На правах рукописи

Закаблуков Дмитрий Владимирович

МЕТОДЫ СИНТЕЗА ОБРАТИМЫХ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ NOT, CNOT И 2-CNOT

Специальность 01.01.09 — дискретная математика
и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2018

Работа выполнена на кафедре «Информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный технический университет имени Н. Э. Баумана» (МГТУ им. Н. Э. Баумана).

Научный руководитель: **Жуков Алексей Евгеньевич**, кандидат физико-математических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н. Э. Баумана

Официальные оппоненты: **Ложкин Сергей Андреевич**, доктор физико-математических наук, профессор кафедры математической кибернетики МГУ им. М. В. Ломоносова

Вялый Михаил Николаевич, кандидат физико-математических наук, старший научный сотрудник ФИЦ ИУ РАН

Ведущая организация: ФГБУН Институт системного программирования Российской академии наук

Защита диссертации состоится «___»_____ 2018 года в _____ на заседании диссертационного совета Д 002.073.05 при Федеральном государственном учреждении «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» по адресу: 119333, г. Москва, ул. Вавилова, д. 40.

С диссертацией можно ознакомиться в библиотеке Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» и на сайте `http://frccsc.ru`.

Автореферат разослан «___»_____ 2018 года.

Учёный секретарь
диссертационного совета Д 002.073.05
доктор физико-математических наук,
профессор Рязанов В. В.

Общая характеристика работы

Актуальность темы.

При проектировании цифровых микросхем всё чаще во главу угла ставится требование компактности микросхемы и её низкого энергопотребления. При разработке мобильных систем ограниченное энергопотребление становится уже критически важным.

Известно, что необратимость вычислений приводит к выделению тепловой энергии. Сформулированный Р. Ландауэром в 1961 году фундаментальный физический принцип гласит: в любой вычислительной системе, независимо от её физической реализации, при потере 1 бита информации выделяется минимум $kT \ln 2$ Дж тепла, где k — постоянная Больцмана, T — абсолютная температура, при которой происходят вычисления[1]. В 2012 году был проведён эксперимент с коллоидной частицей, подтвердивший данный принцип[2].

Некоторые разрабатываемые технологии теоретически могут позволить достичь плотности размещения логических устройств в 10^{17} элементов на кубический сантиметр[3]. Согласно принципу Р. Ландауэра, если все производимые вычисления будут необратимы, такое количество вычислительных устройств при комнатной температуре во время работы на частоте в 10 ГГц должно выделять более $3 \cdot 10^6$ Вт. Отвод такого количества тепловой энергии представляет собой неразрешимую технологическую проблему. Ч. Беннет показал[4], что нулевой уровень тепловых потерь возможен только тогда (необходимое, но не достаточное условие), когда все логические устройства схемы являются обратимыми, другими словами, когда они реализуют биективное отображение.

С другой стороны, обратимые схемы являются неотъемлемой частью квантовых вычислений, позволяющих решать некоторые экспоненциально сложные проблемы за полиномиальное время[5,6]. Также обратимые логические устройства могут быть получены при помощи КМОП технологий (адиабатической и термодинамической), оптических технологий, нанотехнологий и технологий с использованием молекул ДНК.

---

[1] Landauer R. «*Irreversibility and Heat Generation in the Computing Process*» // IBM Journal of Research and Development, 1961.Vol. 5(3). Pp. 183-191.

[2] Bérut A., Arakelyan A., Petrosyan A., Ciliberto S., Dillenschneider R., Lutz E. «*Experimental Verification of Landauer's Principle Linking Information and Thermodynamics*» // Nature, 2012. Vol. 483. Pp. -187-189.

[3] Merkle R. C., Drexler K. E. «*Helical Logic*» // Nanotechnology, 1996. Vol. 7. Pp. 325–339.

[4] Bennett C. H. «*Logical reversibility of computation*» // IBM Journal of Research and Development, 1973. Vol. 17(6). Pp. 525–532.

[5] Shor P. W. «*Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*» // SIAM Journal on Computing, 1997. Vol. 26(5). Pp. 1484–1509.

[6] Hallgren S. «*Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem*» // Journal of the ACM, 2007. Vol. 54(1). Pp. 4:1–4:19.

С математической точки зрения только биективные отображения не приводят к потере информации. Большинство функциональных элементов не являются обратимыми (к примеру, конъюнктор и дизъюнктор). В то же время обратимыми являются такие функциональные элементы, как инвертор (NOT); элемент Фейнмана, именуемый также контролируемой инверсией (Controlled NOT, CNOT); элемент Тоффоли, именуемый также контролируемой контролируемой инверсией (Controlled Controlled NOT, CCNOT или 2-CNOT); элемент Фредкина и ряд других.

Было доказано[7], что с помощью элементов NOT, CNOT и 2-CNOT можно реализовать любую чётную подстановку на множестве $\mathbb{Z}_2^n$ в обратимой схеме ровно с n входами, а если при этом использовать один дополнительный вход, то можно реализовать любую подстановку на множестве $\mathbb{Z}_2^n$. Таким образом, в качестве меры сложности подстановки на множестве $\mathbb{Z}_2^n$ можно рассматривать сложность реализующей её обратимой схемы. Задача же синтеза обратимой схемы может свестись к поиску минимального представления элемента (подстановки) в системе образующих (множество подстановок, задаваемых обратимыми функциональными элементами) соответствующей группы подстановок.

В последнее время было предложено множество различных алгоритмов синтеза обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Часть из них является переборными алгоритмами, другие используют для синтеза либо теорию групп подстановок, либо изменение таблицы истинности для входного булева преобразования. Однако для случая, когда заданная чётная подстановка на множестве $\mathbb{Z}_2^n$ имеет малое количество подвижных точек, не было предложено эффективных методов синтеза реализующей её обратимой схемы.

Открытым вопросом на текущий момент также является поиск эффективных алгоритмов снижения сложности обратимой схемы. В большинстве случаев существующие алгоритмы используют заранее построенные таблицы эквивалентных замен композиций функциональных элементов. Данные таблицы обычно строятся для фиксированного значения числа входов обратимой схемы и могут требовать значительного объёма памяти для своего хранения.

Ещё одним открытым вопросом является изучение зависимости сложности синтезируемой обратимой схемы от количества используемых дополнительных входов в общем случае. Исторически сложилось, что почти все существующие работы по синтезу обратимых схем ставят перед собой цель получить обратимую схему без дополнительных входов. Однако известен

[7] Shende V. V., Prasad A. K., Markov I. L. and Hayes J. P. «*Synthesis of Reversible Logic Circuits*» // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2003. Vol. 22(6). Pp. 710–722.

эффект снижения сложности и глубины обратимых схем за счет использования дополнительных входов[8,9].

Теория схемной сложности берёт своё начало с работы К. Шеннона[10], в которой он предложил в качестве меры сложности булевой функции рассматривать сложность минимальной контактной схемы, реализующей эту функцию. Асимптотически оптимальный метод синтеза схем в базисе функциональных элементов, соответствующих всем двуместным булевым функциям, был разработан О. Б. Лупановым[11]. Им также была установлена асимптотика функции Шеннона для сложности реализации булевых функций во всех основных классах схем, в том числе и для схем с ограничением на количество соединений для одного функционального элемента.

Вопрос о вычислениях с ограниченной памятью (ограниченным числом ячеек памяти) рассматривался Н. А. Карповой[12]. Ею было доказано, что в базисе классических функциональных элементов, реализующих все p-местные булевы функции, асимптотическая оценка функции Шеннона сложности схемы с тремя и более регистрами памяти зависит от значения p, но не изменяется при увеличении количества используемых регистров памяти.

О. Б. Лупановым также были рассмотрены схемы из функциональных элементов с задержками[13]. Вопрос асимптотической глубины в различных управляющих системах был рассмотрен С. А. Ложкиным[14].

Авторами перечисленных работах было показано, что асимптотическая сложность и глубина/задержка схем из классических функциональных элементов не изменяется в общем случае при асимптотическом росте количества используемой памяти.

Важным параметром является нижняя асимптотическая оценка сложности обратимой схемы, состоящей из функциональных элементов NOT, CNOT и 2-CNOT и не имеющей дополнительных входов[7]. Был предложен

[8] Miller D. M., Wille R., Drechsler R. «*Reducing Reversible Circuit Cost by Adding Lines*» // Proceedings of the 40th IEEE International Symposium on Multiple-Valued Logic (ISMVL'10), Spain, May 2010. Pp. 217–222.

[9] Abdessaied N., Wille R., Soeken M., Drechsler R. «*Reducing the Depth of Quantum Circuits Using Additional Circuit Lines*» // Proceedings of the 5th International Conference on Reversible Computation (RC'13), Victoria, BC, Canada, July 2013. Pp. 221–233.

[10] Shannon C. E. «*The synthesis of two-terminal switching circuits*» // Bell System Technical Journal, 1949. Vol. 28(8). Pp. 59–98.

[11] Лупанов О. Б. «*Об одном методе синтеза схем*» // Известия вузов, Радиофизика, 1958. Т. 1, № 1. С. 120–140.

[12] Карпова Н. А. «*О вычислениях с ограниченной памятью*» // Математические вопросы кибернетики, вып. 2. — М.: Наука, 1989. С. 131–144.

[13] Лупанов О. Б. «*О схемах из функциональных элементов с задержками*» // Проблемы кибернетики, вып. 23. — М.: Наука, 1970. С. 43–81.

[14] Ложкин С. А. «*О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучшие оценки высокой степени точности*» // Вестник Московского университета. Сер. 1. Математика. Механика. — 2007. — № 3. — С. 19–25.

алгоритм синтеза[15], позволяющий получить обратимую схему с наилучшей известной на сегодняшний день асимптотической сложностью, состоящую из функциональных элементов NOT, CNOT и 2-CNOT и не имеющую дополнительных входов. Однако верхняя оценка сложности данной схемы не эквивалентна с точностью до порядка известной нижней оценке сложности таких схем. При этом не было найдено никаких опубликованных результатов по оценке сложности и глубины обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT и имеющих дополнительные входы.

Ещё одним многообещающим направлением исследований является изучение однонаправленности (one-wayness) преобразований через построение реализующих их схем[16]. В обратимой схеме при использовании дополнительных входов возможно появление так называемого «вычислительного мусора» на выходах: ненулевых значений, не являющихся частью результата. Было показано, что любое биективное отображение можно реализовать обратимой схемой без порождения вычислительного мусора[17]. Впоследствии был предложен подход по изучению асимметричных преобразований через построение реализующих их обратимых схем[18] и было сделано предположение, что сложность прямого и обратного преобразований определяется сложностью подсхем по уборке вычислительного мусора для этих преобразований[19].

Цель диссертации.

Основными целями диссертации являются изучение обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT, разработка новых методов синтеза таких схем и изучение зависимости их сложности и глубины от количества используемых дополнительных входов схемы.

Научная новизна.

Все полученные в диссертации результаты являются новыми. В настоящей работе впервые систематически изучается вопрос синтеза схем из обратимых функциональных элементов при различном количестве используемых в схеме дополнительных входов (дополнительной памяти). Разра-

[15] Maslov D. A., Dueck G. W., Miller D. M. «*Techniques for the Synthesis of Reversible Toffoli Networks*» // ACM Transactions on Design Automation of Electronic Systems (TODAES), 2007. Vol. 12(4).

[16] 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 pp.

[17] Китаев А., Шень А., Вялый М. «*Классические и квантовые вычисления*». — М.: МЦНМО, ЧеРо, 1999. — 192 с.

[18] Жуков А. Е. «*Схемы из обратимых логических элементов: один подход к изучению однонаправленности*» // III Международная конференция «Информационные системы и технологии» (IST'06): труды, Минск, 2006.

[19] Жуков А. Е. «*Математические модели криптографии*» // Защита информации. INSIDE. — 2011. № 5. — С. 78–83. — № 6. — С. 40–46.

ботан новый быстрый алгоритм синтеза обратимой схемы, реализующей заданную чётную подстановку с малым числом подвижных точек. Предложены и систематизированы различные способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли. Получены асимптотические оценки сложности, глубины и квантового веса обратимых схем и показано, что данные оценки существенно зависят от количества используемых дополнительных входов схемы. Разработан асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов. Предложены различные способы синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

Теоретическая ценность и практическая значимость.

Работа носит не только теоретический, но и практический характер. Предложенные методы синтеза и способы снижения сложности обратимых схем были реализованы в программном обеспечении[20] по синтезу обратимых схем без дополнительных входов. Данное программное обеспечение, по мнению автора, может быть применено в будущем при решении задач синтеза квантовых схем малой сложности. С другой стороны, разработанные методы снижения сложности обратимых схем позволяют изучать структуру подстановок на множестве двоичных векторов при помощи изучения структуры реализующих их обратимых схем.

Методы исследования.

В работе используются методы теории синтеза управляющих систем, методы теории групп подстановок, мощностные методы установления нижних оценок.

Публикации и апробирование.

Основные результаты диссертации опубликованы автором в работах [1–12], из которых статьи [1–5] — в рецензируемых научных изданиях из перечня ВАК. Результаты диссертации докладывались и обсуждались на спецсеминаре кафедры математической кибернетики факультета ВМК МГУ, на семинаре отдела «Интеллектуальных систем» ФИЦ ИУ РАН и на следующих конференциях:

1. XX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы» (Москва, МИФИ, февраль 2013).

2. V Международная конференция «Безопасные информационные технологии - 2014» (Москва, МГТУ им. Баумана, ноябрь 2014).

[20] Программное обеспечение ReversibleLogicGenerator //
URL: https://github.com/dmitry-zakablukov/ReversibleLogicGenerator

3. 9-я Международная конференция «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, МГУ, май 2015).

4. 8th Conference on Reversible Computation (RC 2016) (Италия, Болонья, июль 2016).

Структура и объём диссертации.

Диссертация состоит из введения, 5 глав, заключения и списка литературы. Текст диссертации изложен на 151 странице, содержит 32 иллюстрации и 9 таблиц. Список литературы включает 105 наименований.

Краткое содержание работы

Во **введении** рассматривается история вопроса с обзором литературы по теме. Описываются цели диссертационной работы, научная новизна, методы исследования и приводится список выступлений и публикаций по теме. Также даётся краткое описание глав диссертации.

В **первой главе** даются базовые определения обратимых функциональных элементов NOT, CNOT и 2-CNOT, а также обобщённого элемента k-CNOT.

Определение 1.4. *N_j^n — инвертор NOT с n входами, инвертирующий свой j-й вход:*

$$N_j^n(\langle x_1, \ldots, x_j, \ldots, x_n\rangle) = \langle x_1, \ldots, x_j \oplus 1, \ldots x_n\rangle \ .$$

Определение 1.5. *$C^n_{i_1,i_2,\ldots,i_k;j}$ — обобщённый элемент Тоффоли k-CNOT с n входами, инвертирующий свой j-й вход тогда и только тогда, когда значение на всех контролирующих входах $i_1, \ldots, i_k$ равно 1, $j \neq i_1, \ldots, i_k$:*

$$C^n_{i_1,i_2,\ldots,i_k;j}(\langle x_1, \ldots, x_j, \ldots, x_n\rangle) = \langle x_1, \ldots, x_j \oplus x_{i_1} \wedge \ldots \wedge x_{i_k}, \ldots, x_n\rangle \ .$$

Определение 1.6. *$C_{I;J;t}$ — функциональный элемент, задающий булево преобразование $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ вида*

$$C_{I;J;t}\left(\langle x_1, \ldots, x_t, \ldots, x_n\rangle\right) = \left\langle x_1, \ldots, x_t \oplus \left(\bigwedge_{i\in I} x_i\right) \wedge \left(\bigwedge_{j\in J} \bar{x}_j\right), \ldots, x_n \right\rangle \ ,$$

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

Вводится унифицированное обозначение обратимого элемента $E(t, I, J)$, где t, I и J — контролируемый выход, множество прямых контролирующих и множество инвертированных контролирующих входов соответственно.

Даётся определение обратимых схем, состоящих из обратимых элементов NOT, CNOT и 2-CNOT. Показывается связь модели обратимых схем с моделью Н. А. Карповой функциональных схем с ограниченной памятью. Вводится множество Ω_n^2, состоящее из всех элементов NOT, CNOT и 2-CNOT с n входами, и множество подстановок $S_{\Omega_n^2} \in S(\mathbb{Z}_2^n)$, задаваемых всеми элементами множества Ω_n^2. В разделах 1.4–1.5 при помощи теории групп подстановок доказываются следующие леммы:

Лемма 1.19. *Множество подстановок $S_{\Omega_n^2}$ при $n < 4$ порождает симметрическую группу $S(\mathbb{Z}_2^n)$.*

Лемма 1.25. *Множество подстановок $S_{\Omega_n^2}$ при $n \geqslant 4$ порождает знакопеременную группу $A(\mathbb{Z}_2^n)$.*

Формулировка этих лемм и их доказательства (отличные от приведённых в данной диссертации) были известны ранее. Здесь же приведены доказательства с целью пояснения полученных в следующих главах верхних оценок сложности обратимых схем.

В разделе 1.6 вводится понятие обратимой схемы, реализующей заданное булево отображение с использованием и без использования дополнительной памяти (дополнительных входов) при помощи расширяющего отображения $\phi_{n,n+k}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^{n+k}$ вида $\phi_{n,n+k}(\langle x_1, \ldots, x_n\rangle) = \langle x_1, \ldots, x_n, 0, \ldots, 0\rangle$ и редуцирующее отображения $\psi^{\pi}_{n+k,n}\colon \mathbb{Z}_2^{n+k} \to \mathbb{Z}_2^n$ вида $\psi^{\pi}_{n+k,n}(\langle x_1, \ldots, x_{n+k}\rangle) = \langle x_{\pi(1)}, \ldots, x_{\pi(n)}\rangle$, где π — некоторая подстановка на множестве $\mathbb{Z}_{n+k}$.

Определение 1.26. *Обратимая схема $\mathfrak{S}_g$ с $(n+q) \geqslant m$ входами, задающая булево преобразование $g\colon \mathbb{Z}_2^{n+q} \to \mathbb{Z}_2^{n+q}$, реализует отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с использованием $q \geqslant 0$ дополнительных входов (дополнительной памяти), если существует такая подстановка $\pi \in S(\mathbb{Z}_{n+q})$, что*

$$\psi^{\pi}_{n+q,m}(g(\phi_{n,n+q}(\mathbf{x}))) = f(\mathbf{x}) \,,$$

где $\mathbf{x} \in \mathbb{Z}_2^n$, $f(\mathbf{x}) \in \mathbb{Z}_2^m$.

Вводится понятие значимых входов и выходов обратимой схемы, а также понятие *вычислительного мусора* на незначимых выходах. Устанавливается связь между схемной сложностью реализации прямого и обратного отображения через сложность обратимой схемы, реализующей прямое отображение.

Доказывается следующее утверждение:

Утверждение 1.31. *Для любой нечётной подстановки $h \in S(\mathbb{Z}_2^n)$, $n \geqslant 4$, существует реализующая ее обратимая схема с одним дополнительным входом, состоящая из элементов множества Ω_n^2.*

Оценивается количество дополнительных входов, необходимых для реализации некоторого заданного сюръективного отображения. Доказывается, что для реализации любого отображения $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$, $m \leqslant n$, требуется не более n дополнительных входов.

Во **второй главе** рассматриваются существующие алгоритмы синтеза обратимых схем: переборные алгоритмы, неперебoрные быстрые алгоритмы и алгоритмы снижения сложности обратимой схемы. Приводится сравнение данных алгоритмов по основным параметрам: время синтеза, количество требуемой для синтеза памяти, сложность синтезированной обратимой схемы. На основании данного сравнения делается вывод, что до текущего момента не было разработано быстрых и эффективных алгоритмов синтеза обратимой схемы, реализующей заданную подстановку с малым числом подвижных точек. Показывается, что существующие алгоритмы синтеза в данном случае либо требуют значительного времени для своей работы, либо синтезируемая схема имеет избыточную сложность.

Даётся описание двух новых быстрых алгоритмов синтеза **A4.1** и **A4.2**, использующих теорию групп подстановок. Принцип работы этих алгоритмов основывается на доказательстве Леммы 1.25 из первой главы о том, что множество подстановок, задаваемых всеми функциональными элементами множества Ω_n^2, при $n \geqslant 4$ генерирует знакопеременную группу подстановок $A(\mathbb{Z}_2^n)$. Доказывается, что наилучший из предложенных алгоритмов синтеза **A4.2** позволяет получить обратимую схему $\mathfrak{S}$ сложности $L(\mathfrak{S}) \lesssim 7n2^m$ для любой чётной подстановки из $A(\mathbb{Z}_2^n)$, у которой не более 2^m подвижных точек, $m \leqslant n$.

В конце второй главы сравниваются существующие и предложенные быстрые алгоритмы синтеза, использующие теорию групп подстановок. На основании этого сравнения делается вывод об эффективности новых алгоритмов с точки зрения их быстродействия и сложности синтезируемых обратимых схем.

В **третьей главе** рассматриваются различные способы снижения сложности обратимых схем. В разделе 3.2 доказывается необходимое и достаточное условие коммутируемости двух обратимых функциональных элементов.

Лемма 3.2. *Элементы $E(t_1, I_1, J_1)$ и $E(t_2, I_2, J_2)$ являются коммутирующими тогда и только тогда, когда выполняется хотя бы одно из условий:*

1. $t_1 \notin I_2 \cup J_2$ *и* $t_2 \notin I_1 \cup J_1$ *(в частности,* $t_1 = t_2$*);*
2. $I_1 \cap J_2 \neq \varnothing$ *или* $I_2 \cap J_1 \neq \varnothing$.

В разделе 3.3 предлагаются различные эквивалентные замены композиций обратимых функциональных элементов с доказательством корректности таких замен.

Замена 3.1. *Композиция элементов $E(t, I, J) * E(t, I, J)$ может быть исключена из схемы.*

Замена 3.2. *Если* $I_1 = I_2 \cup \{ k \}$, $J_2 = J_1 \cup \{ k \}$, $k \notin I_2 \cup J_1$, *то композиция элементов* $E(t, I_1, J_1) * E(t, I_2, J_2)$ *может быть заменена одним элементом* $E(t, I_2, J_1)$.

Замена 3.3. *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 элементов* $E(t, I_1, J_1) * E(t, I_2, J_2)$ *может быть заменена композицией* $E(t, I_1, J_3) * E(t, I_2, J_3)$, *где* $J_3 = J_1 \setminus \{ q \} = J_2 \setminus \{ p \}$.

Замена 3.4. *Если* $t_1 \in I_2 \cup J_2$, $t_2 \notin I_1 \cup J_1$, *то композиция некоммутирующих элементов* $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ *может быть заменена композицией* $E(t_2, I_1 \cup I_2 \setminus \{ t_1 \}, J_1 \cup J_2 \setminus \{ t_1 \}) * E(t_2, I_2, J_2) * E(t_1, I_1, J_1)$.

Замена 3.5. *Если в условии замены 3.4* $I_1 \subseteq I_2$ *и* $J_1 \subseteq J_2$, *то композиция некоммутирующих элементов* $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ *может быть заменена композицией* $E(t_2, I_2 \cup \{ t_1 \}, J_2 \setminus \{ t_1 \}) * E(t_1, I_1, J_1)$, *если* $t_1 \in J_2$, *и композицией* $E(t_2, I_2 \setminus \{ t_1 \}, J_2 \cup \{ t_1 \}) * E(t_1, I_1, J_1)$, *если* $t_1 \in I_2$.

Замена 3.6. *Если* $t_2 \in I_1 \cup J_1$, $t_1 \notin I_2 \cup J_2$, *то композиция некоммутирующих элементов* $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ *может быть заменена композицией* $E(t_2, I_2, J_2) * E(t_1, I_1, J_1) * E(t_1, I_1 \cup I_2 \setminus \{ t_2 \}, J_1 \cup J_2 \setminus \{ t_2 \})$.

Замена 3.7. *Если в условии замены 3.6* $I_2 \subseteq I_1$ *и* $J_2 \subseteq J_1$, *то композиция некоммутирующих элементов* $E(t_1, I_1, J_1) * E(t_2, I_2, J_2)$ *может быть заменена композицией* $E(t_2, I_2, J_2) * E(t_1, I_1 \cup \{ t_2 \}, J_1 \setminus \{ t_2 \})$, *если* $t_2 \in J_1$, *и композицией* $E(t_2, I_2, J_2) * E(t_1, I_1 \setminus \{ t_2 \}, J_1 \cup \{ t_2 \})$, *если* $t_2 \in I_1$.

Замена 3.8. *Элемент* $E(t, I, J)$ *можно заменить на композицию функциональных элементов вида* $\left(\underset{t \in J}{*} E(t) \right) * E(t, I \cup J) * \left(\underset{t \in J}{*} E(t) \right)$.

Замена 3.9. *Если* $k \in J$, *то элемент* $E(t, I, J)$ *можно заменить на композицию элементов* $E(t, I \cup \{ k \}, J \setminus \{ k \}) * E(t, I, J \setminus \{ k \})$.

Замена 3.10. *Если* $I_1 = I_2 \cup \{ k \}$, *то композиция элементов* $E(t, I_1, J) * E(t, I_2, J)$ *может быть заменена одним элементом* $E(t, I_2, J \cup \{ k \})$.

Замена 3.11. *Если* $J_1 = J_2 \cup \{ k \}$, *то композиция элементов* $E(t, I, J_1) * E(t, I, J_2)$ *может быть заменена одним элементом* $E(t, I \cup \{ k \}, J_2)$.

В разделе 3.4 описывается алгоритм снижения сложности обратимых схем, состоящих из элементов $E(t, I, J)$, использующий предложенные эквивалентные замены композиций функциональных элементов. Даётся оценка снизу временно́й сложности данного алгоритма.

В разделе 3.5 рассматриваются различные способы снижения сложности обратимой схемы на этапе её синтеза. Первый способ (параграф 3.5.1): поиск грани булева куба $\mathbb{B}^n$, такой что для найденной грани размерности k в синтезируемой схеме можно заменить композицию порядка 2^{n-k-2} подряд идущих функциональных элементов на композицию не более n элементов $E(t, I, J)$. Второй способ (параграф 3.5.2): эффективное разбиение циклов в представлении исходной подстановки в виде произведения независимых циклов для увеличения размерности грани булева куба в первом способе. Описывается алгоритм быстрого поиска такого разбиения. Третий способ

(параграф 3.5.3): рассмотрение произведения справа и слева в представлении исходной подстановки в виде произведения транспозиций для увеличения размерности грани булева куба в первом способе.

В разделе 3.6 показывается эффективность предложенных способов снижения сложности обратимой схемы на практике. Описываются результаты экспериментов синтеза обратимых схем при помощи разработанного программного обеспечения[19]. Приводятся характеристики более 40 полученных обратимых схем, у которых либо меньшее количество входов, либо меньшая сложность, либо меньший квантовый вес по сравнению с известными результатами.

В **четвёртой главе** рассматривается вопрос асимптотической сложности и глубины обратимых схем, состоящих из функциональных элементов множества Ω_n^2 и реализующих некоторое отображение $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. В разделе 4.1 вводится множество $F(n,q)$ всех отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$, которые могут быть реализованы такими обратимыми схемами с $(n+q)$ входами. Рассматриваются обратимые схемы, реализующие отображение $f \in F(n,q)$ с использованием q дополнительных входов (дополнительной памяти). Вводятся функции Шеннона сложности $L(n,q)$, глубины $D(n,q)$ и квантового веса $W(n,q)$ обратимой схемы как функции от n и количества дополнительных входов схемы q:

$$L(n,q) = \max_{f \in F(n,q)} L(f,q) \ ,$$
$$D(n,q) = \max_{f \in F(n,q)} D(f,q) \ ,$$
$$W(n,q) = \max_{f \in F(n,q)} W(f,q) \ .$$

Здесь $L(f,q)$, $D(f,q)$ и $W(f,q)$ — минимальная сложность, глубина и квантовый вес соответственно обратимой схемы, реализующей отображение $f \in F(n,q)$.

В разделе 4.2 при помощи мощностного метода Риордана–Шеннона доказываются общие нижние оценки для функций $L(n,q)$, $D(n,q)$ и $W(n,q)$.

Теорема 4.1.

$$L(n,q) \geqslant \frac{2^n(n-2)}{3\log_2(n+q)} - \frac{n}{3} \ .$$

Теорема 4.2.

$$D(n,q) \geqslant \frac{2^n(n-2)}{3(n+q)\log_2(n+q)} - \frac{n}{3(n+q)} \ .$$

Теорема 4.3.

$$W(n,q) \geqslant \min\left(W^{(C)}, W^{(T)}\right) \cdot \left(\frac{2^n(n-2)}{3\log_2(n+q)} - \frac{n}{3}\right) .$$

Здесь $W^{(C)}$ и $W^{(T)}$ — квантовый вес функциональных элементов NOT/CNOT и 2-CNOT соответственно.

В разделе 4.3 предлагается обобщение алгоритма синтеза **A4.2**, описанного во второй главе: исходная подстановка из $A(\mathbb{Z}_2^n)$ представляется в виде произведения не пар независимых транспозиций, а групп по K независимых транспозиций в каждой группе. Доказывается, что любая такая группа может быть задана композицией одного обобщённого элемента Тоффоли с большим количеством контролирующих входов и множества элементов CNOT и 2-CNOT. Доказываются верхние оценки для характеристик обратимых схем без дополнительной памяти:

Теорема 4.5.

$$L(n,0) \leqslant \frac{3n2^{n+4}}{\log_2 n - \log_2\log_2 n - \log_2\phi(n)}\left(1+\varepsilon(n)\right) ,$$

где $\phi(n)$ — любая сколь угодно медленно растущая функция такая, что $\phi(n) < n \,/\log_2 n$,

$$\varepsilon(n) = \frac{1}{6\phi(n)} + \left(\frac{8}{3} - o(1)\right)\frac{\log_2 n \cdot \log_2\log_2 n}{n} .$$

Теорема 4.6.

$$L(n,0) \asymp \frac{n2^n}{\log_2 n} .$$

Теорема 4.7.

$$D(n,0) \leqslant \frac{n2^{n+5}}{\log_2 n - \log_2\log_2 n - \log_2\phi(n)}\left(1+\varepsilon(n)\right) ,$$

где $\phi(n)$ — любая сколь угодно медленно растущая функция такая, что $\phi(n) < n \,/\log_2 n$,

$$\varepsilon(n) = \frac{1}{4\phi(n)} + (4+o(1))\frac{\log_2 n \cdot \log_2\log_2 n}{n} .$$

Теорема 4.8.

$$W(n,0) \leqslant \frac{n2^{n+4}\left(W^{(C)}(1+\varepsilon_C(n)) + 2W^{(T)}(1+\varepsilon_T(n))\right)}{\log_2 n - \log_2\log_2 n - \log_2\phi(n)} ,$$

где $\phi(n)$ — любая сколь угодно медленно растущая функция такая, что $\phi(n) < n \,/\, \log_2 n$,

$$\varepsilon_C(n) = \frac{1}{2\phi(n)} - \left(\frac{1}{2} - o(1)\right) \cdot \frac{\log_2 \log_2 n}{n} \,,$$
$$\varepsilon_T(n) = (4 - o(1)) \frac{\log_2 n \cdot \log_2 \log_2 n}{n} \,.$$

В разделе 4.4 описывается асимптотически оптимальный метод синтеза обратимых схем с дополнительной памятью, аналогичный методу Лупанова для классических схем. При описании данного метода подсчитывается количество используемых дополнительных входов обратимой схемы (дополнительной памяти) при достижении минимальной сложности и минимальной глубины схемы. Доказываются верхние оценки для характеристик обратимых схем с дополнительной памятью.

Теорема 4.10. *$L(n, q_0) \lesssim 2^n$ при $q_0 \sim n2^{n-\lceil n \,/\, \phi(n)\rceil}$, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/(\log_2 n + \log_2 \psi(n))$.*

Теорема 4.11. *$L(n, q_0) \asymp 2^n$ при $q_0 \sim n2^{n-\lceil n \,/\, \phi(n)\rceil}$, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/(\log_2 n + \log_2 \psi(n))$.*

Теорема 4.12. *$W(n, q_0) \lesssim W^{(C)} \cdot 2^n + W^{(T)} \cdot n2^{n-\lceil n \,/\, \phi(n)\rceil}$ при $q_0 \sim n2^{n-\lceil n \,/\, \phi(n)\rceil}$, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/(\log_2 n + \log_2 \psi(n))$.*

Теорема 4.13. *Любое булево отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ можно реализовать с помощью обратимой схемы $\mathfrak{S}$, имеющей сложность $L(\mathfrak{S}) \lesssim m2^n \,/\, n$, при использовании $q \sim (m+1)2^{n-\lceil n \,/\, \phi(n)\rceil}$ дополнительных входов, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/(\log_2 n + \log_2 \psi(n))$.*

Теорема 4.15. *$D(n, q_1) \lesssim 3n$ при $q_1 \sim 2^n$. Обратимая схема $\mathfrak{S}$, реализующая отображение $f \in F(n, q_1)$ с глубиной $D(\mathfrak{S}) \sim 3n$, имеет сложность $L(\mathfrak{S}) \sim 2^{n+1}$ и квантовый вес $W(\mathfrak{S}) \sim W^{(C)} \cdot 2^{n+1} + W^{(T)}. \cdot n2^{n-\lceil n \,/\, \phi(n)\rceil}$, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/(\log_2 n + \log_2 \psi(n))$.*

Теорема 4.16. *$D(n, q_2) \lesssim 2n$ при $q_2 \sim \phi(n)2^n$, где $\phi(n)$ — любая сколь угодно медленно растущая функция такая, что $\phi(n) = o(n)$. Обратимая схема $\mathfrak{S}$, реализующая отображение $f \in F(n, q_2)$ с глубиной $D(\mathfrak{S}) \sim 2n$, имеет сложность $L(\mathfrak{S}) \sim \phi(n)2^{n+1}$ и квантовый вес $W(\mathfrak{S}) \sim W^{(C)} \cdot \phi(n)2^{n+1} + W^{(T)}. \cdot 2^{n-\lceil n \,/\, \phi(n)\rceil}$.*

Получены общие верхние оценки сложности, глубины и квантового веса обратимых схем.

Теорема 4.18. *Для любого значения q такого, что $8n < q \lesssim n2^{n-\lceil n \,/\, \phi(n)\rceil}$, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие*

функции такие, что $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$, *верно соотношение*

$$L(n,q) \lesssim 2^n + \frac{8n2^n}{\log_2(q-4n) - \log_2 n - 2}\,.$$

Следствие 4.19. *Для любого значения* q *такого, что* $8n < q \lesssim n2^{n-\lceil n\,/\,\phi(n)\rceil}$, *где* $\phi(n)$ *и* $\psi(n)$ *— любые сколь угодно медленно растущие функции такие, что* $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$, *верны соотношения*

$$W(n,q) \lesssim W^{(T)} \cdot \left(2^n + \frac{8 \cdot 2^n}{\log_2(q-4n) - \log_2 n - 2}\right) + \\ + \frac{32W^{(C)}n2^n}{\log_2(q-4n) - \log_2 n - 2}\,,$$

$$W(n,q) \lesssim W^{(T)} \cdot \left(2^n + \frac{8n2^n}{\log_2(q-4n) - \log_2 n - 2}\right) + \\ + \frac{32W^{(C)}2^n}{\log_2(q-4n) - \log_2 n - 2}\,.$$

Теорема 4.20. *Для любого значения* q *такого, что* $n^2 \lesssim q \lesssim 2^{n-\lceil n\,/\,\phi(n)\rceil+1}$, *где* $\phi(n)$ *и* $\psi(n)$ *— любые сколь угодно медленно растущие функции такие, что* $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$, *верно соотношение*

$$L(n,q) \asymp \frac{n2^n}{\log_2 q}\,.$$

Теорема 4.21. *Для любого значения* q *такого, что* $0 \leqslant q \lesssim 2^{n-\lceil n\,/\,\phi(n)\rceil+1}$, *где* $\phi(n)$ *и* $\psi(n)$ *— любые сколь угодно медленно растущие функции такие, что* $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$, *верно соотношение*

$$L_A(n,q) \asymp \frac{n2^n}{\log_2(n+q)}\,.$$

Здесь $L_A(n,q)$ — функция Шеннона сложности обратимых схем, реализующих отображения $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ только из знакопеременной группы $A(\mathbb{Z}_2^n)$.

Теорема 4.23. *Для любого значения* q *такого, что* $8n < q \lesssim n2^{n-\lceil n\,/\,\phi(n)\rceil}$, *где* $\phi(n)$ *и* $\psi(n)$ *— любые сколь угодно медленно растущие функции такие, что* $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$, *верно соотношение*

$$D(n,q) \lesssim 2^{n+1}(2,5 + \log_2 n - \log_2(\log_2(q-4n) - \log_2 n - 2))\,.$$

На основании полученных асимптотических оценок делается вывод о зависимости значений характеристик обратимой схемы от количества до-

полнительных входов в ней.

Утверждение 4.24. *Использование дополнительной памяти в обратимых схемах, состоящих из элементов NOT, CNOT и 2-CNOT, почти всегда позволяет существенно снизить сложность, глубину и квантовый вес таких схем.*

В **пятой главе** показывается применение обратимых схем для решения задачи схемной реализации некоторых вычислительно асимметричных преобразований. В разделе 5.1 подробно рассматривается алгоритм дискретного логарифмирования по основанию примитивного элемента в конечном поле характеристики 2 на примере фактор-кольца $\mathbb{F}_2[x] \,/\, f(x)$, где $f(x)$ — неприводимый многочлен степени n, и его реализация обратимой схемой.

В разделе 5.2 приводятся результаты экспериментов синтеза обратимых схем без дополнительной памяти и с дополнительной памятью, реализующих алгоритм дискретного логарифмирования, при помощи разработанного программного обеспечения[19]. Показывается, что уже при использовании n дополнительных входов сложность таких схем существенно снижается.

В параграфе 5.2.3 доказывается верхняя асимптотическая оценка сложности обратимой схемы $\mathfrak{S}$, реализующей алгоритм дискретного логарифмирования в фактор-кольце $\mathbb{F}_2[x] \,/\, f(x)$, описываемый отображением $f_{\log}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$:

Теорема 5.4. *Существует обратимая схема $\mathfrak{S}_{\log}$, состоящая из функциональных элементов множества Ω^2_{n+q} и реализующая отображение $f_{\log}$ со сложностью $L(\mathfrak{S}_{\log}) \lesssim (2^{n+1} \cdot \log_2 n) \,/\, n$ при использовании $q \sim 2^{n-\lceil n \,/\, \phi(n) \rceil + 2} \cdot \log_2 n$ дополнительных входов, где $\phi(n)$ и $\psi(n)$ — любые сколь угодно медленно растущие функции такие, что $\phi(n) \leqslant n \,/ (\log_2 n + \log_2 \psi(n))$.*

Данная оценка асимптотически ниже, чем для произвольного булева преобразования, и достигается при асимптотически меньшем количестве дополнительных входов.

В разделе 5.3 рассматривается вопрос схемной сложности реализации алгоритма, обратного к заданному, и делается попытка объяснить разницу в схемной сложности для прямого и обратного алгоритмов через необратимость и потерю части информации во время работы прямого алгоритма:

Гипотеза 5.5. *Обратимая схема, реализующая алгоритм, обратный к заданному, имеет сложность с бóльшей на порядок степенью роста по отношению к сложности обратимой схемы, реализующей прямой алгоритм, если при переходе от прямого алгоритма к обратному теряется какая-то часть информации.*

В подтверждение Гипотезы 5.5 приводятся примеры обратимых схем, реализующие такие вычислительно асимметричные преобразования, как сложение в кольце многочленов, умножение и возведение в степень в конечном поле характеристики 2.

Заключение содержит список основных результатов, полученных в работе, список открытых вопросов и предложений по дальнейшим исследованиям.

Основные результаты диссертации

1. Разработан новый быстрый алгоритм синтеза обратимой схемы, состоящей из функциональных элементов NOT, CNOT и 2-CNOT и реализующей заданную чётную подстановку с малым числом подвижных точек.
2. Предложены и систематизированы различные способы снижения сложности обратимых схем, состоящих из обобщённых элементов Тоффоли с прямыми и инвертированными контролирующими входами.
3. Получены нижние и верхние асимптотические оценки сложности, глубины и квантового веса обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Показано, что данные оценки существенно зависят от количества используемых дополнительных входов схемы.
4. Разработан быстрый, асимптотически оптимальный метод синтеза обратимых схем без дополнительных входов, состоящих из функциональных элементов NOT, CNOT и 2-CNOT.
5. Предложены различные способы синтеза обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT и реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

Работы автора по теме диссертации

Статьи в рецензируемых научных изданиях из перечня ВАК:

[1] Закаблуков Д. В. «*Быстрый алгоритм синтеза обратимых схем на основе теории групп подстановок*» // Прикладная дискретная математика, 2014, № 2. С. 101–109.

[2] Закаблуков Д. В. «*Вентильная сложность обратимых схем как мера сложности четных подстановок*» // Вестник МГТУ им. Н. Э. Баумана, серия «Приборостроение», 2015, № 1(100). С. 67–82.

[3] Закаблуков Д. В. «*Снижение вентильной сложности обратимых схем без использования таблиц эквивалентных замен композиций*

вентилей» // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2014. № 3. DOI: 10.7463/0314.0699195.

[4] Закаблуков Д. В. «*О сложности обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT*» // Дискретная математика, 2016. Т. 28, № 2. С. 12–26.

[5] Закаблуков Д. В. «*Оценка глубины обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT*» // Вестник Московского университета, серия «Математика. Механика», 2016, № 3. С. 3–12.

Другие публикации:

[6] Жуков А. Е., Закаблуков Д. В., Засорина Ю. В., Чикин А. А. «*Вычислительно асимметричные преобразования и схемы из обратимых элементов*» // Вопросы кибербезопасности, 2015, № 2(10). С. 49–55.

[7] Закаблуков Д. В. «*Асимптотическая сложность и глубина обратимых схем из элементов NOT, CNOT и 2-CNOT*» // Дискретные модели в теории управляющих систем: IX Международная конференция, Москва и Подмосковье, 20–22 мая 2015 г.: Труды / Отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. — М.: МАКС Пресс, 2015. — С. 82–84.

[8] Закаблуков Д. В., Жуков А. Е. «*Исследование схем из обратимых логических элементов*» // Информатика и системы управления в XXI веке: Сборник трудов № 9 молодых ученых, аспирантов и студентов. — М.: МГТУ им. Н. Э. Баумана, 2012. — С. 148–157.

[9] Закаблуков Д. В. «*Синтез схем из обратимых элементов*» // Тезисы доклада XX Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», МИФИ, 2013. — С. 100–101.

[10] Закаблуков Д. В. «*Синтез обратимых схем на основе теории групп подстановок*» // «Безопасные информационные технологии». Сборник трудов Пятой Всероссийской научно-технической конференции / под ред. Матвеева В. А., — М.: НИИ Радиоэлектроники и лазерной техники МГТУ им. Н. Э. Баумана, 2015. — С. 84–85.

[11] Zakablukov D. V. «*Application of Permutation Group Theory in Reversible Logic Synthesis*» // In book: Devitt S., Lanese I. (eds) Reversible Computation — RC 2016. (Series: Lecture Notes in Computer Science). Springer Cham, 2016. Vol. 9720. Pp. 223–238. DOI: 10.1007/978-3-319-40578-0_17.

[12] Zakablukov D. V. «*On Asymptotic Gate Complexity and Depth of Reversible Circuits Without Additional Memory*» // Journal of Computer and System Sciences, 2017. Vol. 84. Pp. 132–143. DOI: 10.1016/j.jcss.2016.09.010.