$ в классе ZhE.

Как и в доказательстве теоремы 3, пусть функция $f(x_1, ..., x_n)$ имеет представление:

$$f(x_1 ..., x_n) = \bigoplus_{\tilde{\tau}\in\{0,1\}^n} \alpha_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_n}) = P_1$$

Пусть для сложности полинома P_1 имеет место равенство:

$$\sum_{\tilde{\tau}\in\{0,1\}^n} \alpha_{\tilde{\tau}} = \frac{1}{2}2^n + l.$$

Поскольку

$$f(x_1 ..., x_n) = x_1^{\bar{\sigma_1}} \cdot ... \cdot x_n^{\bar{\sigma_n}} \oplus \bigoplus_{\tilde{\tau}\in\{0,1\}^n} \bar{\alpha}_{\tilde{\tau}} d^{\tilde{\tau}}(x_1^{\sigma_1} \cdot ... \cdot x_n^{\sigma_1}) = P_2,$$

то

$$\sum_{\tilde{\tau}\in\{0,1\}^n} \bar{\alpha}_{\tilde{\tau}} + 1 = \frac{1}{2}2^n - l + 1.$$

Тогда схемное представление полинома P_1 будет иметь сложность:

$$L_{RS}(P_1) = \frac{1}{2}2^n + l + 2w,$$

где сумма $\frac{1}{2}2^n + l$ – число элементов из базиса T, которые реализуют соответствующие слагаемые из P_1;
$2w = 2 \cdot \sum_{1\le i\le n} \bar{\sigma}_i$ – число отрицаний T_1^{n+1}, реализующих поляризацию входов, плюс число отрицаний T_1^{n+1}, убирающих поляризацию на выходах.

Схемное представление полинома P_2 будет иметь сложность:

$$L_{RS}(P_2) = \frac{1}{2}2^n - l + 1 + 2n.$$

В этом случае, аналогично,
$\frac{1}{2}2^n - l + 1$ — число элементов из базиса T, реализующих слагаемые полинома P_2;
$2 \cdot \sum_{1\le i\le n} \bar{\sigma}_i$ — реализация поляризации и восстановления выходов для слагаемых P_2, кроме первого, и

$2 \cdot \sum_{1 \le i \le n} \sigma_i$ — реализация поляризации и восстановления выходов для первого слагаемого P_2;

$$2 \cdot \sum_{1 \le i \le n} \bar{\sigma}_i + 2 \cdot \sum_{1 \le i \le n} \sigma_i = 2 \cdot \sum_{1 \le i \le n} (\sigma_i + \bar{\sigma}_i) = 2n.$$

При выборе минимальной схемы возможны два случая:

1) $\frac{1}{2}2^n + l + 2w < \frac{1}{2}2^n - l + 1 + 2n$;

2) $\frac{1}{2}2^n - l + 1 + 2n < \frac{1}{2}2^n + l + 2w$.

Учитывая, что $n, l, 2w$ — целые неотрицательные числа, получаем $l \le n - w$ и $l \ge n - w + 1$ в случаях 1) и 2), соответственно.

Поскольку $w \le n$, оба варианта дают верхнюю оценку на схемную сложность функции f:

$$L_{RS}(f) \le \frac{1}{2}2^n + 2n.$$

Для установления нижней оценки рассмотрим сложность функций из множества M_n.

По лемме 2 сложность этих функций в классе Zh либо совпадает и равна $\frac{1}{2}2^n$, либо сложности попарно различны и их значения содержатся в множестве $\left\{\frac{1}{2}2^n - 1,\ \frac{1}{2}2^n,\ \frac{1}{2}2^n + 1\right\}$. В соответствии с этим разделим поляризации $\tilde{\sigma}$ на

$\tilde{\sigma}'$ – поляризации, при которых функции из M_n имеют одинаковую сложность $\frac{1}{2}2^n$;

$\tilde{\sigma}''$ — поляризации, при которых сложности функций из M_n принимают значения из множества $\left\{\frac{1}{2}2^n - 1,\ \frac{1}{2}2^n,\ \frac{1}{2}2^n + 1\right\}$.

Тогда схемная реализация данных функций дает сложность:

$$L_{RS}(M_n) = \min\left\{\min_{\tilde{\sigma}''}(\frac{1}{2}2^n + 1 + 2w), \min_{\tilde{\sigma}'}(\frac{1}{2}2^n + 2w)\right\}.$$

Из доказательства леммы 2 следует
$\min_{\tilde{\sigma}''}(\frac{1}{2}2^n + 1 + 2w) = \frac{1}{2}2^n + 1$; $\min_{\tilde{\sigma}'}(\frac{1}{2}2^n + 2w) = \frac{1}{2}2^n + 2$.
Отсюда получаем нижнюю оценку:

$$L_{RS}(n) \ge L_{RS}(M_n) = \frac{1}{2}2^n + 1.$$

□

Следствие 1. *Для функции $L_{RS}(n)$ выполняется асимптотическое равенство:*

$$L_{RS}(n) \cong \frac{1}{2}2^n.$$

5. Заключение

Теорема 3 дает точное значение функции Шеннона сложности функций алгебры логики в классе расширенных полиномов Жегалкина. Однако, в классе обратимых схем теорема 4 дает границы для функции Шеннона, отличающиеся на линейное слагаемое. Вопрос о точном значении $L_{RS}(n)$ сводится к построению (последовательности) функций, имеющих в классе поляризованных полиномов сложность $\frac{1}{2}2^n + k$, где $1 < k \leq n$, либо к доказательству отсутствия таких функций.

Пока известны функции, имеющие в классе поляризованных полиномов сложность $\left\lfloor \frac{2}{3}2^n \right\rfloor$, которые подробно рассмотрены в [3], и функции сложности $\frac{1}{2}2^n + 1$, построенные в настоящей работе.

Список литературы

1. Винокуров С. Ф. Приближенный алгоритм вычисления сложности обратимой функции в базисе Тоффоли / С. Ф. Винокуров, А. С. Францева // Изв. Иркут. гос. ун-та. Сер. Математика. – 2011. – Т. 4, № 4. – С. 12–26.
2. Винокуров С. Ф. Сложность булевых функций в некоторых классах обратимых схем / С. Ф. Винокуров, А. С. Францева // Материалы XVIII междунар. школы-семинара «Синтез и сложность управляющих систем» им. акад. О. Б. Лупанова, Пенза, 28 сент. – 3 окт. 2009 г. / под ред. О. М. Касим-Заде. – М. : Изд-во механ.-мат. фак. МГУ, 2009. – С. 20–22.
3. Избранные вопросы теории булевых функций / под ред. С. Ф. Винокурова, Н. А. Перязева. – М. :ФИЗМАТЛИТ, 2001. – 192 с.
4. Toffoli T. Bicontinuous Extensions of Invetible Combinatorial Functions / T. Toffoli // Mathematical Systems Theory. – 1981. – Vol. 14. – P. 13–23.
5. Toffoli T. Reversible Computing / T. Toffoli // Automata, Languages and Programming (Series: Lecture Notes in Computer Science). – Springer Berlin Heidelberg, 1980. – Vol. 85. – P. 632–644.

Винокуров Сергей Федорович, доктор физико-математических наук, профессор, Институт математики, экономики и информатики, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1 тел.: (3952)242210 (e-mail: servin38@gmail.com)

Францева Анастасия Сергеевна, старший преподаватель, Педагогический институт, Иркутский государственный университет, 664003, Иркутск, ул. К. Маркса, 1, тел.: (3952) 240435
(e-mail: a.s.frantseva@gmail.com)

S. F. Vinokurov, A. S. Frantseva

The Complexity of the Representation of Multiple-Output Boolean Functions

Abstract. This paper considers cost of logic circuits that implement Boolean functions. The realization of Boolean functions is considered in the class of reversible logic circuits. Reversible circuits are constructed with elementary reversible circuits known as Toffoli gates or Toffoli basis. Traditional Boolean functions are not reversible except for two unary functions. However, Boolean functions can be modeled as so-called multiple-output functions for which the number of outputs is equal to the number of arguments and that are permutations on the set of arguments sets. In the paper, Boolean function is implemented as the multiple-output function that in turn is realized as a reversible circuit constructed in the Toffoli basis. The circuit implementing this function is not uniquely defined. Thus the complexity of the function can be defined as the complexity of the minimal circuit implementing this function. This paper presents results on the complexity of most complex functions and on Shannon function value for the Boolean functions in the class of reversible circuits implemented in a subset of Toffoli basis. The solution to the problem is reduced to solving the problem of finding the Shannon function value for the Boolean functions class in the class of extended Reed-Muller forms. A special sequence of functions is constructed for this class. We have proved that this sequence consists of the most complex functions and found the complexity of these functions.

Keywords: boolean function, Shannon function, complexity, Toffoli gates, reversible circuits, Reed-Muller forms.

References

1. Vinokurov S.F., Frantseva A.S. An approximate algorithm for computing the complexity of reversible functions in the basis of Toffoli (in Russian). *Izvestiya Irkutskogo gosudarstvennogo universiteta. Series "Mathematics"*, 2011, vol. 4, no 4, pp. 12-26.
2. Vinokurov S.F., Frantseva A.S. Complexity of Boolean functions in some classes of reversible circuits. *Articles XVIII International school-seminar "Synthesis and complexity of control systems"(Penza, 28 Sept. - Oct. 2009), ed. by O.M. Kasim-Zade*. M., Publishing House of the Mechanics and Mathematics Faculty of Moscow State University, 2009, pp. 20-22
3. Selected problems of the theory of Boolean functions (in Russian), ed. by Vinokurov S.F., Peryazev N.A. M., FIZMALIT, 2001. 192 p.
4. Toffoli T. Bicontinuous Extensions of Invertible Combinatorial Functions. *Mathematical Systems Theory*, 1981, vol. 14, pp. 13-23
5. Toffoli T. Reversible Computing. *Automata, Languages and Programming (Series: Lecture Notes in Computer Science)*. Springer Berlin Heidelberg, 1980, vol. 85, pp. 632-644

Vinokurov Sergey, Doctor of Sciences (Physics and Mathematics), professor, Irkutsk State University, 1, K. Marx st., Irkutsk, 664003 tel.: (3952)242210 (e-mail: servin38@gmail.com)

Frantseva Anastasiya, Senior Lecturer, Pedagogical Institute, Irkutsk State University, 1, K. Marx st., Irkutsk, 664003, tel.: (3952) 240435 (e-mail: a.s.frantseva@gmail.com)