Отзыв

официального оппонента на диссертацию Д. В. Закаблукова «Методы синтеза обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT», представленную на соискание ученой степени кандидата физико-математических наук по специальности 01.01.09 – дискретная математика и математическая кибернетика

В данной работе изучаются схемы из функциональных элементов в обратимых базисах. Интерес к таким схемам возникает в связи с теорией квантовых вычислений и потенциальными технологическими проблемами из-за дополнительного тепловыделения при реализации необратимых функциональных элементов. В современной технике тепловые потери из-за необратимости незначительны, но при дальнейшем росте плотности размещения логических устройств могут стать критическими.

Что касается квантовых вычислений, то во многих эффективных квантовых алгоритмах есть необходимости выполнять классические вычисления на квантовых элементах. Стандартным (хотя и не единственно возможным способом) является как раз реализация классических схем из обратимых функциональных элементов.

Таким образом, данный специфический случай схем из функциональных элементов заслуживает отдельного изучения. В данной диссертации проведена систематическая работа по анализу схем из обратимых элементов.

Диссертация состоит из 5 глав, введения, заключения и списка литературы.

Первая глава содержит общие сведения об обратимой логике, в ней также вводятся терминология и обозначения, которые используются в остальной части работы. Приводятся также доказательства некоторых известных фактов о порождении группы перестановок и знакопеременной группы. Эти доказательства отличаются от стандартных и используются в дальнейшей части работы.

Во второй главе рассматриваются алгоритмы синтеза обратимых схем. Построены два новых алгоритма синтеза схем, которые эффективны при малом числе подвижных точек реализуемого преобразования.

В третьей главе рассматриваются способы снижения сложности обратимых схем. Они основаны на соотношениях коммутирования обратимых элементов и на модификациях алгоритмов синтеза, описанных в предыдущей главе. Представлены результаты экспериментальной проверки предлагаемых методов. Для ряда функций получены схемы с рекордными значениями параметров сложности.

В четвертой главе рассматриваются функции Шеннона сложности, глубины и квантового веса для рассматриваемых классов схем, включая зависимость от числа используемых дополнительных входов. Мощностным методом получены нижние оценки для этих функций. Верхние оценки для функций Шеннона получены подходящими модификациями изложенных ранее алгоритмов синтеза. (Отдельно рассмотрены случай отсутствия дополнительной памяти, случай «большой» дополнительной памяти и общий случай.) Из полученных оценок следует, что использование дополнительной памяти почти всегда позволяет снизить сложность, глубину и квантовый вес схем. Это существенное отличие от случая схем из необратимых функциональных элементов.

Пятая глава иллюстрирует полученные ранее результаты применительно к задаче дискретного логарифмирования. Задача дискретного логарифмирования считается вычислительно трудной и имеет важные приложения в криптографии. На примере этой задачи показаны возможности общих алгоритмов синтеза и приводятся некоторые уточнения общих оценок, достигаемые с помощью приемов, специфических для данной задачи.

Также в пятой главе обсуждаются общие вопросы схемной реализации алгоритма, обратного к заданному.

Характеризуя работу в целом, можно утверждать, что она представляет собой законченное исследование и является существенным вкладом в теорию сложности схем из функциональных элементов.

Все основные результаты работы являются новыми. Автореферат диссертации соответствует основным идеям и выводам работы.

Можно отметить некоторые неточности в изложении. В частности, при обсуждении уменьшения числа состояний в результате применения сюръективной функции (правильно: неинъективной) на с. 6 не уточняются область определения и область значений функции, из-за чего вывод об уменьшении числа состояний ровно в два раза выглядит необоснованным. На с. 12, не уточняется размер обратимых схем, реализующих алгоритм Шора (и не вполне ясно, о чем идет речь). В формулировках теорем 4.5 (с. 86), 4.7 (с. 91), 4.8 (с. 93) формулы записаны в избыточно сложном, на первый взгляд, виде. Для сравнения с нижней оценкой теоремы 4.1 лучше было выделить множитель 2^n в этих формулах. В разделе 5.1 (с.122) указываются алгоритмы субэспоненциальной временно́й сложности для задачи дискретного логарифмирования, но не обсуждается возможная их реализация обратимыми схемами. Высказанная в разделе 5.3 гипотеза 5.5 о потере информации иллюстрируется на примерах. Однако отсутствует обсуждение соотношения этой гипотезы и популярной гипотезы о существовании односторонних перестановок: совместимы ли эти гипотезы и, если совместимы, как понимать потерю информации при обратимом преобразовании?

Эти неточности не являются принципиальными и не снижают ценности работы.

Работа удовлетворяет требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор заслуживает присвоения искомой степени.

Официальный оппонент
старший научный сотрудник ФИЦ ИУ РАН,
кандидат физико-математических наук
Вялый Михаил Николаевич
119333, Москва, ул. Вавилова, 42
тел. 8-926-112-28-24
эл. почта vyalyi@gmail.com

27 марта 2018 года

Подпись М.Н.Вялого заверяю
Учёный секретарь ФИЦ ИУ РАН
д.т.н. /В.Н.Захаров/

27 марта 2018 года