SIZE 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 considers even permutation complexity by estimating the size of reversible circuits composed of NOT, CNOT and 2-CNOT gates implementing these permutations. It is proved that every even permutation of $\mathbb{Z}_2^n$ set can be implemented by a reversible circuit with the gate complexity equivalent up to about $n2^n/\log_2 n$ order, without the use of additional inputs; all other even permutations can be implemented by reversible circuit with less gate complexity, without the use of additional inputs. It is established that every even permutation of $\mathbb{Z}_2^n$ set can be implemented by a reversible circuit with $\lesssim 2^{n+1}$ gate complexity, using $\sim 5 \cdot 2^n/n$ additional inputs. For every even permutation usage of additional inputs allows decreasing the gate complexity of reversible circuits by implementing them.

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

Introduction. In discrete mathematics a measure of transformation complexity is introduced to estimate the complexity of this transformation. The gate complexity is often considered as the measure of Boolean function complexity, that is the minimal size of any circuit computing this function. It was first suggested by K. Shannon in work [1], which is the origin of the circuit complexity theory. Nowadays, the complexity of Boolean functions is well researched: the lower asymptotic bound (Shannon's theorem) and the upper asymptotic bound (Lupanov's theorem), as well as their asymptotic equation $2^n/n$ for the n-ary Boolean function [2] have been proved. In work [3] the problem about complexity of $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ Boolean transformations is considered: it has been proved that the complexity of this transformation does not exceed $O\left(\frac{n2^n}{n+\log_2 n}\right)$; it is proved by explicit construction of the circuit defining this transformation and composed of NOT, AND and XOR gates.

In this article the gate complexity of circuits composed of reversible gates NOT, CNOT and 2-CNOT is considered. The definition of reversible gates NOT and k-CNOT, as well as the definition of reversible circuits including these gates, are presented, for example, in the work [4]. In works [5, 6] it is proved that:

- gates NOT, CNOT and 2-CNOT define even permutation in the circuit with $n > 3$ inputs;
- the set of permutations defined by gates NOT, CNOT and 2-CNOT with n inputs, given $n \leqslant 3$ generating a symmetric group $S(\mathbb{Z}_2^n)$, but given $n > 3$ alternating-sign group $A(\mathbb{Z}_2^n)$.

In view of the aforesaid, the gate complexity of the minimal reversible circuit consisting of gates NOT, CNOT and 2-CNOT will be regarded as the measurement of complexity of even permutation.

In works [5–13] various algorithms of synthesis of reversible circuits are suggested, and in some cases upper bound of synthesized circuit is given. But until now, exact asymptotic bounds of reversible circuits, composed of gates NOT, CNOT and 2-CNOT and defining some even permutation from $A(\mathbb{Z}_2^n)$ group were unknown.

In this article it will be proved by estimating the number of nonequivalent reversible circuits, that there is an even permutation $h \in A(\mathbb{Z}_2^n)$ that cannot be defined by the reversible circuit composed of gates NOT, CNOT and 2-CNOT, without the use of additional inputs with $\lesssim n2^{n-1}/\log_2 n$ gate complexity. Also it will be proved that any even permutation $h \in A(\mathbb{Z}_2^n)$ can be defined by a reversible circuit composed of gates NOT, CNOT и 2-CNOT without the use of additional inputs with $\lesssim 52n2^n/\log_2 n$ gate complexity. It will be shown, that every even permutation $h \in A(\mathbb{Z}_2^n)$ can be implemented by reversible circuit composed of NOT, CNOT and 2-CNOT gates, using $\sim 5{\cdot}2^n/n$ additional inputs with $\lesssim 2^{n+1}$gate complexity.

Terms of reference. Let us consider the following model of a reversible circuit: all of the gates in the circuit have the same number of the inputs; outputs of one gate are directly connected to the inputs of the following gate. In this case, inputs of the first gate are inputs of the reversible circuit, outputs of the last gate are outputs of the reversible circuit.

Basic definition of the reversible gates NOT and k-CNOT was given in work [4]. Recall that NOT gate, inversing value at j^{th} input is denoted by N_j in work [4]; and the gate k-CNOT (extended Toffoly's element with k controlling inputs), inverting the value at j^{th} input then and only then, when the value is equal to 1 at all of the inputs $i_1, \ldots, i_k$ is denoted through $C_{i_1,\ldots,i_k;j} = C_{I;j}$; $i_1, \ldots, i_k$ is a set of controlling inputs, $j \notin I$.

Any reversible circuit with $n > 3$ inputs composed of gates NOT, CNOT and 2-CNOT defines some sort of even permutation at $\mathbb{Z}_2^n$ set. In this case, this circuit can *implement* some Boolean transformation. To work with definition of the reversible circuit implementing given Boolean transformation $\mathbb{Z}_2^m \to \mathbb{Z}_2^m$, the $\varphi_{n,n+k} : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n+k}$ and $\psi^{\pi}_{n+k,n} : \mathbb{Z}_2^{n+k} \to \mathbb{Z}_2^n$, images of the following type will be needed

$$\varphi_{n,n+k}(\langle x_1, \ldots, x_n\rangle) = \langle x_1, \ldots, x_n, 0, \ldots, 0\rangle;$$
$$\psi^{\pi}_{n+k,n}(\langle x_1, \ldots, x_{n+k}\rangle) = \langle x_{\pi(1)}, \ldots, x_{\pi(n)}\rangle, \pi \in S(\mathbb{Z}_{n+k}).$$

Let us denote $\varphi_{n,n+k}$ as an *extending* image; $\psi^{\pi}_{n+k,n}$ as a *reducing* image; π permutation as the output rearrangement.

Let us consider an arbitrary even permutation $h \in A(\mathbb{Z}_2^n)$ that defines $f_h : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ Boolean transformation. Let us introduce definitions of reversible circuits, implementing f_h transformation either with or without additional inputs.

Definition 1. *Reversible circuit $\mathfrak{S}_g$ implements transformation f_h without the use of extra inputs (extra memory), if it has precisely n inputs, in addition there exists such permutation $\pi \in S(\mathbb{Z}_n)$, that Boolean transformation $g : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ defined by this circuit fulfils $\psi_{n,n}^{\pi}(g(\mathbf{x})) = f_h(\mathbf{x})$, $(\mathbf{x}) \in \mathbb{Z}_2^n$ condition.*

Definition 2. *Reversible circuit $\mathfrak{S}_g$ implements transformation f_h using $k > 0$ extra inputs (extra memory) if it has $n + k$ inputs; in addition there is such permutation $\pi \in S(\mathbb{Z}_{n+k})$, that Boolean transformation $g : \mathbb{Z}_2^{n+k} \to \mathbb{Z}_2^{n+k}$ defined by this circuit fulfils $\psi_{n+k,n}^{\pi}(g(\varphi_{n,n+k}(\mathbf{x}))) = f_h(\mathbf{x})$, $(\mathbf{x}) \in \mathbb{Z}_2^n$ condition.*

Let us note that a reversible circuit $\mathfrak{S}_g$ defines transformation f_h when $g(\mathbf{x}) = f_h(\mathbf{x})$.

We recall some notions from the mathematical analysis [2]. If $f(n)$ and $g(n)$ are real-valued positive functions of natural variable *n*, then:

• $f(n) \gtrsim g(n)$, if for any $\varepsilon > 0$ there is $N = N(\varepsilon)$, then for any $n \geqslant N$ inequation $(1-\varepsilon)g(n) \leqslant f(n)$ (function $f(n)$ *asymptotically exceeds or is equal to* $g(n)$ function) is true;

• $f(n) \sim g(n)$, if $f(n) \gtrsim g(n)$ and $g(n) \gtrsim f(n)$ ($f(n)$ and $g(n)$ functions are *asymptotically equal or equivalent*), then $\lim\limits_{n\to\infty} f(n)/g(n) = 1$;

• $f(n) \asymp g(n)$ if $0 < c_1 < f(n)/g(n) < c_2$ ($f(n)$ and $g(n)$ functions *are equivalent with the order accuracy*).

Now we can proceed to the estimation of the gate complexity of a reversible circuit, composed of gates NOT, CNOT and 2-CNOT, defining even permutation $h \in A(\mathbb{Z}_2^n)$.

Asymptotic lower bound. Let us introduce a set of reversible gates named Ω_n^m, that includes all NOT and *k*-CNOT gates, $k \leqslant m$, each has exactly *n* inputs.

There are total $(n-k)\binom{k}{n}$ different *k*-CNOT gates having *n* inputs. We are interested in Ω_n^2 set that consists of all possible NOT, CNOT and 2-CNOT gates with *n* inputs. The size of this set is equal to

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

In the reversible circuit model in question this situation is possible, when rearrangement of two adjacent gates produces the equivalent circuit

(defining the same even permutation), if these gates are *independent.* Conditions of independence of two k-CNOT gates were described in work [4].

In the Ω_n^2 set all the gates have no more than two controlling inputs, therefore when $n \to \infty$ some sequential gates can be pairwise independent. Determine the probability of the case, when k of such gates are pairwise independent. Let us assume the following: $C_{I;t}$ gate is independent of every preceding gate, if there is no such $C_{I';t'}$ gate preceding to the concerned one, that $t \in I'$ or $t' \in I$. We denote by P_i the probability of the case, when these conditions are met for i^{th} gate in the sequence, $P_1 = 1$. In this case, the probability $P(k)$ when k sequential gates are pairwise independent, is $P(k) = \prod_{i=1}^{k} P_i$.

The probability P_i is higher for NOT and CNOT gates for 2-CNOT gates, because they have less controlling inputs. For these gates the probability of meeting the second condition described above is higher. Therefore, it is possible to state without loss of generality in $P(k)$ calculation, that all gates are 2-CNOT.

The first gate $C_{\{j_1,l_1\};t_1}$ can be chosen by any possible way. When choosing the next gate $C_{\{j_2,l_2\};t_2}$, independently from the first one, the values of j_2 and l_2 must not coincide with t_1: There exist $\binom{n-1}{2}$ ways to do this. The value of t_2 must not be equal to j_1, l_1, j_2, l_2: There are $n-4$ ways to choose the value of t_2. Similar reasoning can be done also for the third gate $C_{\{j_3,l_3\};t_3}$: there are $\binom{n-2}{2}$ ways to choose values of j_3 and l_3 and $n-6$ ways to choose the value of t_3 Therefore, probability P_k satisfies the $P_k \geqslant \frac{(n-2k)\binom{n-k+1}{2}}{(n-2)\binom{n}{2}}$ or $P_k \geqslant \frac{(n-2k)(n-k+1)(n-k)}{(n-2)n(n-1)}$ relation. The "$\geqslant$" sign means that in the real circuit there are more ways to choose i^{th} gate so it is independent with every preceding gate. Given $k = o(n)$ and $n \to \infty$ the probability $P_k \geqslant 1 - o(1)$, $P_k \sim 1$, then also $P(k) \sim 1$. Therefore, the proportion of reversible circuits, composed of the gates from Ω_n^2 set, with at least two dependent gates among $k = o(n)$ sequential gates, tends to zero.

Let us prove by estimating the number of different nonequivalent circuits that there is an even permutation $h \in A(\mathbb{Z}_2^n)$ that can not be defined by a reversible circuit composed of the gates from Ω_n^2 set and without the use of additional inputs with $\lesssim n2^{n-1}/\log_2 n$ gate complexity.

Let us denote the complexity of minimal reversible circuit by $L(h)$, composed of gates from Ω_n^2 set, without the use of additional inputs and defining $h \in A(\mathbb{Z}_2^n)$ even permutation. Let us define the Shannon function

$L(n) = \max\limits_{h \in A(\mathbb{Z}_2^n)} L(h)$. Let us consider $L^*(h)$ and $L^*(n)$ in the same way for reversible circuits using additional inputs.

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

◀ Now we will show that for almost all permutations $h \in A(\mathbb{Z}_2^n)$ there is an equation $L(n) \gtrsim n2^{n-1}/\log_2 n$. Let us estimate the number of reversible circuits composed of gates from Ω_n^2 set and defining various even permutations on $\mathbb{Z}_2^n$ set with s gate complexity. Let us denote this value by $C^*(n, s)$.

If $r = |\Omega_n^2|$, then $C^*(n, s) \leqslant r^s$. We denote by $C(n, s)$ the total number of all nonequivalent reversible circuits composed of gates from Ω_n^2 set and with the gate complexity not greater than s: $C(n, s) = \sum\limits_{i=0}^{s} C^*(n, i) \leqslant$ $\leqslant \dfrac{r^{s+1} - 1}{r - 1}$.

We denote by k the number of sequential gates in the circuit. Given $k = o(n)$ and $k = o(s)$, it is possible to state, based on the criterion of equivalence of the reversible circuits, that

$$C(n, s) \leqslant \frac{r^{s+1} - 1}{(k!)^{s/k}(r - 1)} \leqslant \frac{r^{s+1} - 1}{(k!)^{(s/k)-1}(r - 1)}. \qquad (2)$$

The number of all even permutations on $\mathbb{Z}_2^n$ set is equal to $|A(\mathbb{Z}_2^n)| =$ $= (2^n)!/2$. Using the Stirling formula $x! \gtrsim (x/e)^x$, we estimate the value of $\log_2(C(n, s)/|A(\mathbb{Z}_2^n)|)$:

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

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

$$-(s - k)\log_2 k - \log_2(r - 1) - n2^n.$$

According to formula (1), $r \leqslant n^3$: $\log_2 \dfrac{C(n, s)}{|A(Z_2^n)|} \gtrsim 3s\log_2 n +$ $+2(2^n + s - k) - (s - k)\log_2 k - n2^n$.

Choose the value of s, so that $\log_2(C(n, s)/|A(\mathbb{Z}_2^n)|) \leqslant -\log_2 n$. If $k = n/\log_2 n$, then:

$$3s\log_2 n + 2\left(2^n + s - \frac{n}{\log_2 n}\right) -$$

$$-\left(s - \frac{n}{\log_2 n}\right)(\log_2 n - \log_2\log_2 n) - n2^n = -\log_2 n;$$

$$s(2\log_2 n + 2 + \log_2\log_2 n) + 2^{n+1} -$$

$$-\frac{2n}{\log_2 n}+n-\frac{n\log_2\log_2 n}{\log_2 n}-n2^n=-\log_2 n;$$

$$s=\frac{n2^n+o(n2^n)}{2\log_2 n+o(\log_2 n)}.$$

It is obvious that given the value of s, $\log_2(C(n,s)/|A(\mathbb{Z}_2^n)|) \to$ $\to -\infty$ given $n \to \infty$, i.e. the part of reversible circuits composed of gates from Ω_n^2 set without the use of additional inputs, with a complexity less than s, tends to zero.

It is important that if the above described values of s and k , the conditions $k=o(n), k=o(s)$ are fulfilled, therefore the application of formula (2) is correct. Then $s \sim n2^{n-1}/\log_2 n$. That shows the validity of the theorem. ►

Asymptotic upper bound. In paper [7] the algorithm of synthesis of reversible circuits, composed of gates NOT, CNOT and 2-CNOT, based on the theory of permutation groups, was proposed. It was proved that the gate complexity of the synthesized circuit satisfies the following ratio:

$$L(n) \lesssim 7n2^n. \tag{3}$$

This algorithm is based on the representing of permutation as the production of pairs of independent transpositions followed by the implementation of these pairs using reversible gates. Generalizing this algorithm for the synthesis of the large number of independent transpositions, it is possible to obtain an asymptotic upper bound of the circuit-size complexity $L(n)$.

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

◄ Let us demonstrate that $L(h) \lesssim 52n2^n/\log_2 n$ for all values of $h \in A(\mathbb{Z}_2^n)$. Any permutation $h \in A(\mathbb{Z}_2^n)$ can be represented as a composition of disjoint cycles so that the sum of the lengths of these cycles does not exceed $2n$. For the composition of two independent cycles the following equation is true:

$$(i_1,i_2,\ldots,i_{l_1})\circ(j_1,j_2,\ldots,j_{l_2}) = \\ =(i_1,i_2)\circ(j_1,j_2)\circ(i_1,i_3,\ldots,i_{l_1})\circ(j_1,j_3,\ldots,j_{l_2}), \tag{4}$$

and for the cycle with the length $l \geqslant 5$ the following equation is true

$$(i_1,i_2,\ldots,i_l)=(i_1,i_2)\circ(i_3,i_4)\circ(i_1,i_3,i_5,i_6,\ldots,i_l). \tag{5}$$

We represent the permutation h as a composition of independent transposition groups, with K transpositions in each group, and the remaining permutation h':

$$h=\mathop{\circ}_{\mathbf{x}_t,\mathbf{y}_t\in\mathbb{Z}_2^n}((\mathbf{x}_1,\mathbf{y}_1)\circ\ldots\circ(\mathbf{x}_K,\mathbf{y}_K))\circ h'. \tag{6}$$

Now we will estimate the number of independent cycles and their length for the h' permutation. According to (4) and (5) formulae, it's impossible to obtain K independent transpositions in the h' decomposition, if the number of independent cycles is strictly less than K and their length is strictly less than 5. Therefore, the sum of the lengths of cycles in the h' decomposition does not exceed $4(K-1)$.

A set of moving points of an arbitrary permutation $g \in S(\mathbb{Z}_2^n)$: $M_g = \{\mathbf{x} \in \mathbb{Z}_2^n | g(\mathbf{x}) \neq \mathbf{x}\}$ can be denoted by M_g: given the foregoing, $|M_h| \leqslant 2^n$, $|M_{h'}| \leqslant 4(K-1)$.

According to (4)–(6) formulae, it is possible to get no more than $|M_h|/K$ groups in the decomposition of h permutation, each group having K independent transpositions, and no more than $|M_{h'}|/2$ pairs of independent transpositions in the decomposition of h' permutation and no more than one pair of dependent transpositions.

A pair of dependent transpositions $(i,j) \circ (i,k)$ can be expressed by the product of two pairs of independent transpositions: $(i,j) \circ (i,k) = = ((i,j) \circ (r,s)) \circ ((r,s) \circ (i,k))$.

Considering the above information, it is possible to estimate the upper bound of $L(h)$:

$$\begin{gathered} L(h) \leqslant \frac{|M_h|}{K} L(g^{(K)}) + \frac{|M_{h'}|}{2} L(g^{(2)}) + 2L(g^{(2)}); \\ L(h) \lesssim \frac{2^n}{K} L(g^{(K)}) + 2KL(g^{(2)}), \end{gathered} \tag{7}$$

where $g^{(i)}$ is an arbitrary permutation, representing the product of i independent transpositions.

Now we will estimate the value of $L(g^{(K)})$ for the arbitrary $g^{(K)}$permutation. Suppose $k = |M_{g^{(K)}}| = 2K$. Implementing the $g^{(K)}$ permutation with the gates from Ω_n^2 set will be carried out by the method described in work [7]: by conjugation we will reduce $g^{(K)}$ permutation to a certain permutation, defined by a simple way. The conjugation does not change the cyclic structure of the permutation, as well as the result of the conjugation, $g^{(K)}$ permutation will always remain as a composition of K independent transpositions.

For $g^{(K)} = (\mathbf{x}_1, \mathbf{y}_1) \circ \ldots \circ (\mathbf{x}_K, \mathbf{y}_K)$ permutation A matrix is as follows:

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

Let us impose restrictions on the k value, so that it can only be a power of two: $k = 2^{\log_2 k}$. If $k \leqslant \log_2 n$, there are no more than 2^k pairwise distinct columns in A matrix. Without the loss of generality, let us assume that such columns are the first 2^k columns. If so, for any j^{th} column $j > 2^k$ there is an equal i^{th} column, $i \leqslant 2^k$. Effecting on permutation $g^{(K)}$ with the permutation conjugation defined by $C_{i;j}$ gate, it is possible to zero the j^{th} column of A matrix (this requires two CNOT gates). By repeating these steps for all the columns with indexes more than 2^k, we will get a new $g_1^{(K)}$ permutation, for which the A matrix will have the form

$$A_1 = \left(\begin{array}{ccc|ccc} & & & & & \\ a_{1,1} & \dots & a_{1,2^k} & 0 & \cdots & 0 \\ a_{2,1} & \dots & a_{2,2^k} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{k-1,1} & \cdots & a_{k-1,2^k} & 0 & \dots & 0 \\ a_{k,1} & \cdots & a_{k,2^k} & 0 & \dots & 0 \\ & & & \underbrace{\qquad\qquad}_{n-2^k} & & \end{array} \right).$$

To obtain A_1 matrix, $L_1 \leqslant 2n$ CNOT gates are needed.

For all $a_{1,i} = 1$ we will effect on permutation $g_1^{(K)}$ with the permutation conjugation, defined by N_i gate. To do this, $L_2 \leqslant 2^{k+1}$ NOT gates are needed. The result is a permutation $g_2^{(K)}$ and corresponding A_2 matrix:

$$A_2 = \left(\begin{array}{ccc|ccc} & & & & & \\ 0 & \dots & 0 & 0 & \cdots & 0 \\ b_{2,1} & \cdots & b_{2,2^k} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{k-1,1} & \cdots & b_{k-1,2^k} & 0 & \cdots & 0 \\ b_{k,1} & \cdots & b_{k,2^k} & 0 & \cdots & 0 \\ & & & \underbrace{\qquad\qquad}_{n-2^k} & & \end{array} \right).$$

Elements of A_2 matrix are denoted by $b_{i,j}$ to show their distinction from elements of A_1 matrix.

Now we will find a number in correspondence with the vector by image $\varphi_m : \mathbb{Z}_2^m \to \mathbb{Z}_{2^m}$: $\varphi_m(\langle x_1, \dots, x_m \rangle) = \sum_{i=1}^{m} x_i 2^{i-1}$. We will sequentially apply a conjugation to $g_2^{(K)}$ permutation, affecting all rows of A_2 matrix, starting with the second row. Let the current row have index i. This row is pairwise different from all the rows with an index less than i, because all the rows of A_2 matrix are different. There are two options:

1. There exists $b_{i,j} = 1$, $j > \log_2 k$ matrix element. In this case, for all $b_{i,j'} = 1$, $j' \neq j$, $j' > \log_2 k$ elements, we will apply the conjugation with the permutation, defined by $C_{j;j'}$ gate. To do this, no more than $2(2^k - \log_2 k - 1)$ CNOT gates are needed. Then, for all $j' \leqslant \log_2 k$ we will apply the conjugation with the permutation, defined by $C_{j;j'}$ gate, so that

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

To do this, no more than $2\log_2 k$ CNOT gates are needed. At the last step we apply the conjugation with the permutation, defined by gate $C_{\{1,\ldots,\log_2 k\};j}$. Before and after doing this, it is possible, we will need to invert no more than $\log_2 k$ values of $b'_{i,j'} = 0$, $j' \leqslant \log_2 k$, using permutations defined by NOT gates. The gate $C_{\{1,\ldots,\log_2 k\};j}$ has $\log_2 k$ controlling inputs, and so it can be changed to a set of no more than $8(\log_2 k - 3)$ 2-CNOT gates [5].

After doing these transformations we have a row of matrix, with all elements of indices higher than $\log_2 k$, which is equal to 0, with the first $\log_2 k$ elements of this row satisfying (9) condition. To do this $L_3^{(i)}$ gates from set Ω_n^2 are needed in total:

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

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

2. There is no such an element $b_{i,j}$ of A_2 matrix, when $b_{i,j} = 1$, $j > \log_2 k$. It is possible to say, that for all $i' < i$ the following inequation is true: $\varphi_{\log_2 k}(\langle b_{i,1}, \ldots, b_{i,\log_2 k}\rangle) \neq \varphi_{\log_2 k}(\langle b_{i',1}, \ldots, b_{i',\log_2 k}\rangle)$. In the opposite case, there would be two identical rows in A_2 matrix, which does not comply with a cyclic type of $g_2^{(K)}$ permutation. We apply the conjugation with the permutation defined by $C_{\{1,\ldots,\log_2 k\};\log_2 k+1}$ gate, so that it results in $b_{i,\log_2 k+1} = 1$. Before and after doing this, we will possibly need to invert no more than $\log_2 k$ values $b_{i,j'} = 0$, $j' \leqslant \log_2 k$ using permutations defined by NOT gates. The $C_{\{1,\ldots,\log_2 k\};j}$ gate has $\log_2 k$ controlling inputs, and so it can be changed to a set of no more than $8(\log_2 k - 3)$ 2-CNOT gates[5].

After this, we perform the same operations, as in the previous case. Therefore, to reduce the i^{th} row to the same view as in previous case (see p. 1), in total $L_3^{(i)}$ gates from Ω_n^2 set are required: $L_3^{(i)} \leqslant 2(\log_2 k + \\ + 8(\log_2 k - 3) + \log_2 k) + 2^{k+1} + 20\log_2 k = 2^{k+1} + 40\log_2 k$.

As the result of all the above described operations, sequentially applied to all rows of A_2 matrix starting from the second one, a new permutation $g_3^{(K)}$ and corresponding A_3 matrix will be formed:

$$A_3 = \left(\begin{array}{ccccc|ccc} 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ 1 & 1 & 1 & \dots & 1 & 0 & \dots & 0 \\ \underbrace{\qquad\qquad\qquad\qquad\qquad}_{\log_2 k} & & & & & \underbrace{\qquad\qquad}_{n-\log_2 k} & & \end{array} \right).$$

To do this L_3 gates from Ω_n^2 set are needed in total: $L_3 = \sum_{i=2}^{k} L_3^{(i)} \leqslant$ $\leqslant (k-1)(2^{k+1} + 40\log_2 k)$.

Now we will apply the conjugation with the permutation to permutation $g_3^{(K)}$ defined by N_i gate for all $i > \log_2 k$. To do this $L_4 \leqslant 2(n - \log_2 k)$ NOT gates are required. The result is a permutation $g_4^{(K)}$ and corresponding A_4 matrix:

$$A_4 = \left(\begin{array}{ccccc|ccc} 0 & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ \underbrace{\qquad\qquad\qquad\qquad\qquad}_{\log_2 k} & & & & & \underbrace{\qquad\qquad}_{n-\log_2 k} & & \end{array} \right).$$

Matrix A was formed according to formula (8), the permutation $g_4^{(K)}$ is a composition of K independent transpositions, therefore, it can be said that $g_4^{(K)}$ permutation can be defined by $C_{\{n,n-1,\dots,\log_2 k+1\};1}$ gate. This gate has $n - \log_2 k$ controlling inputs, so it can be replaced by a composition of no more than $L_5 = 8(n - \log_2 k - 3)$ 2-CNOT gates [5].

The given algorithm allows obtaining $g_4^{(K)}$ permutation from the given $g^{(K)}$ permutation by the conjugation: $g_4^{(K)} = \left(g^{(K)}\right)^{g_1 \circ g_2 \circ g_3 \circ g_4}$, where g_i is a permutation, defined by the algorithm of $L_i/2$ complexity using gates from Ω_n^2 set. As it was shown in work [7], for any g permutation, defined by a composition of gates from Ω_n^2 set, equation $g = g^{-1}$ is true. Therefore $g^{(K)} = \left(g_4^{(K)}\right)^{g_4^{-1} \circ g_3^{-1} \circ g_2^{-1} \circ g_1^{-1}}$. So, the upper bound of $L(g^{(K)})$ can be estimated:

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

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

Reducing this formula, we will obtain $L(g^{(K)}) \leqslant 12n + k(2^{k+1} + \\ + 40\log_2 k) - 50\log_2 k - 24$. Given $K = 2$ the inequation $L(g^{(2)}) \leqslant 12n + \\ + 324$ is true.

Let us substitute calculated estimations into formula (7):

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

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

Given $k = o(n)$ the estimation of $L(h)$ can be reduced: $L(h) \lesssim 2^{n+1} \times \\ \times (\frac{12n}{k} + 2^{k+1})$.

Let $m = \log_2 n - \log_2\log_2 n$. The proof required k to be the power of two. Let $k = 2^{\log_2 m}$, then $m/2 \leqslant k \leqslant m$ and $L(h) \lesssim 2^{n+1}\Big(\frac{12n}{m/2} + \\ +2^{m+1}\Big) = 2^{n+1}\left(\frac{24n}{\log_2 n - \log_2\log_2 n} + \frac{2n}{\log_2 n}\right)$. Therefore $L(h) \lesssim \\ \lesssim 52n2^n/\log_2 n$ for all $h \in A(\mathbb{Z}_2^n)$. Hence, $L(n) \lesssim 52n2^n/\log_2 n$. ►

Corollary. Given $k = 4$ *the* $L(n) \lesssim 6n2^n$ *relation is true, which is asymptotically less than estimation* (3)*, given in work* [7].

Combining the lower and upper bounds $L(n)$ it is possible to formulate the main theorem of this work.

Theorem 3. $L\,(n) \asymp n2^n/\log_2$

◄ Results from theorems 1 and 2. ►

Reducing gate complexity, using additional inputs. In work [3] it was proved that for any Boolean transformation $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ it is possible to construct the implementing circuit composed of gates on $\{\neg, \wedge, \vee\}$ basis, with $O(2^m/m)$ gate complexity, where $m = n + \log_2 n$. Such a circuit includes a multi-terminal circuit as a sub-circuit, computing all Boolean functions of $n - k$ variables. In order to prove the following representation of f transformation was used (equivalent to Boolean function expansion for k variables):

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

Using the same approach we will prove that the upper bound of reversible circuits can be reduced by using additional inputs. Let us

recall, that the value of $L^*(n)$ corresponds to the maximum size of reversible circuit from all minimal circuits, implementing even permutation $h \in A(\mathbb{Z}_2^n)$ using additional inputs.

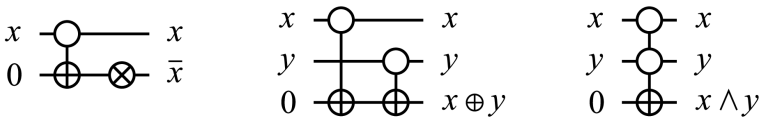
Theorem 4. *Given $N \sim 5 \cdot 2^n/n$ additional inputs in the circuit, composed of gates from Ω^2_{n+N} set, $L^*(n) \lesssim 2^{n+1}$ is true.*

◄ Let us show, that $L^*(h) \lesssim 2^{n+1}$ for all $h \in A(\mathbb{Z}_2^n)$. Any $h \in A(\mathbb{Z}_2^n)$ permutation defines some Boolean transformation $f_h : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. It will be represented in the following form:

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

The $f_h(\langle a_1, \ldots, a_k, x_{k+1}, \ldots, x_n \rangle)$ transformation corresponds to some Boolean transformation of $n - k$ variables.

Let us construct a multi-terminal circuit, calculating all Boolean functions of $n - k$ variables. We will denote by Ω_{NXA} a set of gates $\{\neg, \oplus, \wedge\}$ (NXA – NOT, XOR, AND). The Ω_{NXA} set is the functionally complete basis. It is known that no more than $2^{2^{n-k}}$ gates from Ω_{NXA} set is required to construct the multi-terminal circuit described above. All these gates can be represented as a composition of NOT, CNOT and 2-CNOT reversible gates. According to the figure below, no more than two reversible gates and no more than one additional input are required. Therefore, reversible sub-circuit defining described above multi-terminal circuit has the size of $L_1 \leqslant 2^{2^{n-k}+1}$ and it uses $N_1 = 2^{2^{n-k}} - (n - k)$ additional inputs. Every output that corresponds to one of the additional inputs is an output of the $n - k$ variable Boolean functions.



Representing functional elements from Ω_{NXA} basis as a composition of NOT, CNOT and 2-CNOT reversible gates

Before calculating all possible values of $x_1^{a_1} \wedge \ldots \wedge x_k^{a_k}$ we will calculate all $\bar{x}_i$, $1 \leqslant i \leqslant k$ inversions with reversible gates. To do this $L_2 = 2k$ NOT and CNOT gates and $N_2 = k$ additional inputs are needed. Then we calculate all possible values of $x_1^{a_1} \wedge \ldots \wedge x_k^{a_k}$ by induction: for one input, for two etc. To do this $L_3 = \sum_{i=1}^{k-1} 2^{i+1} = 2^{k+1} - 4$ 2-CNOT gates and $N_3 = L_3$ additional inputs are needed.

Then we construct a sub-circuit to calculate f_h transform. For each vector $\langle a_1, \ldots, a_k \rangle$ $L_4 = n$ 2-CNOT gates are needed to define a conjunction

with $f_h(\langle a_1, \ldots, a_k, x_{k+1}, \ldots, x_n\rangle)$ transformation outputs, where values are to be taken from the outputs of multi-terminal circuit. XOR gate from formula (10) is implemented by 2-CNOT gate, so at this stage $N_4 = n$ additional inputs are needed. The values of the outputs that correspond to these additional inputs are outputs of f_h transform.

Now it is possible to estimate $L^*(h)$ value: $L^*(h) \leqslant L_1 + L_2 + L_3 + 2^k L_4$; $L^*(h) \leqslant 2^{2^{n-k}+1} + 2k + 2^{k+1} + n2^k = 2^{2^{n-k}+1} + 2k + 2^k(n+2)$. Also we estimate a number of the required additional inputs: $N = N_1 + N_2 + N_3 + N_4$; $N = 2^{2^{n-k}} - (n-k) + k + 2^{k+1} - 4 + n = 2^{2^{n-k}} + 2k + 2^{k+1} - 4$.

In work [3] it was stated, that: $n - k = \log_2(n - \log_2 n)$

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

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

The conclusion can be drawn about dependency of circuit-size complexity on the number of additional inputs, relying on theorem 4.

Statement 1. *For almost all permutations $h \in A(\mathbb{Z}_2^n)$ usage of additional inputs allows reducing their circuit-size complexity.*

◄ Based on theorems 3 and 4. ►

Conclusion. When synthesizing a reversible circuit, implementing some even permutation, it is necessary to find a compromise between circuit-size complexity and number of additional inputs in the circuit.

In this paper several asymptotic bounds of reversible circuits composed of NOT, CNOT and 2-CNOT gates have been proved. It was stated that among all minimal reversible circuits without the usage of additional inputs maximal circuit-size complexity is equivalent to the accuracy up to an order of $n2^n/\log_2 n$. At the same time $\sim 5 \cdot 2^n/n$ additional inputs allow to construct a reversible circuit, implementing the given even permutation with $\lesssim 2^{n+1}$ circuit-size complexity.

Further investigations focuse on the dependency of the reversible circuits compexity composed of NOT, CNOT and 2-CNOT gates from the number of additional inputs being used in the scheme.

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] Zakablukov D.V. Reduction of the reversible circuits gate complexity without using the equivalent replacement tables for the gate compositions. *Jelektr. Nauchno-Tehn. Izd. "Nauka i obrazovanie" MGTU im. N.E. Baumana* [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, MGTU im. N.E. Baumana 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

The original manuscript was received by the editors of "Vestnik" on 07.05.2014

Contributor

Zakablukov D.V. – Ph.D. student, Department of Information Security, Bauman Moscow State Technical University. Author of two publications in the field of reversible elements. Bauman Moscow State Technical University, ul. 2-ya Baumanskaya 5, Moscow, 105005 Russian Federation.

The translation of this article from Russian into English is done by E.S. Sitchikhin, a student, Bauman Moscow State Technical University under the general editorship of I.R. Shafikova, a senior lecturer, Linguistics Department, Bauman Moscow State Technical University.