

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 004.312, 519.7

## ВЕНТИЛЬНАЯ СЛОЖНОСТЬ ОБРАТИМЫХ СХЕМ КАК МЕРА СЛОЖНОСТИ ЧЕТНЫХ ПОДСТАНОВОК

**Д.В. Закаблук**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация  
e-mail: dmitriy.zakablukov@gmail.com

*Рассмотрен вопрос сложности четных подстановок через оценку вентиляльной сложности задающих их обратимых схем, состоящих из вентилях NOT, CNOT и 2-CNOT. Доказано, что все четные подстановки на множестве  $\mathbb{Z}_2^n$  задаются обратимой схемой, не использующей дополнительные входы, с вентиляльной сложностью, эквивалентной с точностью до порядка  $n2^n / \log_2 n$ ; оставшиеся четные подстановки задаются обратимой схемой, не использующей дополнительные входы, с меньшей вентиляльной сложностью. Установлено, что любая четная подстановка на множестве  $\mathbb{Z}_2^n$  реализуется обратимой схемой с вентиляльной сложностью  $\lesssim 2^{n+1}$  при использовании  $\sim 5 \cdot 2^n / n$  дополнительных входов. Для всех четных подстановок применение дополнительных входов позволяет снизить вентиляльную сложность реализующих их обратимых схем.*

**Ключевые слова:** обратимые схемы, вентиляльная сложность, сложность четных подстановок.

## GATE COMPLEXITY OF REVERSIBLE CIRCUITS AS A MEASURE OF EVEN PERMUTATION COMPLEXITY

**D.V. Zakablukov**

Bauman Moscow State Technical University, Moscow, Russian Federation  
e-mail: dmitriy.zakablukov@gmail.com

*The article discusses even permutation complexities via the evaluation of the gate complexity of reversible circuits consisting of NOT, CNOT and 2-CNOT gates, which implements these permutations. It is proved that almost every even permutation on the  $\mathbb{Z}_2^n$  set is implemented by the reversible circuit not using additional inputs with the gate complexity equivalent up to about  $n2^n / \log_2 n$ ; all other even permutations are implemented by reversible circuit not using additional inputs with the less gate complexity. It is established that every even permutation on the  $\mathbb{Z}_2^n$  set is implemented by the reversible circuit using  $\sim 5 \cdot 2^n / n$  additional inputs with the gate complexity  $\lesssim 2^{n+1}$ . It is stated that for almost every even permutations the usage of additional inputs allows to decrease gate complexity of reversible circuits implementing them.*

**Keywords:** reversible circuits, gate complexity, even permutation complexity.

**Введение.** В дискретной математике для оценки сложности того или иного преобразования вводится мера сложности этого преобразования. В качестве меры сложности булевой функции зачастую рассматривают вентиляльную сложность минимальной схемы, задающей эту функцию. Впервые это было предложено К. Шенноном в работе [1], с которой берет свое начало теория схемной сложности. В настоящее

время сложность булевых функций хорошо изучена: доказаны нижняя асимптотическая оценка сложности (теорема Шеннона) и верхняя асимптотическая оценка сложности (теорема Лупанова), а также их асимптотическое равенство  $2^n/n$  для булевой функции  $n$  переменных [2]. В работе [3] изучен вопрос сложности булева преобразования  $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ : доказано, что сложность такого преобразования не превышает  $O\left(\frac{n2^n}{n + \log_2 n}\right)$ ; доказательство проводится путем явного построения схемы, задающей это преобразование и состоящей из функциональных элементов NOT, AND и XOR.

В настоящей работе рассмотрен вопрос вентиляльной сложности схем, состоящих из обратимых логических вентилях NOT, CNOT и 2-CNOT. Определение обратимых вентилях NOT и  $k$ -CNOT, а также обратимых схем, включающих в себя эти вентиля, было изложено, например, в работе [4]. В работах [5, 6] было доказано следующее:

- вентиля NOT, CNOT и 2-CNOT задают четную подстановку в схеме с  $n > 3$  входами;
- множество подстановок, задаваемых вентилями NOT, CNOT и 2-CNOT с  $n$  входами, при  $n \leq 3$  генерирует симметрическую группу  $S(\mathbb{Z}_2^n)$ , а при  $n > 3$  — знакопеременную группу  $A(\mathbb{Z}_2^n)$ .

В связи с изложенным в качестве меры сложности четной подстановки предлагается рассматривать вентиляльную сложность задающей ее минимальной обратимой схемы, состоящей из вентилях NOT, CNOT и 2-CNOT.

В работах [5–13] предложены различные алгоритмы синтеза обратимых схем и в некоторых случаях дана оценка сверху вентиляльной сложности синтезированной схемы. Однако до сих пор не были известны строгие асимптотические оценки вентиляльной сложности обратимой схемы, состоящей из вентилях NOT, CNOT и 2-CNOT и задающей какую-либо четную подстановку из группы  $A(\mathbb{Z}_2^n)$ .

В настоящей работе с помощью оценки числа различных неэквивалентных обратимых схем будет доказано, что существует такая четная подстановка  $h \in A(\mathbb{Z}_2^n)$ , которая не может быть задана обратимой схемой, состоящей из вентилях NOT, CNOT и 2-CNOT и не использующей дополнительные входы с вентиляльной сложностью  $\lesssim n2^{n-1}/\log_2 n$ . Также будет доказано, что любая четная подстановка  $h \in A(\mathbb{Z}_2^n)$  может быть задана обратимой схемой, включающей в себя вентилях NOT, CNOT и 2-CNOT и не использующей дополнительные входы с вентиляльной сложностью  $\lesssim 52n2^n/\log_2 n$ . Будет показано, что любая четная подстановка  $h \in A(\mathbb{Z}_2^n)$  может быть реализована обратимой схемой, состоящей из вентилях NOT, CNOT и 2-CNOT и использующей  $\sim 5 \cdot 2^n/n$  дополнительных входов с вентиляльной сложностью  $\lesssim 2^{n+1}$ .

**Основные понятия.** Рассмотрим следующую модель обратимой схемы: все вентилях в схеме имеют одинаковое число входов, выходы

одного вентиля напрямую соединены с входами следующего за ним вентиля. В таком случае входами обратимой схемы являются входы первого вентиля, выходами – выходы последнего вентиля.

Базовое определение обратимых вентилях NOT и  $k$ -CNOT было дано в работе [4]. Напомним, что через  $N_j$  в работе [4] обозначен вентиль NOT, инвертирующий значение на  $j$ -м входе; через  $C_{i_1, \dots, i_k; j} = C_{I; j}$  – вентиль  $k$ -CNOT (обобщенный элемент Тоффли с  $k$  контролирующими входами), инвертирующий значение на  $j$ -м входе тогда и только тогда, когда значение на всех входах  $i_1, \dots, i_k$  равно 1;  $I = \{i_1, \dots, i_k\}$  – множество контролирующих входов,  $j \notin I$ .

Любая обратимая схема с  $n > 3$  входами, состоящая из вентилях NOT, CNOT и 2-CNOT, задает какую-либо четную подстановку на множестве  $\mathbb{Z}_2^n$ . При этом такая схема может *реализовывать* некоторое булево преобразование. Для того чтобы ввести определение обратимой схемы, реализующей заданное булево преобразование  $\mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ , понадобятся отображения  $\varphi_{n, n+k} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{n+k}$  и  $\psi_{n+k, n}^\pi : \mathbb{Z}_2^{n+k} \rightarrow \mathbb{Z}_2^n$  вида

$$\begin{aligned} \varphi_{n, n+k}(\langle x_1, \dots, x_n \rangle) &= \langle x_1, \dots, x_n, 0, \dots, 0 \rangle; \\ \psi_{n+k, n}^\pi(\langle x_1, \dots, x_{n+k} \rangle) &= \langle x_{\pi(1)}, \dots, x_{\pi(n)} \rangle, \pi \in S(\mathbb{Z}_{n+k}). \end{aligned}$$

Назовем  $\varphi_{n, n+k}$  *расширяющим* отображением;  $\psi_{n+k, n}^\pi$  – *редуцирующим* отображением, подстановку  $\pi$  – перестановкой выходов.

Рассмотрим произвольную четную подстановку  $h \in A(\mathbb{Z}_2^n)$ , которая задает булево преобразование  $f_h : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ . Введем определения обратимых схем, реализующих преобразование  $f_h$  либо без использования дополнительных входов, либо с использованием дополнительных входов.

**Определение 1.** Обратимая схема  $\mathfrak{S}_g$  реализует преобразование  $f_h$  без использования дополнительных входов (дополнительной памяти), если она имеет ровно  $n$  входов, при этом существует такая подстановка  $\pi \in S(\mathbb{Z}_n)$ , что задаваемое этой схемой булево преобразование  $g : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  удовлетворяет условию  $\psi_{n, n}^\pi(g(\mathbf{x})) = f_h(\mathbf{x})$ ,  $\mathbf{x} \in \mathbb{Z}_2^n$ .

**Определение 2.** Обратимая схема  $\mathfrak{S}_g$  реализует преобразование  $f_h$  с использованием  $k > 0$  дополнительных входов (дополнительной памяти), если она имеет  $n + k$  входов, при этом существует такая подстановка  $\pi \in S(\mathbb{Z}_{n+k})$ , что задаваемое этой схемой булево преобразование  $g : \mathbb{Z}_2^{n+k} \rightarrow \mathbb{Z}_2^{n+k}$  удовлетворяет условию  $\psi_{n+k, n}^\pi(g(\varphi_{n, n+k}(\mathbf{x}))) = f_h(\mathbf{x})$ ,  $\mathbf{x} \in \mathbb{Z}_2^n$ .

Отметим, что обратимая схема  $\mathfrak{S}_g$  задает преобразование  $f_h$  при  $g(\mathbf{x}) = f_h(\mathbf{x})$ .

Напомним некоторые понятия из анализа [2]. Пусть  $f(n)$  и  $g(n)$  – вещественные положительные функции натуральной переменной  $n$ , тогда:

- $f(n) \succcurlyeq g(n)$ , если для любого  $\varepsilon > 0$  найдется  $N = N(\varepsilon)$  такое, что при любом  $n \geq N$  верно неравенство  $(1 - \varepsilon)g(n) \leq f(n)$  (функция  $f(n)$  асимптотически больше или равна функции  $g(n)$ );

- $f(n) \sim g(n)$ , если  $f(n) \succcurlyeq g(n)$  и  $g(n) \succcurlyeq f(n)$  (функции  $f(n)$  и  $g(n)$  асимптотически равны, или эквивалентны), в настоящем случае  $\lim_{n \rightarrow \infty} f(n)/g(n) = 1$ ;

- $f(n) \asymp g(n)$ , если  $0 < c_1 < f(n)/g(n) < c_2$  (функции  $f(n)$  и  $g(n)$  эквивалентны с точностью до порядка).

Теперь можно перейти к оценке вентиляльной сложности обратной схемы, состоящей из вентилях NOT, CNOT и 2-CNOT, задающей четную подстановку  $h \in A(\mathbb{Z}_2^n)$ .

**Асимптотическая нижняя оценка вентиляльной сложности.** Введем множество обратимых вентилях  $\Omega_n^m$ , состоящее из всех вентилях NOT и  $k$ -CNOT,  $k \leq m$ , каждый из которых имеет ровно  $n$  входов.

Всего существует  $(n - k) \binom{n}{k}$  различных вентилях  $k$ -CNOT, имеющих ровно  $n$  входов. Нас интересует множество  $\Omega_n^2$ , состоящее из всех возможных вентилях NOT, CNOT и 2-CNOT с  $n$  входами, мощность которого равна

$$|\Omega_n^2| = \sum_{k=0}^2 (n - k) \binom{n}{k} = n + n(n - 1) + \frac{n(n - 1)(n - 2)}{2} = O(n^3). \quad (1)$$

В рассматриваемой модели обратной схемы возможна ситуация, когда перестановка двух соседних вентилях схемы порождает эквивалентную ей схему (задающую такую же четную подстановку), если эти вентиля *независимы*. Условия независимости двух вентилях  $k$ -CNOT были рассмотрены в работе [4].

В множестве  $\Omega_n^2$  все вентиля имеют не более двух контролируемых входов, поэтому при  $n \rightarrow \infty$  несколько подряд идущих вентилях могут быть попарно независимыми. Определим вероятность события, что  $k$  таких вентилях являются попарно независимыми. Примем следующее: вентиль  $C_{I;t}$  независим с каждым предшествующим ему вентилям, если не существует такого вентиля  $C_{I';t'}$ , стоящего до рассматриваемого вентиля, что  $t \in I'$  или  $t' \in I$ . Обозначим через  $P_i$  вероятность того, что эти условия выполняются для  $i$ -го вентиля в последовательности,  $P_1 = 1$ . Тогда вероятность  $P(k)$  того, что  $k$  последовательно расположенных вентилях попарно независимы составляет

$$P(k) = \prod_{i=1}^k P_i.$$

Для вентилях NOT и CNOT вероятность  $P_i$  выше, чем для вентилях 2-CNOT, так как они имеют меньше контролируемых входов. Для указанных вентилях выше вероятность выполнения второго условия

независимости, рассмотренного ранее. Поэтому без ограничения общности при расчете  $P(k)$  примем, что все вентили являются вентилями 2-CNOT.

Первый вентиль  $C_{\{j_1, l_1\}; t_1}$  можно выбрать любым возможным способом. При выборе второго вентиля  $C_{\{j_2, l_2\}; t_2}$ , независимого от первого, необходимо выбрать значения  $j_2$  и  $l_2$  так, чтобы они не совпадали со значением  $t_1$ : всего существует  $\binom{n-1}{2}$  способов выполнить это. Значение  $t_2$  не должно совпадать со значениями  $j_1, l_1, j_2, l_2$ : всего есть  $n - 4$  способов выбрать значение  $t_2$ . Аналогичные рассуждения можно провести и для третьего вентиля  $C_{\{j_3, l_3\}; t_3}$ : всего существует  $\binom{n-2}{2}$  способов выбрать значения  $j_3$  и  $l_3$  и  $n - 6$  способов — значение  $t_3$ . Отсюда следует, что вероятность  $P_k$  удовлетворяет соотношению  $P_k \geq \frac{(n-2k) \binom{n-k+1}{2}}{(n-2) \binom{n}{2}}$ , или  $P_k \geq \frac{(n-2k)(n-k+1)(n-k)}{(n-2)n(n-1)}$ . Знак “ $\geq$ ” означает, что в реальной схеме больше способов выбрать  $i$ -й вентиль так, чтобы он был независим с каждым предыдущим вентиляем. При  $k = o(n)$  и  $n \rightarrow \infty$  вероятность  $P_k \geq 1 - o(1)$ ,  $P_k \sim 1$ , тогда, и  $P(k) \sim 1$ . Следовательно, доля обратимых схем, состоящих из вентиляей множества  $\Omega_n^2$ , у которых из  $k = o(n)$  подряд идущих вентиляей найдется хотя бы два зависимых вентиля, стремится к нулю.

Докажем с помощью оценки числа различных неэквивалентных обратимых схем, что существует такая четная подстановка  $h \in A(\mathbb{Z}_n^2)$ , которая не может быть задана обратимой схемой, состоящей из вентиляей множества  $\Omega_n^2$  и не использующей дополнительные входы с вентиляльной сложностью  $\lesssim n2^{n-1}/\log_2 n$ .

Сложность минимальной обратимой схемы, состоящей из вентиляей множества  $\Omega_n^2$ , не использующей дополнительные входы и задающей четную подстановку  $h \in A(\mathbb{Z}_n^2)$ , обозначим через  $L(h)$ . Определим функцию Шеннона  $L(n) = \max_{h \in A(\mathbb{Z}_n^2)} L(h)$ . Аналогично рассмотрим величины  $L^*(h)$  и  $L^*(n)$  для обратимых схем, использующих дополнительные входы.

**Теорема 1.**  $L(n) \gtrsim n2^{n-1}/\log_2 n$ .

◀ Покажем, что имеет место неравенство  $L(h) \gtrsim n2^{n-1}/\log_2 n$  почти для всех подстановок  $h \in A(\mathbb{Z}_n^2)$ . Оценим число обратимых схем, состоящих из вентиляей множества  $\Omega_n^2$ , которые задают различные четные подстановки на множестве  $\mathbb{Z}_n^2$  и имеют вентиляльную сложность  $s$ . Обозначим эту величину через  $C^*(n, s)$ .

Если  $r = |\Omega_n^2|$ , то  $C^*(n, s) \leq r^s$ . Обозначим через  $C(n, s)$  общее число различных, неэквивалентных обратимых схем, состоящих из вентиляей множества  $\Omega_n^2$  и имеющих вентиляльную сложность не более

$$s: C(n, s) = \sum_{i=0}^s C^*(n, i) \leq \frac{r^{s+1} - 1}{r - 1}.$$

Обозначим через  $k$  число подряд идущих вентиляй в схеме. При  $k = o(n)$  и  $k = o(s)$ , можно утверждать на основании условия эквивалентности обратимых схем, что

$$C(n, s) \leq \frac{r^{s+1} - 1}{(k!)^{\lfloor s/k \rfloor} (r-1)} \leq \frac{r^{s+1} - 1}{(k!)^{(s/k)-1} (r-1)}. \quad (2)$$

Число всех четных подстановок на множестве  $\mathbb{Z}_2^n$  равно  $|A(\mathbb{Z}_2^n)| = (2^n)!/2$ . По формуле Стирлинга  $x! \gtrsim (x/e)^x$ . Оценим величину  $\log_2(C(n, s)/|A(\mathbb{Z}_2^n)|)$ :

$$\log_2 \frac{C(n, s)}{|A(\mathbb{Z}_2^n)|} \leq \log_2 \frac{2r^{s+1}}{(k!)^{(s/k)-1} (r-1) (2^n)!} \leq \log_2 \frac{2r^{s+1} e^{2^n+s-k}}{k^{s-k} (r-1) 2^{n2^n}};$$

$$\log_2 \frac{C(n, s)}{|A(\mathbb{Z}_2^n)|} \gtrsim 1 + (s+1) \log_2 r + (2^n + s - k) \log_2 e - (s-k) \log_2 k - \log_2 (r-1) - n2^n.$$

Согласно формуле (1),  $r \leq n^3$ :  $\log_2 \frac{C(n, s)}{|A(\mathbb{Z}_2^n)|} \gtrsim 3s \log_2 n + 2(2^n + s - k) - (s-k) \log_2 k - n2^n$ .

Выберем значение  $s$  так, чтобы выполнялось условие  $\log_2(C(n, s)/|A(\mathbb{Z}_2^n)|) \leq -\log_2 n$ . Пусть  $k = n/\log_2 n$ , тогда

$$\begin{aligned} & 3s \log_2 n + 2 \left( 2^n + s - \frac{n}{\log_2 n} \right) - \\ & - \left( s - \frac{n}{\log_2 n} \right) (\log_2 n - \log_2 \log_2 n) - n2^n = -\log_2 n; \\ & s(2 \log_2 n + 2 + \log_2 \log_2 n) + 2^{n+1} - \\ & - \frac{2n}{\log_2 n} + n - \frac{n \log_2 \log_2 n}{\log_2 n} - n2^n = -\log_2 n; \\ & s = \frac{n2^n + o(n2^n)}{2 \log_2 n + o(\log_2 n)}. \end{aligned}$$

Очевидно, что при таком значении  $s$  величина  $\log_2(C(n, s)/|A(\mathbb{Z}_2^n)|) \rightarrow -\infty$  при  $n \rightarrow \infty$ , т.е. доля четных подстановок, которые задаются обратимой схемой, состоящей из вентиляй множества  $\Omega_n^2$  и не использующей дополнительные входы, с вентиляльной сложностью менее  $s$ , стремится к нулю.

Следует отметить, что при указанном выборе значений  $s$  и  $k$  выполняются условия  $k = o(n)$ ,  $k = o(s)$ , таким образом, применение формулы (2) корректно. Тогда  $s \sim n2^{n-1}/\log_2 n$ , откуда следует истинность утверждения теоремы. ►

**Асимптотическая верхняя оценка вентиляльной сложности.** В работе [7] был предложен алгоритм синтеза обратимых схем, состоящих

из вентилей NOT, CNOT и 2-CNOT, основанный на теории групп подстановок. Было доказано, что вентиляционная сложность синтезированной схемы удовлетворяет соотношению

$$L(n) \lesssim 7n2^n. \quad (3)$$

Этот алгоритм основан на представлении подстановки в виде произведения пар независимых транспозиций с последующей реализацией этих пар с помощью обратимых вентилей. Если обобщить этот алгоритм для синтеза большего числа независимых транспозиций, можно получить асимптотическую верхнюю оценку сложности  $L(n)$ .

**Теорема 2.**  $L(n) \lesssim 52n2^n / \log_2 n$ .

◀ Покажем, что  $L(h) \lesssim 52n2^n / \log_2 n$  для всех  $h \in A(\mathbb{Z}_2^n)$ . Любую подстановку  $h \in A(\mathbb{Z}_2^n)$  можно представить в виде композиции непересекающихся циклов так, чтобы сумма длин этих циклов не превосходила  $2^n$ . Для композиции двух независимых циклов верно равенство

$$\begin{aligned} (i_1, i_2, \dots, i_{l_1}) \circ (j_1, j_2, \dots, j_{l_2}) &= \\ &= (i_1, i_2) \circ (j_1, j_2) \circ (i_1, i_3, \dots, i_{l_1}) \circ (j_1, j_3, \dots, j_{l_2}), \end{aligned} \quad (4)$$

а для цикла длиной  $l \geq 5$  — равенство

$$(i_1, i_2, \dots, i_l) = (i_1, i_2) \circ (i_3, i_4) \circ (i_1, i_3, i_5, i_6, \dots, i_l). \quad (5)$$

Представим подстановку  $h$  в виде композиции групп независимых транспозиций, по  $K$  транспозиций в каждой группе, и оставшейся подстановки  $h'$ :

$$h = \bigcirc_{\mathbf{x}_t, \mathbf{y}_t \in \mathbb{Z}_2^n} ((\mathbf{x}_1, \mathbf{y}_1) \circ \dots \circ (\mathbf{x}_K, \mathbf{y}_K)) \circ h'. \quad (6)$$

Для подстановки  $h'$  оценим число независимых циклов и их длину в разложении. Согласно формулам (4) и (5), в разложении  $h'$  нельзя получить  $K$  независимых транспозиций, если число независимых циклов строго меньше  $K$  и их длина строго меньше 5. Отсюда следует, что сумма длин циклов в разложении  $h'$  не превосходит  $4(K - 1)$ .

Обозначим через  $M_g$  множество подвижных точек произвольной подстановки  $g \in S(\mathbb{Z}_2^n)$ :  $M_g = \{\mathbf{x} \in \mathbb{Z}_2^n | g(\mathbf{x}) \neq \mathbf{x}\}$ . С учетом изложенного выше,  $|M_h| \leq 2^n$ ,  $|M_{h'}| \leq 4(K - 1)$ .

В соответствии с формулами (4)–(6), в декомпозиции подстановки  $h$  можно получить не более  $|M_h|/K$  групп, в каждой из которых  $K$  независимых транспозиций, а в декомпозиции подстановки  $h'$  — не более  $|M_{h'}|/2$  пар независимых транспозиций и не более одной пары зависимых транспозиций.

Пара зависимых транспозиций  $(i, j) \circ (i, k)$  выражается через произведение двух пар независимых транспозиций:  $(i, j) \circ (i, k) = ((i, j) \circ (r, s)) \circ ((r, s) \circ (i, k))$ .

С учетом изложенного оценим сверху величину  $L(h)$ :

$$L(h) \leq \frac{|M_h|}{K} L(g^{(K)}) + \frac{|M_{h'}|}{2} L(g^{(2)}) + 2L(g^{(2)}); \quad (7)$$

$$L(h) \lesssim \frac{2^n}{K} L(g^{(K)}) + 2KL(g^{(2)}),$$

где  $g^{(i)}$  — произвольная подстановка, представляющая собой произведение  $i$  независимых транспозиций.

Для произвольной подстановки  $g^{(K)}$  оценим величину  $L(g^{(K)})$ . Пусть  $k = |M_{g^{(K)}}| = 2K$ . Задание подстановки  $g^{(K)}$  вентилями множества  $\Omega_n^2$  будем проводить способом, описанным в работе [7]: действием сопряжения приведем подстановку  $g^{(K)}$  к подстановке определенного вида, которая задается простым способом. Действие сопряжением не меняет цикловой структуры подстановки, поэтому подстановка  $g^{(K)}$  в результате действия сопряжением всегда будет оставаться композицией  $K$  независимых транспозиций.

Для подстановки  $g^{(K)} = (\mathbf{x}_1, \mathbf{y}_1) \circ \dots \circ (\mathbf{x}_K, \mathbf{y}_K)$  составим матрицу  $A$ :

$$A = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{y}_1 \\ \dots \\ \mathbf{x}_K \\ \mathbf{y}_K \end{pmatrix} = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ a_{2,1} & \dots & a_{2,n} \\ \dots & \dots & \dots \\ a_{k-1,1} & \dots & a_{k-1,n} \\ a_{k,1} & \dots & a_{k,n} \end{pmatrix}. \quad (8)$$

Наложим ограничение на значение  $k$  так, чтобы оно было степенью двойки:  $k = 2^{\lfloor \log_2 k \rfloor}$ . Если  $k \leq \log_2 n$ , то в матрице  $A$  найдется не более  $2^k$  попарно различных столбцов. Без ограничения общности примем, что такими столбцами являются первые  $2^k$  столбцов. Тогда для любого  $j$ -го столбца,  $j > 2^k$ , найдется равный ему  $i$ -й столбец,  $i \leq 2^k$ . Применяя к подстановке  $g^{(K)}$  действие сопряжением подстановкой, задаваемой вентиляем  $C_{i,j}$ , можно обнулить  $j$ -й столбец матрицы  $A$  (для этого потребуется два вентиля CNOT). Повторяя указанное действие для всех столбцов с индексами больше  $2^k$ , получаем новую подстановку  $g_1^{(K)}$ , для которой матрица  $A_1$  будет иметь вид

$$A_1 = \begin{pmatrix} a_{1,1} & \dots & a_{1,2^k} & 0 & \dots & 0 \\ a_{2,1} & \dots & a_{2,2^k} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k-1,1} & \dots & a_{k-1,2^k} & 0 & \dots & 0 \\ a_{k,1} & \dots & a_{k,2^k} & 0 & \dots & 0 \end{pmatrix}.$$

$\underbrace{\hspace{10em}}_{n-2^k}$



Для получения матрицы  $A_1$  потребуется  $L_1 \leq 2n$  вентилях CNOT.

Для всех элементов  $a_{1,i} = 1$  применяем к подстановке  $g_1^{(K)}$  действие сопряжением подстановкой, задаваемой вентиляем  $N_i$ . Для этого потребуется  $L_2 \leq 2^{k+1}$  вентилях NOT. В итоге получим подстановку  $g_2^{(K)}$  и соответствующую ей матрицу  $A_2$ :

$$A_2 = \begin{pmatrix} 0 & \dots & 0 & 0 & \dots & 0 \\ b_{2,1} & \dots & b_{2,2^k} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{k-1,1} & \dots & b_{k-1,2^k} & 0 & \dots & 0 \\ b_{k,1} & \dots & b_{k,2^k} & 0 & \dots & 0 \end{pmatrix}.$$

$\underbrace{\hspace{15em}}_{n-2^k}$

Элементы матрицы  $A_2$  обозначены через  $b_{i,j}$ , чтобы показать их возможное отличие от элементов матрицы  $A_1$ .

Поставим в соответствие вектору число с помощью отображения  $\varphi_m : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_{2^m} : \varphi_m(\langle x_1, \dots, x_m \rangle) = \sum_{i=1}^m x_i 2^{i-1}$ . Будем последовательно действовать сопряжением на подстановку  $g_2^{(K)}$ , рассматривая все строки матрицы  $A_2$  начиная со второй. Пусть текущая строка имеет номер  $i$ . Эта строка попарно отличается от всех строк, чей номер меньше  $i$ , так как все строки матрицы  $A_2$  различны. Возможны два варианта.

1. Существует элемент матрицы  $b_{i,j} = 1, j > \log_2 k$ . В таком случае для всех элементов  $b_{i,j'} = 1, j' \neq j, j' > \log_2 k$ , применяем действие сопряжением подстановкой, задаваемой вентиляем  $C_{j;j'}$ . Для этого потребуется не более  $2(2^k - \log_2 k - 1)$  вентилях CNOT. Затем для всех  $j' \leq \log_2 k$  используем действие сопряжением подстановкой, задаваемой вентиляем  $C_{j;j'}$ , так, чтобы выполнялось условие

$$\varphi_{\log_2 k}(\langle b'_{i,1}, \dots, b'_{i,\log_2 k} \rangle) = i - 1. \quad (9)$$

Для этого необходимо не более  $2 \log_2 k$  вентилях CNOT. На последнем шаге применяем действие сопряжением подстановкой, задаваемой вентиляем  $C_{\{1, \dots, \log_2 k\};j}$ . Перед этим и после этого, возможно, потребуется инвертировать не более  $\log_2 k$  значений  $b'_{i,j'} = 0, j' \leq \log_2 k$ , с помощью подстановок, задаваемых вентилями NOT. Вентиль  $C_{\{1, \dots, \log_2 k\};j}$  имеет  $\log_2 k$  контролирующих входов, в результате он может быть заменен композицией не более  $8(\log_2 k - 3)$  вентилях 2-CNOT [5].

Вследствие таких преобразований получим строку матрицы, у которой все элементы с индексом больше  $\log_2 k$  являются нулевыми, а первые ее  $\log_2 k$  элементов удовлетворяют условию (9). В сумме для

этого потребуется  $L_3^{(i)}$  вентиляй множества  $\Omega_n^2$ :

$$L_3^{(i)} \leq 2(2^k - \log_2 k - 1) + 2 \log_2 k + 2(\log_2 k + 8(\log_2 k - 3) + \log_2 k);$$

$$L_3^{(i)} \leq 2^{k+1} + 20 \log_2 k.$$

2. Не существует такого элемента  $b_{i,j}$  матрицы  $A_2$ , что  $b_{i,j} = 1$ ,  $j > \log_2 k$ . Тогда можно утверждать, что для всех  $i' < i$  верно неравенство:  $\varphi_{\log_2 k}(\langle b_{i,1}, \dots, b_{i,\log_2 k} \rangle) \neq \varphi_{\log_2 k}(\langle b_{i',1}, \dots, b_{i',\log_2 k} \rangle)$ . В противном случае нашлись бы две одинаковые строки в матрице  $A_2$ , что противоречит циклическому виду подстановки  $g_2^{(K)}$ . Применяем действие сопряжением подстановкой, задаваемой вентиляем  $C_{\{1, \dots, \log_2 k\}; \log_2 k + 1}$  так, чтобы в итоге этого действия  $b_{i, \log_2 k + 1} = 1$ . Перед этим и после этого, возможно, потребуется инвертировать не более  $\log_2 k$  значений  $b_{i,j'} = 0$ ,  $j' \leq \log_2 k$ , с помощью подстановок, задаваемых вентилями NOT. Вентиль  $C_{\{1, \dots, \log_2 k\}; j}$  имеет  $\log_2 k$  контролируемых входов, таким образом, он может быть заменен композицией не более  $8(\log_2 k - 3)$  вентиляй 2-CNOT [5].

Далее выполняем те же действия, что и в предыдущем варианте. Следовательно, для приведения  $i$ -й строки к такому же виду, что и в предыдущем случае (см. п. 1), в сумме потребуется  $L_3^{(i)}$  вентиляй множества  $\Omega_n^2$ :  $L_3^{(i)} \leq 2(\log_2 k + 8(\log_2 k - 3) + \log_2 k) + 2^{k+1} + 20 \log_2 k = 2^{k+1} + 40 \log_2 k$ .

В результате последовательного применения указанных действий ко всем строкам матрицы  $A_2$  начиная со второй, будет получена новая подстановка  $g_3^{(K)}$  и соответствующая ей матрица  $A_3$ :

$$A_3 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ 1 & 1 & 1 & \dots & 1 & 0 & \dots & 0 \end{pmatrix}.$$

$\underbrace{\hspace{10em}}_{\log_2 k}$ 
 $\underbrace{\hspace{10em}}_{n - \log_2 k}$

Для этого в сумме потребуется  $L_3$  вентиляй множества  $\Omega_n^2$ :  $L_3 = \sum_{i=2}^k L_3^{(i)} \leq (k - 1)(2^{k+1} + 40 \log_2 k)$ .

Теперь для всех  $i > \log_2 k$  применяем к подстановке  $g_3^{(K)}$  действие сопряжением подстановкой, задаваемой вентиляем  $N_i$ . Для этого необходимо  $L_4 \leq 2(n - \log_2 k)$  вентиляй NOT. Получим итоговую под-

становку  $g_4^{(K)}$  и соответствующую ей матрицу  $A_4$ :

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 & \dots & 1 \end{pmatrix}.$$

$\underbrace{\hspace{15em}}_{\log_2 k}$ 
 $\underbrace{\hspace{15em}}_{n - \log_2 k}$

Матрица  $A$  была сформирована согласно формуле (8), подстановка  $g_4^{(K)}$  представляет собой композицию  $K$  независимых транспозиций, следовательно, можно утверждать: подстановка  $g_4^{(K)}$  задается вентиляем  $C_{\{n, n-1, \dots, \log_2 k + 1\}; 1}$ . Этот вентиль имеет  $n - \log_2 k$  контролируемых входов, поэтому его можно заменить композицией не более  $L_5 = 8(n - \log_2 k - 3)$  вентиляей 2-CNOT [5].

Приведенный алгоритм позволяет получить из исходной подстановки  $g^{(K)}$  подстановку  $g_4^{(K)}$  путем действия сопряжением:  $g_4^{(K)} = (g^{(K)})^{g_1 \circ g_2 \circ g_3 \circ g_4}$ , где  $g_i$  — подстановка, задаваемая описанным алгоритмом со сложностью  $L_i/2$  вентилями множества  $\Omega_n^2$ . Как было показано в работе [7], для любой подстановки  $g$ , задаваемой композицией вентиляей множества  $\Omega_n^2$ , верно равенство  $g = g^{-1}$ . Отсюда следует  $g^{(K)} = (g_4^{(K)})^{g_4^{-1} \circ g_3^{-1} \circ g_2^{-1} \circ g_1^{-1}}$ . Таким образом, можно оценить сверху величину  $L(g^{(K)})$ :

$$L(g^{(K)}) \leq \sum_{i=1}^5 L_i;$$

$$L(g^{(K)}) \leq 2n + 2^{k+1} + (k - 1)(2^{k+1} + 40 \log_2 k) + 2(n - \log_2 k) + 8(n - \log_2 k - 3).$$

Упрощая эту формулу, получаем  $L(g^{(K)}) \leq 12n + k(2^{k+1} + 40 \log_2 k) - 50 \log_2 k - 24$ . При  $K = 2$  верно неравенство  $L(g^{(2)}) \leq 12n + 324$ .

Подставляем полученные оценки в формулу (7):

$$L(h) \lesssim \frac{2^n}{k/2} (12n + k(2^{k+1} + 40 \log_2 k)) + k(12n + 324);$$

$$L(h) \lesssim 2^{n+1} \left( \frac{12n}{k} + 2^{k+1} + o(k) \right) + O(kn).$$

При  $k = o(n)$  оценку для  $L(h)$  можно упростить  $L(h) \lesssim 2^{n+1} \times \left( \frac{12n}{k} + 2^{k+1} \right)$ .

Пусть  $m = \log_2 n - \log_2 \log_2 n$ . При доказательстве требовалось, чтобы  $k$  было степенью двойки. Пусть  $k = 2^{\lfloor \log_2 m \rfloor}$ , тогда  $m/2 \leq k \leq m$  и  $L(h) \lesssim 2^{n+1} \left( \frac{12n}{m/2} + 2^{m+1} \right) = 2^{n+1} \left( \frac{24n}{\log_2 n - \log_2 \log_2 n} + \frac{2n}{\log_2 n} \right)$ . Отсюда следует, что  $L(h) \lesssim 52n2^n / \log_2 n$  для всех  $h \in A(\mathbb{Z}_2^n)$ . Таким образом,  $L(n) \lesssim 52n2^n / \log_2 n$ . ►

**Следствие 1.** При  $k = 4$  верно соотношение  $L(n) \lesssim 6n2^n$ , что асимптотически меньше, чем оценка (3), предложенная в работе [7].

Объединяя верхнюю и нижнюю оценки  $L(n)$  можно сформулировать основную теорему настоящей работы.

**Теорема 3.**  $L(n) \asymp n2^n / \log_2 n$ .

◄ Следует из теорем 1 и 2. ►

**Снижение вентиляющей сложности при использовании дополнительных входов.** В работе [3] доказано, что для любого булева преобразования  $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  можно построить реализующую его схему, состоящую из функциональных элементов базиса  $\{\neg, \wedge, \vee\}$  и имеющую вентиляющую сложность  $O(2^m/m)$ , где  $m = n + \log_2 n$ . Такая схема включает в себя в качестве подсхемы многополюсник, вычисляющий все булевы функции  $n - k$  переменных. В доказательстве использовано следующее представление преобразования  $f$  (аналог разложения булевой функции по  $k$  переменным):

$$f(\langle x_1, \dots, x_n \rangle) = \bigvee_{a_1, \dots, a_k \in \mathbb{Z}_2} x_1^{a_1} \wedge \dots \wedge x_k^{a_k} \wedge f(\langle a_1, \dots, a_k, x_{k+1}, \dots, x_n \rangle).$$

Используя аналогичный подход, докажем, что верхняя оценка вентиляющей сложности обратимых схем может быть снижена с помощью дополнительных входов. Напомним, что величина  $L^*(n)$  соответствует максимальной вентиляющей сложности обратимой схемы из всех минимальных обратимых схем, реализующих четную подстановку  $h \in A(\mathbb{Z}_2^n)$  с применением дополнительных входов.

**Теорема 4.** При  $N \sim 5 \cdot 2^n / n$  дополнительных входах в схеме, состоящей из вентилях множества  $\Omega_{n+N}^2$ , справедливо соотношение  $L^*(n) \lesssim 2^{n+1}$ .

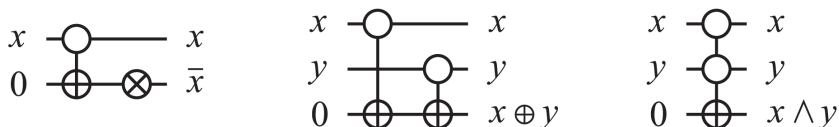
◄ Покажем, что  $L^*(h) \lesssim 2^{n+1}$  для всех  $h \in A(\mathbb{Z}_2^n)$ . Любая подстановка  $h \in A(\mathbb{Z}_2^n)$  задает некоторое булево преобразование  $f_h : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ . Представим его следующим образом:

$$f_h(\langle x_1, \dots, x_n \rangle) = \bigoplus_{a_1, \dots, a_k \in \mathbb{Z}_2} x_1^{a_1} \wedge \dots \wedge x_k^{a_k} \wedge f_h(\langle a_1, \dots, a_k, x_{k+1}, \dots, x_n \rangle). \quad (10)$$

Преобразование  $f_h(\langle a_1, \dots, a_k, x_{k+1}, \dots, x_n \rangle)$  соответствует какому-либо булеву преобразованию  $n - k$  переменных.

Построим многополюсник, вычисляющий все булевы функции  $n - k$  переменных. Обозначим через  $\Omega_{NXA}$  множество функциональных элементов  $\{\neg, \oplus, \wedge\}$  (NXA – NOT, XOR, AND). Множество

$\Omega_{\text{NXA}}$  — функционально полный базис. Известно, что для построения указанного многополюсника потребуется не более  $2^{2^{n-k}}$  элементов из множества  $\Omega_{\text{NXA}}$ . Каждый такой элемент можно выразить через композицию обратимых вентилях NOT, CNOT и 2-CNOT. Согласно рисунку, для этого необходимо не более двух обратимых вентилях и не более одного дополнительного входа. Следовательно, обратимая подсхема, задающая описанный выше многополюсник, имеет вентиляльную сложность  $L_1 \leq 2^{2^{n-k+1}}$  и использует  $N_1 = 2^{2^{n-k}} - (n - k)$  дополнительных входов. Каждый выход, соответствующий одному из дополнительных входов, представляет собой выход одной из булевых функций  $n - k$  переменных.



**Выражение функциональных элементов базиса  $\Omega_{\text{NXA}}$  через композицию обратимых вентилях NOT, CNOT и 2-CNOT**

Перед вычислением всех возможных значений конъюнкций  $x_1^{a_1} \wedge \dots \wedge x_k^{a_k}$  сперва получим с помощью обратимых вентилях все инверсии  $\bar{x}_i$ ,  $1 \leq i \leq k$ . Для этого потребуется  $L_2 = 2k$  вентилях NOT и CNOT и  $N_2 = k$  дополнительных входов. Затем вычисляем все возможные конъюнкций  $x_1^{a_1} \wedge \dots \wedge x_k^{a_k}$  по индукции: для одного входа, для двух и т.д. Для этого необходимо  $L_3 = \sum_{i=1}^{k-1} 2^{i+1} = 2^{k+1} - 4$  вентилях 2-CNOT и  $N_3 = L_3$  дополнительных входов.

Далее строим подсхему для вычисления преобразования  $f_h$ . Для каждого вектора  $\langle a_1, \dots, a_k \rangle$  потребуется  $L_4 = n$  вентилях 2-CNOT для определения конъюнкций с выходами преобразования  $f_h(\langle a_1, \dots, a_k, x_{k+1}, \dots, x_n \rangle)$ , значения для которых берутся с выходов многополюсника. Функция XOR из формулы (10) выполняется вентилям 2-CNOT, поэтому на данном этапе потребуется  $N_4 = n$  дополнительных входов. Значения на выходах, соответствующих этим дополнительным входам, являются выходами преобразования  $f_h$ .

Теперь можно оценить величину  $L^*(h)$ :  $L^*(h) \leq L_1 + L_2 + L_3 + 2^k L_4$ ;  $L^*(h) \leq 2^{2^{n-k+1}} + 2k + 2^{k+1} + n2^k = 2^{2^{n-k+1}} + 2k + 2^k(n + 2)$ . Оценим также число требуемых при данном построении дополнительных входов схемы:  $N = N_1 + N_2 + N_3 + N_4$ ;  $N = 2^{2^{n-k}} - (n - k) + k + 2^{k+1} - 4 + n = 2^{2^{n-k}} + 2k + 2^{k+1} - 4$ .

В работе [3] принято, что  $n - k = \lfloor \log_2(n - \log_2 n) \rfloor$ :

$$L^*(h) \leq \frac{2^{n+1}}{n} + 2(n - \log_2(n - \log_2 n)) + \frac{(n + 2)2^{n+1}}{n - \log_2 n} \lesssim 2^{n+1};$$

$$N = \frac{2^n}{n} + 2(n - \log_2(n - \log_2 n)) + \frac{2^{n+2}}{n - \log_2 n} - 4 \sim \frac{5 \cdot 2^n}{n}. \blacktriangleright$$

Можно сделать важный вывод о зависимости вентиляльной сложности обратимой схемы от числа дополнительных входов на основании теоремы 4.

**Утверждение 1.** Почти для всех подстановок  $h \in A(\mathbb{Z}_2^n)$  использование дополнительных входов позволяет снизить вентиляльную сложность реализующих их обратимых схем.

◀ Следует из теорем 3 и 4. ▶

**Заключение.** При решении задачи синтеза обратимой схемы, реализующей какую-либо четную подстановку, приходится искать компромисс между вентиляльной сложностью синтезированной схемы и числом используемых дополнительных входов в схеме.

В настоящей работе были доказаны некоторые асимптотические оценки вентиляльной сложности обратимых схем, состоящих из вентилях NOT, CNOT и 2-CNOT. Было установлено, что среди всех минимальных обратимых схем, не использующих дополнительные входы, максимальная вентиляльная сложность схемы эквивалентна с точностью до порядка  $n2^n / \log_2 n$ . При этом применение  $\sim 5 \cdot 2^n / n$  дополнительных входов позволяет построить обратимую схему, реализующую заданную четную подстановку с вентиляльной сложностью  $\lesssim 2^{n+1}$ .

Направлением дальнейших исследований является изучение зависимости вентиляльной сложности обратимых схем, состоящих из вентилях NOT, CNOT и 2-CNOT, от числа используемых в схеме дополнительных входов.

## ЛИТЕРАТУРА

1. Shannon C.E. The synthesis of two-terminal switching circuits // Bell System Technical Journal. 1949. Vol. 28. No. 1. С. 59–98.
2. Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986. 384 с.
3. Interlando J.C. Toward a Theory of One-way Functions via Gate Complexity of Boolean Functions // Ph. D. Thesis, University of Notre Dame, Indiana, USA, 2006. 100 p.
4. Feynman R. Quantum Mechanical Computers // Optic News. 1985. Vol. 11. No. 2. P. 11–20.
5. Maslov D.A. Reversible Logic Synthesis // Ph. D. Thesis, University of New Brunswick Fredericton, N.B., Canada, 2003. 165 p.
6. Закаблукоев Д.В. Снижение вентиляльной сложности обратимых схем без использования таблиц эквивалентных замен композиций вентилях // Наука и образование: Электрон. науч.-техн. издание. 2014. № 3. DOI: 10.7463/0314.0699195 (дата обращения: 20.04.2014).

7. Shende V.V., Prasad A.K., Markov I.L., Hayes J.P. Synthesis of Reversible Logic Circuits // *IEEE Trans. on CAD*. 2003. Vol. 22. No. 6. P. 710–722.
8. Закаблуклов Д.В., Жуков А.Е. Исследование схем из обратимых логических элементов // *Информатика и системы управления в XXI веке: Сб. трудов молодых ученых, аспирантов и студентов*. № 9. М.: МГТУ им. Н.Э. Баумана, 2012. С. 148–157.
9. Закаблуклов Д.В. Быстрый алгоритм синтеза обратимых схем на основе теории групп подстановок // *Прикладная дискретная математика*. 2014. № 2. С. 101–109.
10. Khlopotina A.B., Perkowski M.A., Kerntopf P. Reversible Logic Synthesis by Iterative Compositions // *International Workshop on Logic Synthesis*. 2002. P. 261–266.
11. Yang G., Song X., Hung W.N., Perkowski M.A. Fast Synthesis of Exact Minimal Reversible Circuits Using Group Theory // *ASP-DAC'05 Proceedings of the 2005 Asia and South Pacific Design Automation Conference*. 2005. P. 1002–1005. DOI: 10.1145/1120725.1120777 (дата обращения: 20.04.2014).
12. Miller D.M., Maslov D.A., Dueck G.W. A Transformation Based Algorithm for Reversible Logic Synthesis // *DAC'03 Proceedings of the 40th annual Design Automation Conference*. 2003. P. 318–323. DOI: 10.1145/775832.775915 (дата обращения: 20.04.2014).
13. Miller D.M. Spectral and Two-Place Decomposition Techniques in Reversible Logic // *MWSCAS'02 Proceedings of the 45th Midwest Symposium on Circuits and Systems Conference*. 2002. P. 493–496. DOI: 10.1109/MWSCAS.2002.1186906 (дата обращения: 20.04.2014).
14. Saeedi M., Sedighi M., Zamani M.S. A Novel Synthesis Algorithm for Reversible Circuits // *ICCAD'07 Proceedings of International Conference on Computer-Aided Design*. 2007. P. 65–68. DOI:10.1109/ICCAD.2007.4397245 (дата обращения: 20.04.2014).
15. Yang G., Song X., Hung W.N., Xie F., Perkowski M.A. Group Theory Based Synthesis of Binary Reversible Circuits // *TAMC'06 Proceedings of the Third international conference on Theory and Applications of Models of Computation*. 2006. P. 365–374. DOI: 10.1007/11750321\_35 (дата обращения: 20.04.2014).

## REFERENCES

- [1] Shannon C.E. The synthesis of two-terminal switching circuits. *Bell Syst. Tech. J.*, 1949, vol. 28, no. 1, pp. 59–98.
- [2] Yablonskiy S.V. *Vvedenie v diskretnuyu matematiku [Introduction to discrete mathematics]*. Moscow, Nauka Publ., 1986. 384 p.
- [3] Interlando J.C. *Toward a theory of one-way functions via gate complexity of boolean functions*. Ph. D. Dissertation, USA, Indiana, University of Notre Dame, 2006. 100 p.
- [4] Feynman R. Quantum mechanical computers. *Optics News*, 1985, vol. 11, no. 2, pp. 11–20. Available at: <http://dx.doi.org/10.1364/ON.11.2.000011> (accessed 07.05.2014).
- [5] Maslov D.A. *Reversible Logic Synthesis*. Ph. D. Dissertation, Canada, N.B., University of New Brunswick Fredericton, 2003. 165 p.
- [6] Zakabluklov D.V. Reduction of the reversible circuits gate complexity without using the equivalent replacement tables for the gate compositions. *Jelekt. Nauchno-Tehn. Izd. "Nauka i obrazovanie" MGTU im. N.E. Bauman* [El. Sc.-Tech. Publ. "Science and Education" of Bauman MSTU], 2014, no. 3. (in Russ.). DOI: 10.7463/0314.0699195
- [7] Shende V.V., Prasad A.K., Markov I.L., Hayes J.P. Synthesis of reversible logic circuits. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, 2003, vol. 22, no. 6, pp. 710–722.

- [8] Zakablukov D.V., Zhukov A.E. Research circuit from reversible logic elements. *Sb. Tr. Molodykh Uchenykh, Aspirantov i Studentov "Informatika i sistemy upravleniya v XXI veke"* [Collect. Pap. of Young Scientists, Post-graduates and Students "Informatics and Control Systems in the XXI Century"]. Moscow, MGТУ им. Н.Э. Баумана Publ., 2012, iss. 9, pp. 148–157 (in Russ.).
- [9] Zakablukov D.V. Fast algorithm for the synthesis of reversible circuits based on the theory of permutation groups. *Prikl. Diskretnaya Mat.* [J. Appl. Discrete Math.], 2014, no. 2, pp. 101–109 (in Russ.).
- [10] Khlopotine A.B., Perkowski M.A., Kerntopf P. Reversible logic synthesis by iterative compositions. *Proc. of the Int. Workshop on Logic Synthesis*, New Orleans, LA, USA, 2002, pp. 261–266.
- [11] Yang G., Song X., Hung W.N., Perkowski M.A. Fast synthesis of exact minimal reversible circuits using group theory. *Proc. of the 2005 Asia and South Pacific Design Automation Conf. – ASP-DAC'05*, China, Shanghai, 2005, pp. 1002–1005. DOI: 10.1145/1120725.1120777
- [12] Miller D.M., Maslov D.A., Dueck G.W. A transformation based algorithm for reversible logic synthesis. *Proc. of the 40th annual Design Automation Conf. – DAC'03*, Anaheim, CA, USA, 2003, pp. 318–323. DOI: 10.1145/775832.775915
- [13] Miller D.M. Spectral and two-place decomposition techniques in reversible logic. *Proc. of the 45th Midwest Symp. on Circuits and Systems Conf. – MWSCAS'02*, USA, OK, Tulsa, 2002, pp. 493–496. DOI: 10.1109/MWSCAS.2002.1186906
- [14] Saeedi M., Sedighi M., Zamani M.S. A novel synthesis algorithm for reversible circuits. *Proc. of Int. Conf. on Computer-Aided Design – ICCAD'07*, USA, CA, San Jose, 2007, pp. 65–68. DOI:10.1109/ICCAD.2007.4397245
- [15] Yang G., Song X., Hung W.N., Xie F., Perkowski M.A. Group theory based synthesis of binary reversible circuits. *Proc. of the Third Int. Conf. on Theory and Applications of Models of Computation – TAMC'06*, China, Beijing, 2006, pp. 365–374. DOI: 10.1007/11750321\_35

Статья поступила в редакцию 07.05.2014

Закаблуков Дмитрий Владимирович — аспирант кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор двух научных работ в области схем из обратимых элементов.

МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Zakablukov D.V. — post-graduate of “Information Security” department of the Bauman Moscow State Technical University. Author of two publications in the field of reversible elements.

Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.