НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА

НАУКА и ОБРАЗОВАНИЕ

Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408

электронный научно-технический журнал

Снижение вентильной сложности обратимых схем без использования таблиц эквивалентных замен композиций вентилей

 # 03, март 2014

DOI: 10.7463/0314.0699195

Закаблуков Д. В.

УДК 004.312, 530.145

Россия, МГТУ им. Н.Э. Баумана

dmitriy.zakablukov@gmail.com

Введение

Обратимость вычислений может потребоваться в совершенно различных областях науки и техники, таких как квантовые вычисления и нанотехнологии. Данное требование зачастую обусловлено необходимостью максимально снизить величину тепловых потерь. Обратимость вычислений является необходимым условием нулевого уровня тепловых потерь, т. к. потеря информации во время вычислительного процесса приводит к рассеянию энергии, что было доказано в работе [1]. В работе [5] показывается, что величина тепловых потерь, вызванных необратимостью вычислений, в будущем может стать весьма существенной и составлять порядка 10^6 Вт для устройства, состоящего из 10^{17} логических вентилей и работающего при комнатной температуре на частоте 10 ГГц (при условии потери 1 бита информации в каждом из логических вентилей на каждом такте работы устройства). Как следствие, схемы из обратимых вентилей могут найти широкое применение в устройствах, работающих в условиях ограниченных вычислительных ресурсов, в том числе и в устройствах защиты информации.

Если алгоритм защиты можно описать обратимым преобразованием и его можно реализовать в обратимой схеме, то в таком случае в одной и той же схеме за счет обратимости реализуется прямой алгоритм и обратный к нему, поэтому можно говорить об оценке сверху для вентильной сложности реализации этих алгоритмов.

Обратимые вентили изучались во многих работах: к примеру, в работе [2] Фейнманом изучаются вентили инверсии NOT и управляемой инверсии CNOT (1-CNOT); в работе [3] изучается элемент Тоффоли (2-CNOT). В работах [4] и [5] доказывается, во-первых, что вентили NOT, 1-CNOT и 2-CNOT задают четные подстановки на множестве $\mathbb{Z}_2^n$ в схемах

с четырьмя и более входами, и во-вторых, что множество подстановок, задаваемых всеми возможными вентилями NOT, 1-CNOT и 2-CNOT в схеме с $n > 3$ входами, генерирует знакопеременную группу A_{2^n}. Другими словами, любую четную подстановку $h \in A_{2^n}$ при $n > 3$ можно реализовать обратимой схемой, состоящей из вентилей NOT, 1-CNOT и 2-CNOT. Алгоритмы синтеза обратимых схем рассматриваются в работах [4, 6, 8, 9, 10, 11, 12, 13]. В работах [6, 9, 13] показывается, что задачу синтеза обратимой схемы, реализующей заданную четную подстановку, можно свести к задаче декомпозиции этой подстановки в композицию транспозиций определенного вида. В работе [7] рассматриваются вопросы эквивалентных замен композиций вентилей, позволяющих привести обратимую схему к определенному виду без изменения результирующего преобразования схемы в целом.

Перед любым алгоритмом синтеза обратимых схем может встать задача снизить по возможности вентильную сложность синтезированной схемы. В большинстве случаев эта задача решается при помощи поиска в схеме композиции вентилей определенного вида и замены ее на эквивалентную композицию вентилей меньшей сложности из заранее сформированной таблицы замен. Такой подход применяется, к примеру, в алгоритмах синтеза, предложенных в работах [7] и [10]. Недостатком такого способа решения задачи снижения вентильной сложности является необходимость построения и хранения больших таблиц замен, а также долгое время поиска замены по таблице. Также стоит отметить неуниверсальность данного подхода в том смысле, что заменяемая композиция вентилей должна строго соответствовать композиции вентилей из таблицы.

В данной работе предлагается способ решения задачи снижения вентильной сложности обратимых схем без использования таблиц замен, основанный на использовании обобщенного представления вентиля k-CNOT для случая нулевого значения на некоторых контролирующих входах.

1. Базовые понятия

Логический вентиль $n \times m$ — устройство с n входами и m выходами, дающее на выходах результат булевого преобразования $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ над входами. *Обратимый вентиль* $n \times n$ (далее просто обратимый вентиль) — логический вентиль $n \times n$, для которого реализуемое им булево преобразование является биекцией. Далее по тексту n обозначает количество входов и выходов обратимого вентиля, если не оговорено иначе. В данной статье среди всех обратимых вентилей будут рассматриваться только вентили NOT и k-CNOT:

1) N_j — вентиль NOT, инвертирующий свой j-й вход:

$$f_{\text{NOT}}\big(\langle x_1,\ \ldots,\ x_j,\ \ldots,\ x_n\rangle\big) = \langle x_1,\ \ldots,\ x_j \oplus 1,\ \ldots,\ x_n\rangle;$$

2) $C_{i_1,\ldots,i_k;j}$ — вентиль k-CNOT (инвертор с k контролирующими входами), инвертирующий свой j-й вход тогда и только тогда, когда значение на всех входах $i_1, \ldots, i_k$ равно 1:

$$f_{k\text{-CNOT}}\big(\langle x_1,\ \ldots,\ x_j,\ \ldots,\ x_n\rangle\big) = \langle x_1,\ \ldots,\ x_j \oplus x_{i_1} \wedge \ldots \wedge x_{i_k},\ \ldots,\ x_n\rangle.$$

Правильно сформированная *обратимая схема* — ациклическая комбинационная логическая схема, в которой все вентили обратимы и соединены друг с другом последовательно без ветвлений. *Вентильная сложность* схемы — количество вентилей в ней.

В данной статье рассматриваются только те обратимые схемы, в которых все вентили имеют одинаковое количество входов, при этом выходы одного вентиля напрямую соединяются со входами следующего за ним вентиля. В этом случае входами обратимой схемы являются входы первого вентиля в композиции, выходами — выходы последнего вентиля в композиции. Соединение вентилей (операцию композиции вентилей) будем обозначать $*$. Пример обратимой схемы при $n \geq 4$: $C_{4;1} * C_{2,3;4} * N_4$.

2. Обобщенное представление вентиля k-CNOT

Классический вентиль k-CNOT $C_{i_1,\ldots,i_k;j}$ инвертирует значение на контролируемом входе, когда значение на всех контролирующих входах равно 1. В данной работе предлагается обобщить представление вентиля k-CNOT для случая нулевого значения на некоторых контролирующих входах.

Определение 1. $C_{I;J;t}$ — вентиль k-CNOT, реализующий булево преобразование вида:

$$f_{k\text{-CNOT}}\big(\langle x_1,\ \ldots,\ x_t,\ \ldots,\ x_n\rangle\big) = \Big\langle x_1,\ \ldots,\ x_t \oplus \Big(\bigwedge_{i\in I} x_i\Big) \wedge \Big(\bigwedge_{j\in J} \bar{x}_j\Big),\ \ldots,\ x_n\Big\rangle,$$

где I — множество прямых контролирующих входов; J — множество инвертированных контролирующих входов; $t \notin I \cup J$; $I \cap J = \varnothing$; $|I| + |J| = k$.

Для удобства примем следующие обозначения: $E(t)$ — вентиль N_t; $E(t, I)$ — вентиль $C_{I;t}$; $E(t, I, J)$ — вентиль $C_{I;J;t}$. Тогда можно считать, что $E(t, I) = E(t, I, \varnothing)$, $E(t) = E(t, \varnothing, \varnothing)$. Также вектор $\langle x_1,\ \ldots,\ x_n\rangle$ входных значений вентиля будем обозначать $\mathbf{x}$.

Вентиль $E(t, I, J)$ инвертирует значение на контролируемом входе только тогда, когда значение на всех прямых контролирующих входах равно 1 и значение на всех инвертированных контролирующих входах равно 0. Графически прямые контролирующие входы будем обозначать белым кружочком, инвертированные — серым кружочком, контролируемый вход — кружочком со знаком «+» внутри; вентиль NOT — кружочком со знаком «×» внутри (рис. 1).

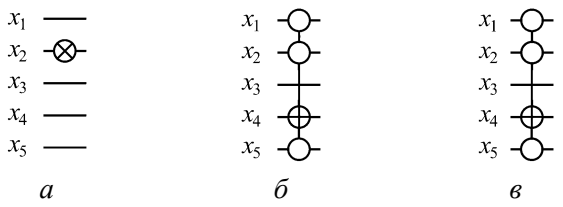


Рис. 1. Графическое обозначение обратимых вентилей ($n = 5$):
а — $E(2)$; *б* — $E(4, \{1, 2, 5\})$; *в* — $E(4, \{1\}, \{2, 5\})$

Вентили $E(t, I, J)$ могут найти применение в алгоритмах синтеза, основанных на теории групп подстановок, предложенных в работах [6] и [13]. Любой вентиль $E(t, I, J)$ можно представить в виде композиции классических вентилей NOT и k-CNOT (рис. 2).

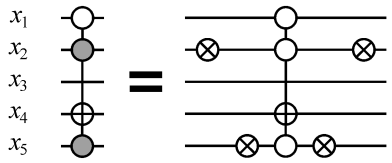


Рис. 2. Представление вентиля $E(4, \{1\}, \{2, 5\})$ в виде композиции вентилей $E(2)$, $E(5)$ и $E(4, \{1, 2, 5\})$ $(n = 5)$

В общем случае вентиль $E(t, I, J)$ можно заменить без изменения результирующего преобразования на композицию вентилей $\left(\underset{t\in J}{*} E(t)\right) * E\big(t, I \cup J\big) * \left(\underset{t\in J}{*} E(t)\right)$.

3. Независимые обратимые вентили

При решении задачи снижения вентильной сложности обратимой схемы часто необходимо выяснить, можно ли два подряд идущих вентиля поменять местами без изменения преобразования, реализуемого схемой.

Определение 2. Обратимые вентили E_1 и E_2 являются *независимыми*, если их композицию $E_1 * E_2$ можно заменить на композицию $E_2 * E_1$ без изменения результирующего преобразования. Иначе вентили E_1 и E_2 являются *зависимыми*.

В работе [7] были рассмотрены условия независимости для классических вентилей k-CNOT. Рассмотрим, при каких условиях являются независимыми вентили $E(t, I, J)$.

Утверждение 1. Вентили $E(t_1, I_1, J_1)$ и $E(t_2, I_2, J_2)$ являются независимыми, если:

1) $t_1 = t_2$;

2) $t_1 \notin I_2 \cup J_2$ и $t_2 \notin I_1 \cup J_1$;

3) $I_1 \cap J_2 \neq \varnothing$ или $I_2 \cap J_1 \neq \varnothing$.

Доказательство. Для каждого случая рассмотрим функции $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$, соответствующую композиции $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$, и $g(\mathbf{x}) = f_1(f_2(\mathbf{x}))$, соответствующую композиции $E(t_2, I_2, J_2) * E(t_1, I_1, J_1)$, где $\mathbf{x}$ — входной вектор значений.

Вентили $E(t_1, I_1, J_1)$ и $E(t_2, I_2, J_2)$ будут независимыми, если $f(\mathbf{x}) = g(\mathbf{x})$.

1. Обозначим $t = t_1 = t_2$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t$; $y_t = x_t \oplus \left(\underset{j\in I_1}{\wedge} x_j\right) \wedge \left(\underset{j\in J_1}{\wedge} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t$.

$z_t = y_t \oplus \left(\underset{j\in I_2}{\wedge} x_j\right) \wedge \left(\underset{j\in J_2}{\wedge} \bar{x}_j\right) = x_t \oplus \left(\underset{j\in I_1}{\wedge} x_j\right) \wedge \left(\underset{j\in J_1}{\wedge} \bar{x}_j\right) \oplus \left(\underset{j\in I_2}{\wedge} x_j\right) \wedge \left(\underset{j\in J_2}{\wedge} \bar{x}_j\right)$.

$f_2(\mathbf{x}) = \mathbf{y}'$; $y'_i = x_i$ при $i \neq t$; $y'_t = x_t \oplus \left(\underset{j\in I_2}{\wedge} x_j\right) \wedge \left(\underset{j\in J_2}{\wedge} \bar{x}_j\right)$.

$g(\mathbf{x}) = f_1(\mathbf{y}') = \mathbf{z}'$; $z'_i = y'_i = x_i$ при $i \neq t$.

$z'_t = y'_t \oplus \left(\underset{j\in I_1}{\wedge} x_j\right) \wedge \left(\underset{j\in J_1}{\wedge} \bar{x}_j\right) = x_t \oplus \left(\underset{j\in I_2}{\wedge} x_j\right) \wedge \left(\underset{j\in J_2}{\wedge} \bar{x}_j\right) \oplus \left(\underset{j\in I_1}{\wedge} x_j\right) \wedge \left(\underset{j\in J_1}{\wedge} \bar{x}_j\right)$.

$\mathbf{z} = \mathbf{z}' \Rightarrow f(\mathbf{x}) = g(\mathbf{x})$.

2. $f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t_1$; $y_{t_1} = x_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t_1, t_2$; $z_{t_1} = y_{t_1} = x_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$z_{t_2} = y_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right) = x_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$f_2(\mathbf{x}) = \mathbf{y}'$; $y'_i = x_i$ при $i \neq t_2$; $y'_{t_2} = x_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}') = \mathbf{z}'$; $z'_i = y'_i = x_i$ при $i \neq t_1, t_2$; $z'_{t_2} = y_{t_2} = x_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$z'_{t_1} = y_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right) = x_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$\mathbf{z} = \mathbf{z}' \Rightarrow f(\mathbf{x}) = g(\mathbf{x})$.

3. Пусть $I_1 \cap J_2 \neq \varnothing$, тогда $\exists k \in I_1 \cap J_2$, $f_1(\mathbf{x}) = \mathbf{x}$ при $x_k = 0$, $f_2(\mathbf{x}) = \mathbf{x}$ при $x_k = 1$.

Рассмотрим случай $x_k = 0$:

$f(\mathbf{x}) = f_2(f_1(\mathbf{x})) = f_2(\mathbf{x})$.

$g(\mathbf{x}) = f_1(f_2(\mathbf{x})) = f_1(\mathbf{y})$.

$k \in I_1 \cap J_2 \Rightarrow y_k = x_k = 0 \Rightarrow g(\mathbf{x}) = f_1(\mathbf{y}) = \mathbf{y} = f_2(\mathbf{x}) \Rightarrow f(\mathbf{x}) = g(\mathbf{y})$.

Рассмотрим случай $x_k = 1$:

$f(\mathbf{x}) = f_2(f_1(\mathbf{x})) = f_2(\mathbf{y})$.

$k \in I_1 \cap J_2 \Rightarrow y_k = x_k = 1 \Rightarrow f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{y} = f_1(\mathbf{x})$.

$g(\mathbf{x}) = f_1(f_2(\mathbf{x})) = f_1(\mathbf{x}) \Rightarrow f(\mathbf{x}) = g(\mathbf{y})$.

Таким образом, для всех значений x_k $f(\mathbf{x}) = g(\mathbf{y})$. Аналогично доказывается для случая $I_2 \cap J_1 \neq \varnothing$. Утверждение доказано.

Примеры независимых вентилей показаны на рис. 3.

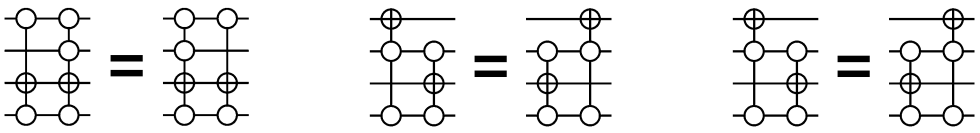


Рис. 3. Три случая независимых вентилей

4. Эквивалентные замены композиций вентилей

В работе [7] было предложено несколько эквивалентных замен одной композиции вентилей $E(t, I)$ на другую. В некоторых случаях такая замена уменьшает вентильную сложность схемы, а в некоторых случаях уменьшает количество контролирующих входов у вентилей. Далее будут приведены эквивалентные замены композиций вентилей $E(t, I, J)$. Стоит отметить, что словосочетание «композиция вентилей может быть заменена» означает, что результат замены не меняет результирующего преобразования исходной композиции вентилей.

Замена 1. Композиция вентилей $E(t, I, J) * E(t, I, J)$ может быть исключена из схемы.

Доказательство тривиально и следует из определения функции, задаваемой вентилем $E(t, I, J)$. По сути, замена 1 — исключение дублирующих вентилей из схемы.

Замена 2 (*слияние*)**.** Если $I_1 = I_2 \cup \{k\}$, $J_2 = J_1 \cup \{k\}$, $k \notin I_2 \cup J_1$, то композиция вентилей $E(t, I_1, J_1) * E(t, I_2, J_2)$ может быть заменена одним вентилем $E(t, I_2, J_1)$.

Доказательство. Пусть $f_1(\mathbf{x})$ задается вентилем $E(t, I_1, J_1)$, $f_2(\mathbf{x})$ — вентилем $E(t, I_2, J_2)$. Рассмотрим функцию $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t$; $y_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$I_1 = I_2 \cup \{k\}, k \notin I_2 \Rightarrow y_t = x_t \oplus x_k \wedge \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t$; $z_t = y_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$J_2 = J_1 \cup \{k\}, k \notin J_1 \Rightarrow z_t = y_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \bar{x}_k \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$z_t = x_t \oplus x_k \wedge \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right) \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \bar{x}_k \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$z_t = x_t \oplus (x_k \oplus \bar{x}_k) \wedge \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right) = x_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

Функция $f(\mathbf{x}) = \mathbf{z}$ задается вентилем $E(t, I_2, J_1)$.

Замена 3 (*уменьшение количества контролирующих входов*)**.** Если существуют такие индексы p и q, что $p \in I_1 \cap J_2$, $q \in J_1 \cap I_2$, $I_2 = I_1 \setminus \{p\} \cup \{q\}$, $J_2 = J_1 \setminus \{q\} \cup \{p\}$, то композиция вентилей $E(t, I_1, J_1) * E(t, I_2, J_2)$ может быть заменена композицией вентилей $E(t, I_1, J_3) * E(t, I_2, J_3)$, где $J_3 = J_1 \setminus \{q\} = J_2 \setminus \{p\}$.

Доказательство. Пусть $f_1(\mathbf{x})$ задается вентилем $E(t, I_1, J_1)$, $f_2(\mathbf{x})$ — вентилем $E(t, I_2, J_2)$. Рассмотрим функцию $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t$; $y_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$q \in J_1 \Rightarrow y_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge (1 \oplus x_q) \wedge \left(\bigwedge\limits_{j \in J_1 \setminus \{q\}} \bar{x}_j\right)$.

$q \notin I_1 \Rightarrow y_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j \oplus \bigwedge\limits_{j \in I_1 \cup \{q\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t$; $z_t = y_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$p \in J_2 \Rightarrow z_t = y_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge (1 \oplus x_p) \wedge \left(\bigwedge\limits_{j \in J_2 \setminus \{p\}} \bar{x}_j\right)$.

$p \notin I_2 \Rightarrow z_t = y_t \oplus \left(\bigwedge\limits_{j \in I_2} x_j \oplus \bigwedge\limits_{j \in I_2 \cup \{p\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

$z_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j \oplus \bigwedge\limits_{j \in I_1 \cup \{q\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right) \oplus \left(\bigwedge\limits_{j \in I_2} x_j \oplus \bigwedge\limits_{j \in I_2 \cup \{p\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

$z_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j \oplus \bigwedge\limits_{j \in I_1 \cup \{q\}} x_j \oplus \bigwedge\limits_{j \in I_2} x_j \oplus \bigwedge\limits_{j \in I_2 \cup \{p\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

$I_2 = I_1 \setminus \{p\} \cup \{q\}, p \in I_1 \Rightarrow I_2 \cup \{p\} = I_1 \cup \{q\} \Rightarrow z_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j \oplus \bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

$z_t = x_t \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right) \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_3} \bar{x}_j\right)$.

Функция $f(\mathbf{x}) = \mathbf{z}$ задается композицией вентилей $E(t, I_1, J_3) * E(t, I_2, J_3)$.

Замена 4 (*перестановка зависимых вентилей*)**.** Если $t_1 \in I_2 \cup J_2$, $t_2 \notin I_1 \cup J_1$, то композиция зависимых вентилей $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ может быть заменена композицией $E(t_2, I_1 \cup I_2 \setminus \{t_1\}, J_1 \cup J_2 \setminus \{t_1\}) * E(t_2, I_2, J_2) * E(t_1, I_1, J_1)$.

Доказательство. $(I_1 \cup I_2) \cap (J_1 \cup J_2) = (I_1 \cap J_1) \cup (I_2 \cap J_1) \cup (I_1 \cap J_2) \cup (I_2 \cap J_2) =$ $= (I_2 \cap J_1) \cup (I_1 \cap J_2) = \varnothing$, так как в противном случае вентили $E(t_1, I_1, J_1)$ и $E(t_2, I_2, J_2)$ будут независимыми. Следовательно, вентиль $E(t_2, I_1 \cup I_2 \setminus \{t_1\}, J_1 \cup J_2 \setminus \{t_1\})$ не нарушает требований, накладываемых на множества прямых и инвертированных контролирующих входов (см. определение 1).

Пусть $f_1(\mathbf{x})$ задается вентилем $E(t_1, I_1, J_1)$, $f_2(\mathbf{x})$ — вентилем $E(t_2, I_2, J_2)$, $f_3(\mathbf{x})$ — вентилем $E(t_2, I_1 \cup I_2 \setminus \{t_1\}, J_1 \cup J_2 \setminus \{t_1\})$. Рассмотрим две функции: $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$ и $g(\mathbf{x}) = f_1(f_2(f_3(\mathbf{x})))$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t_1$; $y_{t_1} = x_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t_2$; $z_{t_2} = y_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} y_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{y}_j\right)$.

Пусть $t_1 \in I_2$, тогда $z_{t_2} = x_{t_2} \oplus y_{t_1} \wedge \left(\bigwedge\limits_{j \in I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$$z_{t_2} = x_{t_2} \oplus \left(x_{t_1} \oplus \left(\bigwedge_{j \in I_1} x_j\right) \wedge \left(\bigwedge_{j \in J_1} \bar{x}_j\right)\right) \wedge \left(\bigwedge_{j \in I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_1 \cup I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2} \bar{x}_j\right).$$

$$t_1 \notin J_2 \Rightarrow z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_1 \cup I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

Если же $t_1 \in J_2$, то $z_{t_2} = x_{t_2} \oplus \bar{y}_{t_1} \wedge \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right)$.

$$z_{t_2} = x_{t_2} \oplus \left((1 \oplus x_{t_1}) \oplus \left(\bigwedge_{j \in I_1} x_j\right) \wedge \left(\bigwedge_{j \in J_1} \bar{x}_j\right)\right) \wedge \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_1 \cup I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

$$t_1 \notin I_2 \Rightarrow z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_1 \cup I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

Таким образом, во всех случаях:

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_1 \cup I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

$f_2(f_3(\mathbf{x})) = \mathbf{y}'$; $y'_i = x_i$ при $i \neq t_2$.

$$y'_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_1 \cup I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_1 \cup J_2 \setminus \{t_1\}} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right).$$

$g(\mathbf{x}) = f_1(\mathbf{y}') = \mathbf{z}'$; $z'_i = y'_i$ при $i \neq t_1$; $z'_{t_1} = y'_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} y'_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{y'}_j\right)$.

$t_2 \notin I_1 \cup J_1 \Rightarrow z'_{t_1} = x_{t_1} \oplus \left(\bigwedge\limits_{j \in I_1} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_1} \bar{x}_j\right)$.

$\mathbf{z}' = \mathbf{z} \Rightarrow f(\mathbf{x}) = g(\mathbf{x}) \Rightarrow$ замена 4 не меняет результирующего преобразования исходной композиции вентилей.

Замена 5 (*следствие замены 4*)**.** Если в условии замены 4 $I_1 \subseteq I_2$ и $J_1 \subseteq J_2$, то композиция зависимых вентилей $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ может быть заменена композицией вентилей $E(t_2, I_2 \cup \{t_1\}, J_2 \setminus \{t_1\}) * E(t_1, I_1, J_1)$, если $t_1 \in J_2$, и композицией вентилей $E(t_2, I_2 \setminus \{t_1\}, J_2 \cup \{t_1\}) * E(t_1, I_1, J_1)$, если $t_1 \in I_2$.

Д о к а з а т е л ь с т в о. Согласно условию замены 4, композиция вентилей $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ может быть заменена композицией $E(t_2, I_1 \cup I_2 \setminus \{t_1\}, J_1 \cup J_2 \setminus \{t_1\}) * E(t_2, I_2, J_2) * E(t_1, I_1, J_1)$.

$I_1 \subseteq I_2, J_1 \subseteq J_2 \Rightarrow E(t_2, I_1 \cup I_2 \setminus \{t_1\}, J_1 \cup J_2 \setminus \{t_1\}) = E(t_2, I_2 \setminus \{t_1\}, J_2 \setminus \{t_1\})$.

Пусть $t_1 \in J_2$, тогда $E(t_2, I_2 \setminus \{t_1\}, J_2 \setminus \{t_1\}) = E(t_2, I_2, J_2 \setminus \{t_1\})$. Рассмотрим функцию $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$, задаваемую композицией $E(t_2, I_2, J_2 \setminus \{t_1\}) * E(t_2, I_2, J_2)$, где $f_1(\mathbf{x})$ задается вентилем $E(t_2, I_2, J_2 \setminus \{t_1\})$, а $f_2(\mathbf{x})$ — вентилем $E(t_2, I_2, J_2)$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t_2$; $y_{t_2} = x_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t_2$; $z_{t_2} = y_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\left(\bigwedge_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right) \oplus \bar{x}_{t_1} \wedge \left(\bigwedge_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right)\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2 \cup \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_2 \setminus \{t_1\}} \bar{x}_j\right).$$

Таким образом, при $t_1 \in J_2$ функция $f(\mathbf{x})$ задается вентилем $E(t_2, I_2 \cup \{t_1\}, J_2 \setminus \{t_1\})$.

Пусть $t_1 \in I_2$, тогда $E(t_2, I_2 \setminus \{t_1\}, J_2 \setminus \{t_1\}) = E(t_2, I_2 \setminus \{t_1\}, J_2)$. Рассмотрим функцию $g(\mathbf{x}) = g_2(g_1(\mathbf{x}))$, задаваемую композицией $E(t_2, I_2 \setminus \{t_1\}, J_2) * E(t_2, I_2, J_2)$, где $g_1(\mathbf{x})$ задается вентилем $E(t_2, I_2 \setminus \{t_1\}, J_2)$, а $g_2(\mathbf{x})$ — вентилем $E(t_2, I_2, J_2)$.

$g_1(\mathbf{x}) = \mathbf{y}'$; $y'_i = x_i$ при $i \neq t_2$; $y'_{t_2} = x_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$g(\mathbf{x}) = g_2(\mathbf{y}') = \mathbf{z}'$; $z'_i = y'_i = x_i$ при $i \neq t_2$; $z'_{t_2} = y'_{t_2} \oplus \left(\bigwedge\limits_{j \in I_2} x_j\right) \wedge \left(\bigwedge\limits_{j \in J_2} \bar{x}_j\right)$.

$$z'_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \oplus \left(\bigwedge_{j \in I_2} x_j\right) \wedge \left(\bigwedge_{j \in J_2} \bar{x}_j\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in J_2} \bar{x}_j\right) \wedge \left(\left(\bigwedge_{j \in I_2 \setminus \{t_1\}} x_j\right) \oplus x_{t_1} \wedge \left(\bigwedge_{j \in I_2 \setminus \{t_1\}} x_j\right)\right).$$

$$z_{t_2} = x_{t_2} \oplus \left(\bigwedge_{j \in I_2 \setminus \{t_1\}} x_j\right) \wedge \left(\bigwedge_{j \in J_2 \cup \{t_1\}} \bar{x}_j\right).$$

Таким образом, при $t_1 \in I_2$ функция $g(\mathbf{x})$ задается вентилем $E(t_2, I_2 \setminus \{t_1\}, J_2 \cup \{t_1\})$.

Замена 6 (*зеркальное отображение замены 4*)**.** Если $t_2 \in I_1 \cup J_1$, $t_1 \notin I_2 \cup J_2$, то композиция зависимых вентилей $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ может быть заменена композицией вентилей $E(t_2, I_2, J_2) * E(t_1, I_1, J_1) * E(t_1, I_1 \cup I_2 \setminus \{t_2\}, J_1 \cup J_2 \setminus \{t_2\})$.

Доказательство этой замены аналогично доказательству для замены 4.

Замена 7 (*следствие замены 6*)**.** Если в условии замены 6 $I_2 \subseteq I_1$ и $J_2 \subseteq J_1$, то композиция зависимых вентилей $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ может быть заменена композицией вентилей $E(t_2, I_2, J_2) * E(t_1, I_1 \cup \{t_2\}, J_1 \setminus \{t_2\})$, если $t_2 \in J_1$, и композицией вентилей $E(t_2, I_2, J_2) * E(t_1, I_1 \setminus \{t_2\}, J_1 \cup \{t_2\})$, если $t_2 \in I_1$.

Доказательство аналогично доказательству для замены 5.

Замена 8. Вентиль $E(t, I, J)$ можно заменить на композицию вентилей:

$$\left(\underset{t \in J}{*} E(t)\right) * E(t, I \cup J) * \left(\underset{t \in J}{*} E(t)\right).$$

Доказательство следует из рис. 2 и определения вентиля $E(t, I, J)$.

Замена 9. Если $k \in J$, то вентиль $E(t, I, J)$ можно заменить на композицию вентилей $E(t, I \cup \{k\}, J \setminus \{k\}) * E(t, I, J \setminus \{k\})$.

Доказательство. Пусть $f_1(\mathbf{x})$ задается вентилем $E(t, I \cup \{k\}, J \setminus \{k\})$, $f_2(\mathbf{x})$ — вентилем $E(t, I, J \setminus \{k\})$. Рассмотрим функцию $f(\mathbf{x}) = f_2(f_1(\mathbf{x}))$.

$f_1(\mathbf{x}) = \mathbf{y}$; $y_i = x_i$ при $i \neq t$; $y_t = x_t \oplus \left(\bigwedge\limits_{j \in I \cup \{k\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right)$.

$f(\mathbf{x}) = f_2(\mathbf{y}) = \mathbf{z}$; $z_i = y_i = x_i$ при $i \neq t$; $z_t = y_t \oplus \left(\bigwedge\limits_{j \in I} x_j\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right)$.

$z_t = x_t \oplus \left(\bigwedge\limits_{j \in I \cup \{k\}} x_j\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right) \oplus \left(\bigwedge\limits_{j \in I} x_j\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right)$.

$z_t = x_t \oplus \left(\bigwedge\limits_{j \in I \cup \{k\}} x_j \oplus \bigwedge\limits_{j \in I} x_j\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right)$.

$k \notin I \Rightarrow z_t = x_t \oplus \left((1 \oplus x_k) \wedge \left(\bigwedge\limits_{j \in I} x_j\right)\right) \wedge \left(\bigwedge\limits_{j \in J \setminus \{k\}} \bar{x}_j\right) = x_t \oplus \left(\bigwedge\limits_{j \in I} x_j\right) \wedge \left(\bigwedge\limits_{j \in J} \bar{x}_j\right)$.

Функция $f(\mathbf{x}) = \mathbf{z}$ задается вентилем $E(t, I, J)$.

Стоит также отметить, что вентиль k-CNOT, $k < n - 1$, может быть заменен композицией не более чем $8(n - 5)$ вентилей 2-CNOT без использования дополнительных входов в схеме [4].

Примеры эквивалентных замен показаны на рис. 4.

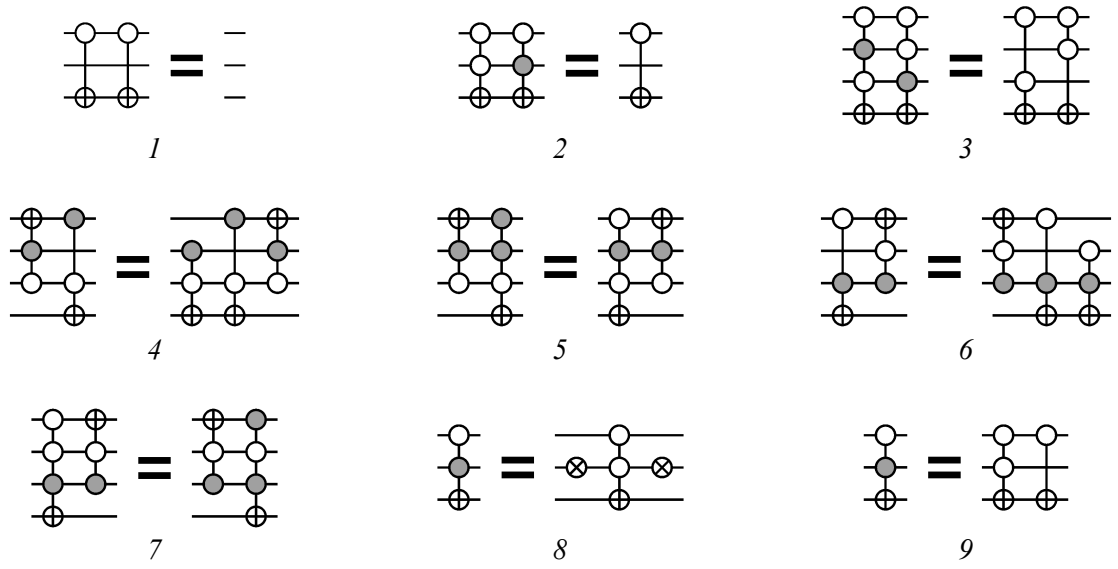


Рис. 4. Примеры эквивалентных замен композиций вентилей

Можно выделить еще два частных случая замены «слиянием».

Замена 10 (*обратная к замене 9*)**.** Если $I_1 = I_2 \cup \{k\}$, то композиция вентилей $E(t, I_1, J) * E(t, I_2, J)$ может быть заменена одним вентилем $E(t, I_2, J \cup \{k\})$.

Замена 11. Если $J_1 = J_2 \cup \{k\}$, то композиция вентилей $E(t, I, J_1) * E(t, I, J_2)$ может быть заменена одним вентилем $E(t, I \cup \{k\}, J_2)$.

Доказательство корректности замен 10 и 11 вытекает из доказательства корректности замен 1 и 9. Примеры замен 10 и 11 показаны на рис. 5.

10 *11*

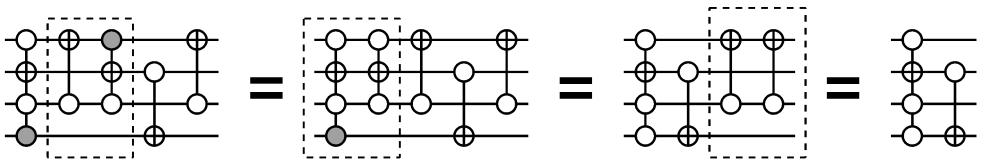
Рис. 5. Частные случаи замены композиций вентилей «слиянием»

5. Снижение вентильной сложности

Предложенные эквивалентные замены композиций вентилей позволяют в некоторых случаях снизить вентильную сложность обратимой схемы. В основном для этого используется замена, исключающая дублирующие вентили (1), и замены слиянием (2, 10 и 11). Замены 3–7 позволяют получить новую обратимую схему с новыми вентилями, для которой можно снова попробовать использовать замены 1, 2, 10 и 11. В случае, когда вентильную сложность уже невозможно снизить, то можно использовать замены 8 и 9, чтобы заменить все вентили $E(t, I, J)$ на классические вентили NOT и k-CNOT и получить обратимую схему, не содержащую вентилей $E(t, I, J)$.

Пусть обратимая схема представляет собой композицию вентилей $\overset{l}{\underset{i=1}{*}} E_i$, где l — вентильная сложность схемы. Если композиция вентилей $E_i * E_j$ удовлетворяют условию какой-либо замены, $i < j$, и при этом существует такой индекс s, $i \leqslant s < j$, что вентили E_i и E_k являются независимыми для всех $i < k \leqslant s$, и вентили E_j и E_k являются независимыми для всех $s < k < j$, то вентили E_i и E_j можно исключить из схемы, а результат замены композиции $E_i * E_j$ вставить в схему между вентилями E_s и E_{s+1}.

На рис. 6 в качестве примера показан процесс применения эквивалентных замен композиций вентилей для некоторой абстрактной схемы.



1 *2* *3* *4*

Рис. 6. Процесс снижения вентильной сложности схемы: *1* — исходная схема; *2* — схема после применения замены 5; *3* — схема после применения замены 11; *4* — схема после применения замены 1

Заключение

Предложенные в данной статье эквивалентные замены композиций обратимых вентилей позволяют решать задачу снижения вентильной сложности обратимой схемы без применения таблиц замен. Использование обобщенных вентилей $E(t, I, J)$ позволяет существенно расширить набор замен, по сравнению с набором замен, предложенным в работе [7]. Достоинством описанного способа решения задачи снижения вентильной сложности обратимой

схемы является отсутствие необходимости в предварительном построении и последующем использовании таблиц замен, что может существенно сократить время работы алгоритма снижения вентильной сложности схемы и требуемый этим алгоритмом объем памяти. Также стоит отметить, что предложенный подход применим для обратимых схем с любым количеством входов и содержащих вентили k-CNOT с любым количеством контролирующих входов, в отличие от подхода, использующего таблицы замен.

Направлением дальнейших исследований является изучение временной сложности алгоритма снижения вентильной сложности обратимой схемы, использующего предложенные замены. Планируется проведение экспериментов по снижению вентильной сложности известных на данный момент обратимых схем, состоящих из вентилей NOT и k-CNOT.

Список литературы

1. Bennett C.H. Logical Reversibility of Computation // IBM Journal of Research and Development. 1973. Vol. 17, no. 6. P. 525–532. DOI: 10.1147/rd.176.0525
2. Feynman R.P. Quantum Mechanical Computers // Foundations of Physics. 1986. Vol. 16, no. 6. P. 507–531. DOI: 10.1007/BF01886518
3. Toffoli T. Reversible Computing // In book: Automata, Languages and Programming. Springer Berlin Heidelberg, 1980. P. 632–644. DOI: 10.1007/3-540-10003-2_104 (Ser. Lecture Notes in Computer Science; vol. 85).
4. Shende V.V., Prasad A.K., Markov I.L., Hayes J.P. Synthesis of Reversible Logic Circuits // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2006. Vol. 22, no. 6. P. 710–722. DOI: 10.1109/TCAD.2003.811448
5. Закаблуков 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. Вып. 9. М.: МГТУ им. Н.Э. Баумана, 2012. С. 148–157.
6. Закаблуков Д.В. Синтез схем из обратимых элементов // XX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы», МИФИ (Москва, 01–06 февраля 2013 г.): тез. докл. М.: МИФИ, 2013. С. 100–101.
7. Iwama K., Kambayashi Y., Yamashita S. Transformation Rules for Designing CNOT-based Quantum Circuits // Proceedings of the 39th annual Design Automation Conference (DAC'02). 2002. P. 419–424. DOI: 10.1145/513918.514026
8. Khlopotine A.B., Perkowski M.A., Kerntopf P. Reversible Logic Synthesis by Iterative Compositions // Proc. of the International Workshop on Logic Synthesis. 2002. P. 261–266.
9. Yang G., Song X., Hung W.N., Perkowski M.A. Fast Synthesis of Exact Minimal Reversible Circuits Using Group Theory // Proceedings of the 2005 Asia and South

Pacific Design Automation Conference (ASP-DAC'05). 2005. P. 1002–1005. DOI: 10.1145/1120725.1120777

10. Miller D.M., Maslov D., Dueck G.W. A Transformation Based Algorithm for Reversible Logic Synthesis // Proceedings of the 40th annual Design Automation Conference (DAC'03). 2003. P. 318–323. DOI: 10.1145/775832.775915
11. Miller D.M. Spectral and Two-Place Decomposition Techniques in Reversible Logic // Proceedings of the 45th Midwest Symposium on Circuits and Systems Conference (MWSCAS'02). 2002. P. 493–496. DOI: 10.1109/MWSCAS.2002.1186906
12. Saeedi M., Sedighi M., Zamani M.S. A Novel Synthesis Algorithm for Reversible Circuits // Proceedings of International Conference on Computer-Aided Design (ICCAD'07). 2007. P. 65–68. DOI: 10.1109/ICCAD.2007.4397245
13. Yang G., Song X., Hung W.N., Xie F., Perkowski M.A. Group Theory Based Synthesis of Binary Reversible Circuits // Proceedings of the Third international conference on Theory and Applications of Models of Computation (TAMC'06). 2006. P. 365–374. DOI: 10.1007/11750321_35

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

EL № FS77 - 48211. №0421200025. ISSN 1994-0408

electronic scientific and technical journal

Reduction of the reversible circuits gate complexity without using the equivalent replacement tables for the gate compositions

 # 03, March 2014

DOI: 10.7463/0314.0699195

Zakablukov D. V.

Bauman Moscow State Technical University
105005, Moscow, Russian Federation
dmitriy.zakablukov@gmail.com

The subject of study of this paper is reversible logic circuits. The irreversibility of computation can lead in the future to significant energy loss during the calculation process. Reversible circuits can be widely used in devices operating under conditions of limited computational resources.

Presently, the problem of reversible logic synthesis is widely studied. The task a synthesis algorithm can face with is to reduce the gate complexity of synthesized circuit. One way to solve this problem is to use equivalent replacement tables for the gate compositions. The disadvantage of this approach is that it is necessary to build replacement tables, it takes a long time to find the replacement in the table, and there is no way to build an appropriate universal replacement table for arbitrary reversible circuit. The aim of this paper is to develop the solution for the problem of gate complexity reduction for the reversible circuits without using equivalent replacement tables for the gate compositions.

This paper makes a generalization of the k-CNOT gate for the case of zero value at some of the gate control inputs. To describe such gates it suggests using a set of direct control inputs and a set of inverted ones. A definition of the independence of two reversible gates is introduced. Two independent gates standing next to each other in the circuit can be swapped without changing the circuit result transformation. Various conditions of the independence of two reversible gates are considered including conditions imposed to the set of direct control inputs and the set of inverted ones. It is proved that two gates are independent if there is, at least, one common control input, which differs only by the type (direct or inverted).

Various equivalent replacements of two k-CNOT gates compositions and its conditions imposed to the set of direct control inputs and to the set of inverted ones are considered. The proof of correctness for such replacements is provided by comparing result transformations of the gate compositions before and after replacement. Operations on the set of direct control inputs and on

the set of inverted ones are widely used in the proof. The paper shows that two identical gates being nearby in the circuit can be excluded from it. It also shows that sometimes a composition of two gates can be replaced with the one gate, if the gates differ from each other by only one control input. The part of the equivalent replacements suggests in the paper does not reduce the gate complexity, but allows the new reversible gates to be available. In some cases after applying such replacements a new pair of gates can be found to satisfy the condition of another replacement reducing the gate complexity. The set of equivalent replacements proposed in this paper is significantly expanded comparing to the sets of equivalent replacements described in other papers.

The paper describes the algorithm to reduce the reversible circuit gate complexity using the conditions of the gates independence and the proposed equivalent replacements of gate compositions. The algorithm is based on searching the pair of gates, which satisfy a condition of some replacement and which can be moved to each other without changing the circuit resultant transformation (conditions of gates independence proposed in this paper are checked). An example of using this algorithm in some abstract reversible circuit is offered.

The advantage of the proposed approach is that it does not require replacement tables to be built, and the gate complexity can be reduced for the arbitrary circuit consisted of k-CNOT gates. Further, an assessment of the time complexity of the proposed algorithm of the gate complexity reduction is supposed to be given.

Publications with keywords: reversible logic, equivalent replacement, complexity reduction
Publications with words: reversible logic, equivalent replacement, complexity reduction

References

1. Bennett C.H. Logical Reversibility of Computation. *IBM Journal of Research and Development*, 1973, vol. 17, no. 6, pp. 525–532. DOI: 10.1147/rd.176.0525
2. Feynman R.P. Quantum Mechanical Computers. *Foundations of Physics*, 1986, vol. 16, no. 6, pp. 507–531. DOI: 10.1007/BF01886518
3. Toffoli T. Reversible Computing. In book: *Automata, Languages and Programming*. Springer Berlin Heidelberg, 1980, pp. 632–644. DOI: 10.1007/3-540-10003-2_104 (Ser. *Lecture Notes in Computer Science*; vol. 85).
4. Shende V.V., Prasad A.K., Markov I.L., Hayes J.P. Synthesis of Reversible Logic Circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2006, vol. 22, no. 6, pp. 710–722. DOI: 10.1109/TCAD.2003.811448
5. Zakablukov D.V., Zhukov A.E. [Study of reversible logic elements schemes]. *Informatika i sistemy upravleniya v 21 veke: sb. trudov molodykh uchenykh, aspirantov i studentov* [Informatics and control systems in the 21st century: collection of papers of young scientists, postgraduates and students]. Iss. 9. Moscow, Bauman MSTU Publ., 2012, pp. 148–157. (in Russian).

6. Zakablukov D.V. [Synthesis of schemes of invertible elements]. 20 Vserossiyskaya nauchno-prakticheskaya konferentsiya “Problemy informatsionnoy bezopasnosti v sisteme vysshey shkoly”: tez. dokl. [Abstracts of 20 International Scientific and Practical Conference “Problems of Information Security in the Higher School”], MIFI, Moscow, 1–6 February 2013. Moscow, MIFI Publ., 2013, pp. 100–101. (in Russian).
7. Iwama K., Kambayashi Y., Yamashita S. Transformation Rules for Designing CNOT-based Quantum Circuits. *Proceedings of the 39th annual Design Automation Conference (DAC’02)*, 2002, pp. 419–424. DOI: 10.1145/513918.514026
8. Khlopotine A.B., Perkowski M.A., Kerntopf P. Reversible Logic Synthesis by Iterative Compositions. *Proc. of the International Workshop on Logic Synthesis*, 2002, pp. 261–266.
9. Yang G., Song X., Hung W.N., Perkowski M.A. Fast Synthesis of Exact Minimal Reversible Circuits Using Group Theory. *Proceedings of the 2005 Asia and South Pacific Design Automation Conference (ASP-DAC’05)*, 2005, pp. 1002–1005.
10. Miller D.M., Maslov D., Dueck G.W. A Transformation Based Algorithm for Reversible Logic Synthesis. *Proceedings of the 40th annual Design Automation Conference (DAC’03)*, 2003, pp. 318–323. DOI: 10.1145/775832.775915
11. Miller D.M. Spectral and Two-Place Decomposition Techniques in Reversible Logic. *Proceedings of the 45th Midwest Symposium on Circuits and Systems Conference (MWSCAS’02)*, 2002, pp. 493–496. DOI: 10.1109/MWSCAS.2002.1186906
12. Saeedi M., Sedighi M., Zamani M.S. A Novel Synthesis Algorithm for Reversible Circuits. *Proceedings of International Conference on Computer-Aided Design (ICCAD’07)*, 2007, pp. 65–68. DOI: 10.1109/ICCAD.2007.4397245
13. Yang G., Song X., Hung W.N., Xie F., Perkowski M.A. Group Theory Based Synthesis of Binary Reversible Circuits. *Proceedings of the Third international conference on Theory and Applications of Models of Computation (TAMC’06)*, 2006, pp. 365–374. DOI: 10.1007/11750321_35