ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Закаблукова Дмитрия Владимировича

«Методы синтеза обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT»,

представленную на соискание учёной степени

кандидата физико-математических наук по специальности

01.01.09 – «Дискретная математика и математическая кибернетика».

Диссертация посвящена исследованию одной интересной и важной как с теоретической, так и с прикладной точек зрения модели дискретных управляющих систем – обратимым схемам из функциональных элементов. Эта модель тесно связана с квантовыми технологиями и квантовыми вычислениями, а также с разработкой энергоэффективных вычислительных устройств. Таким образом, систематическое исследование обратимых схем и разработка методов их синтеза являются весьма насущными, что **обуславливает высокую актуальность темы диссертационной работы.**

Диссертационная работа состоит из введения, пяти глав, заключения и списка литературы, включающего 105 наименований.

Во введении проведён детальный обзор литературы, касающейся истории и развития как теории обратимых вычислений, так и теории управляющих систем в целом. Выделены основные моменты, которые не были изучены для класса обратимых схем, к примеру, вопрос об их асимптотической сложности.

В первой главе приводятся базовые понятия, даются определения обратимых элементов и состоящих из них схем. Вводятся основные характеристики обратимых схем, изучаемых в работе: сложности, глубины и квантового веса. Показывается связь обратимых элементов и схем с подстановками. Даётся математически точное определение обратимых схем с дополнительными входами, являющееся важным для понимания всей работы в целом.

Во второй главе рассматриваются существующие алгоритмы синтеза обратимых схем, анализируются их достоинства и недостатки. На основании сравнения рассмотренных алгоритмов делается вывод о необходимости разработки новых методов синтеза обратимых схем, задающих подстановки с малым числом подвижных точек. Даётся описание двух таких неперебoрных алгоритмов синтеза, имеющих лучшие, по сравнению с их аналогами, характеристики, что подтверждается соответствующими данными.

В третьей главе рассматриваются различные способы снижения сложности обратимых схем. Для этого вводится обобщённый элемент Тоффоли с инвертированными

управляющими входами и доказывается новый признак коммутируемости двух обратимых элементов. Даётся описание эквивалентных замен композиций обратимых элементов при помощи операций на множествах, что позволяет обобщить существующие и получить новые эквивалентные замены. Приводятся результаты практического применения описываемых в главе способов снижения сложности в виде описания более 40 улучшенных по основным характеристикам обратимых схем.

В четвёртой главе рассматривается вопрос об асимптотических оценках сложности, глубины и квантового веса обратимых схем. В ней с помощью мощностного метода доказываются нижние оценки соответствующих функций Шеннона. Приводится описание первого и единственного на сегодняшний день асимптотически оптимального по порядку метода синтеза обратимых схем без дополнительных входов. Рассматриваются различные модификации стандартного метода О.Б. Лупанова в применении к обратимым схемам, при помощи которых удалось установить порядок роста сложности обратимых схем для весьма широкого диапазона значений количества дополнительных входов. При этом оказалось, что использование дополнительных входов в обратимых схемах почти всегда позволяет существенно снизить их сложность, глубину и квантовый вес.

В пятой главе рассматривается практическое применение обратимых схем для реализации вычислительно асимметричных преобразований. В качестве примера такого преобразования рассматривается алгоритм дискретного логарифмирования по основанию примитивного элемента в конечном поле характеристики 2. Получены асимптотические оценки сложности обратимых схем, реализующих данный алгоритм, существенно отличающиеся от оценок в общем случае. Выдвигается гипотеза о природе различия сложностей схемной реализации прямого и обратного преобразований.

В заключении приводится список основных результатов диссертации и направлений дальнейших исследований.

Основные результаты диссертационной работы:

1. Получены верхние и нижние асимптотические оценки сложности, глубины и квантового веса обратимых схем из элементов NOT, CNOT и 2-CNOT. Установлен порядок роста функции Шеннона для сложности обратимых схем в весьма широком диапазоне значений количества дополнительных входов, который существенно зависит от количества дополнительных входов в схеме.
2. Предложены новые и систематизированы существующие способы снижения сложности обратимых схем.

3. Разработан эффективный быстрый алгоритм синтеза обратимых схем, задающих подстановку с малым числом подвижных точек.
4. Разработан оригинальный, асимптотически оптимальный по порядку метод синтеза обратимых схем, состоящих из элементов NOT, CNOT и 2-CNOT и не имеющих дополнительных входов.
5. Предложено несколько способов синтеза обратимых схем, реализующих алгоритм дискретного логарифмирования в конечном поле характеристики 2.

Достоверность изложенных в диссертации результатов обусловлена строгостью математической модели, корректностью математических доказательств всех утверждений, лемм и теорем, а также проведенными экспериментами по синтезу обратимых схем.

Замечания по диссертационной работе:

1. Отсутствуют верхние оценки временной сложности алгоритмов уменьшения сложности обратимых схем, описанных в третьей главе, что мешает пониманию возможности их применения на практике и не позволяет сравнить их с существующими аналогами.
2. Не получены асимптотические оценки сложности обратимых схем, состоящих из обобщённых элементов Тоффоли, которые имеют ключевое значение в описанных способах снижения сложности обратимых схем.
3. Гипотеза из пятой главы подтверждается только одним примером, рассмотренным автором: алгоритмом дискретного логарифмирования в конечном поле характеристики 2.

Все приведённые замечания не являются принципиальными, не снижают научной ценности работы и не влияют на общую положительную оценку диссертации.

Результаты диссертационной работы получены автором лично и изложены в 12 печатных трудах, из которых 5 статей опубликованы в рецензируемых научных изданиях из перечня ВАК. Результаты докладывались и обсуждались на российских и международных конференциях соответствующей тематики.

Диссертация соответствует всем критериям, установленным Положением о порядке присуждения учёных степеней. Диссертационная работа обладает внутренним единством, содержит новые научные результаты и рекомендации по их практическому применению. Автореферат правильно и в полном объёме отражает содержание диссертации.

Диссертация представляет собой законченную научно-квалификационную работу, содержащую решение задачи оптимального по порядку синтеза обратимых схем, имеющее существенное значение для развития теории дискретных управляющих систем. Работа полностью соответствует требованиям ВАК РФ, предъявляемым к диссертациям на соискание учёной степени кандидата физико-математических наук по специальности 01.01.09 – «Дискретная математика и математическая кибернетика», а её **автор, Закаблуков Дмитрий Владимирович, заслуживает присуждения ему учёной степени кандидата физико-математических наук по данной специальности**.

Официальный оппонент
Доктор физико-математических наук, профессор кафедры математической кибернетики факультета вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова»
Адрес: 119991, ГСП-1 Москва, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус
Телефон: +7 (495) 939-30-10
E-mail: lozhkin@cs.msu.su

Ложкин Сергей Андреевич _____ / Ложкин С.А. /

Подпись д.ф.-м.н., проф. Ложкина С.А. и сведения заверяю.
Декан факультета вычислительной математики и кибернетики
МГУ им. М.В. Ломоносова,
академик РАН, профессор, заведующий кафедрой функционального анализа и его применений

Моисеев Евгений Иванович _____ / Моисеев Е.И. /

«15» мая 2018 г.