МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. Ломоносова

МАТЕРИАЛЫ
XX МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ

ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ КИБЕРНЕТИКИ

Москва
5–8 декабря 2024 г.

МАКС ПРЕСС

МОСКВА – 2025

УДК 519.7
ББК 22.18
П78

https://elibrary.ru/brukip

Редакторы:
С.А. Ложкин, Д.С. Романов, В.В. Подымов

П78 **Проблемы теоретической кибернетики** : материалы XX Международной научной конференции (Москва, 5–8 декабря 2024 г.) / редакторы С.А. Ложкин, Д.С. Романов, В.В. Подымов. – М. : МАКС Пресс, 2025. – 200 с.
ISBN 978-5-317-07402-9
https://doi.org/10.29003/m4678.978-5-317-07402-9

В сборнике представлены труды XX Международной научной конференции «Проблемы теоретической кибернетики» (Москва, 5–8 декабря 2024г.), посвященной 270-летию МГУ имени М. В. Ломоносова и 100-летию со дня рождения чл.-корр. РАН С. В. Яблонского. Тематика конференции включает следующие направления: дискретные функциональные системы, свойства дискретных функций, сложность алгоритмов, синтез, сложность, надёжность, контроль и диагностика управляющих систем, автоматы, теория графов, комбинаторика, теория кодирования, математические методы защиты информации, теория распознавания образов, математическая теория интеллектуальных систем, прикладная математическая логика, приложения дискретной математики и математической кибернетики в естествознании и технике.

Для научных работников и специалистов в области математической кибернетики, дискретной математики, информатики и их приложений.

УДК 519.7
ББК 22.18

Problems of theoretical cybernetics : XX International Scientific Conference (Moscow, December 5–8, 2024) : Proceedings / S.A. Lozhkin, D.S. Romanov, V.V. Podymov (Eds.). – Moscow : MAKS Press, 2025. – 200 p.

The collection represents proceedings of the XX International Scientific Conference “Problems of Theoretical Cybernetics” (Moscow, December 5–8, 2024) dedicated to 270th anniversary of Lomonosov Moscow State University and 100th anniversary of S. V. Yablonsky, corresponding member of Russian Academy of Sciences. The conference subject area includes: discrete functional systems; properties of discrete functions; complexity of algorithms; synthesis, complexity, reliability, control and diagnostics of control systems; automata; graph theory; combinatorics; coding theory; mathematical methods of information security; theory of pattern recognition; mathematical theory of intelligence systems; applied mathematical logic; applications of discrete mathematics and mathematical cybernetics to natural sciences and engineering. For scientists and specialists in areas of mathematical cybernetics, discrete mathematics, computer science an their applications.

ISBN 978-5-317-07402-9

Научное издание

Напечатано с готового оригинал-макета

Подписано в печать 23.05.2025 г. Формат 60x90 1/16. Усл.печ.л. 12,5. Тираж 100 экз. Заказ 069.
Издательство ООО “МАКС Пресс”. Лицензия ИД N 00510 от 01.12.99 г. 119992, ГСП-2, Москва, Ленинские горы, МГУ им. М.В. Ломоносова, 2-й учебный корпус, 527 к. Тел. 8(495)939-3890/91. Тел./Факс 8(495)939-3891.

Отпечатано в полном соответствии с качеством предоставленных материалов в ООО «Фотоэксперт»
109316, г. Москва, Волгоградский проспект, д. 42, корп. 5, эт. 1, пом. I, ком. 6.3-23Н

— $\rho_{a\leqslant b\leqslant c} \rightleftharpoons \{(a,a),(a,b),(a,c),(b,b),(b,c),(c,c)\}$;
— $\rho_{0\to a;1\to b;2\to c} \rightleftharpoons \{(0,a),(1,b),(2,c)\}$;
— $\rho_{0\to a;1\to\forall} \rightleftharpoons \{(0,a),(1,0),(1,1),(1,2)\}$;
— $\rho_{0\to a,b;1\to\forall} \rightleftharpoons \{(0,a),(0,b),(1,0),(1,1),(1,2)\}$.

Пусть $\sigma_2 \rightleftharpoons \rho_{0\to 1;1\to 1;2\to 2}$, $\sigma_8 \rightleftharpoons \rho_{0\to 2;1\to 1;2\to 0}$. Автор установил следующие теоремы.

Теорема 3. $[\{b_2\}] = \mathrm{Pol}(\rho^{0,1}_{1in3}, \rho_{0\to 1;1\to\forall}, \rho_{0\to 2;1\to\forall}, \rho_{0\to 1,2;1\to\forall}, \rho_{same\to 1;2}, \rho_{\sigma_2}, \{2\})$.

Теорема 4. $[\{b_7\}] = \mathrm{Pol}(\rho^{0,1}_{1in3}, \rho^{0,1}_{1in3,2\to 2}, \rho_{same\to 0;2}, \rho_{0\leqslant 2\leqslant 1}, \{2\})$.

Теорема 5. $[\{b_8\}] = \mathrm{Pol}(\rho^{0,1}_{1in3}, \rho_{0\leqslant 1\leqslant 2}, \rho_{\sigma_8})$.

Из данного предикатного задания, в частности, следует, что минимальные клоны $[\{b_2\}], [\{b_7\}], [\{b_8\}]$ предикатно описуемы.

Список литературы

[1] Post E. L. The two-valued iterative systems of mathematical logic // Annals of Mathematics Studies. 1941. Princeton, New Jersey : Princeton University Press.

[2] Rosenberg I. G. Minimal clones I: the five types // Lectures in universal algebra. Amsterdam : North-Holland, 1986. P. 405–427.

[3] Csákány B. All minimal clones on the three-element set // Acta Cybernetica. 1983. Vol. 6, no. 3. P. 227–238.

Эффективная реализация квантового хеширования

Зиннатуллин Илнар Гумарович, Хадиев Камиль Равилевич
Казанский (Приволжский) федеральный университет; Казанский физико-технический институт имени Е. К. Завойского ФИЦ Казанский научный центр РАН;
IlnGZinnatullin@kpfu.ru, kamilhadi@gmail.com

В данной работе рассматривается эффективная реализация квантового хеширования. Квантовое хеширование позволяет проектировать эффективные по памяти квантовые алгоритмы и строить защищенные коммуникационные протоколы. Мы предлагаем алгоритм, позволяющий балансировать между числом CNOT-гейтов (глубиной схемы) и точностью углов поворота. Современные квантовые вычислители являются устройствами NISQ (Noisy Intermediate-Scale Quantum) эры и чувствительны к точности углов.

Квантовое хеширование

Квантовое хеширование впервые было определено в [1]. В данной работе рассматриваются амплитудная [1] и фазовая [2] формы квантового хеширования. В общем случае для $x \in \mathbb{Z}_q$ n-кубитный хеш определяется как $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \left(R_a\left(\theta_j\right)|q_n\rangle\right)$, где $\theta_j = \frac{4\pi s_j x}{q}$ и $S = \{s_0, \ldots, s_{d-1}\} \subseteq \mathbb{Z}_q$ — набор параметров такой, что $\frac{1}{d}\left|\sum_{j=0}^{d-1} e^{i\frac{2\pi s_j x}{q}}\right| \leqslant \varepsilon$. Заметим, что $n = \log d + 1$ и $d = O\left(\frac{\log q}{\varepsilon^2}\right)$. Для амплитудной формы $a = y$, т. е. используются повороты вокруг оси y, и $|q_n\rangle = |0\rangle$. Для фазовой формы $a = z$, т. е. используются повороты вокруг оси z, и $|q_n\rangle = |1\rangle$.

Схема для реализации квантового хеширования

Схема для реализации квантового хеширования представлена на рисунке 1. Кроме всего прочего, она состоит из n-кубитных контролируемых поворотов целевого n-го кубита вокруг оси a, в которых первые $n-1$ кубитов задействованы в качестве контролирующих. Структура схемы такова, что повороты осуществляются, используя всевозможные состояния контролирующих кубитов. Такая группа гейтов называется оператором равномерно контролируемого поворота UCR_a^{n-1} (uniformly controlled rotation). Наша задача сводится к эффективному разложению гейта UCR_a^{n-1}.

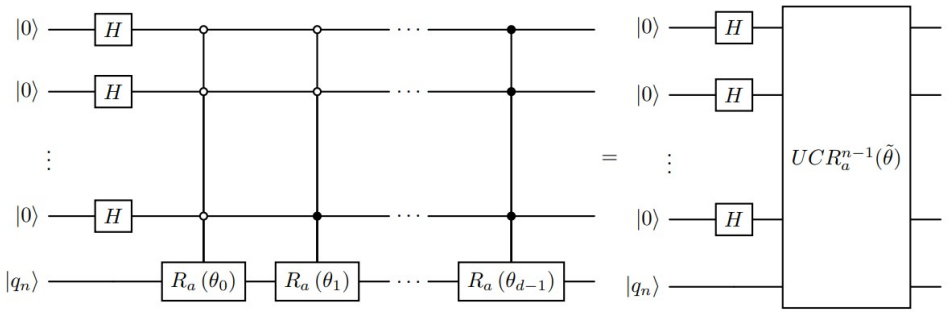

Рис. 1: Схема для реализации квантового хеширования.

Оптимизация схемы

Существует эффективная декомпозиция UCR_a^{n-1}, изложенная в работе [3]. Она может быть получена путём рекурсивного применения схемы, представленной на рисунке 2. В этом случае для декомпозиции требуется d CNOT-гейтов и d R_a-гейтов с точностью углов поворота $O\left(\frac{1}{d2^d}\right)$. Видим, что здесь фигурируют более чувствительные углы, так как изначальная точность была $O\left(\frac{1}{2^d}\right)$.

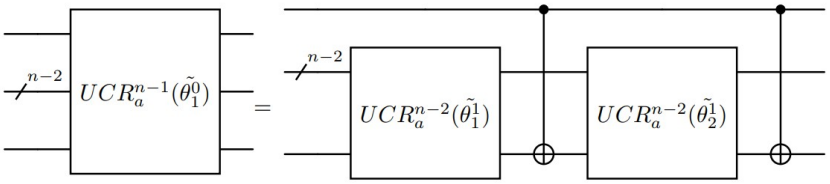

Рис. 2: Шаг рекурсивной декомпозиции UCR_a^{n-1}.

Рассмотрим вспомогательную конструкцию, которая пригодится нам дальше. Используя разложение [4, лемма 7.9], осуществляем декомпозицию контролируемых поворотов, представленную на рисунке 3. Стоит отметить, что эта схема симметрична относительно вертикальной оси. Данная декомпозиция примечательна тем, что для дальнейшего разложения контролируемых отрицаний $C^{n-2}(X)$ кубит с номером $n-1$ можно использовать в качестве анциллы. Известно [4], что в этом случае требуется $24l-52$ CNOT-гейтов, где l — число контролирующих кубитов.

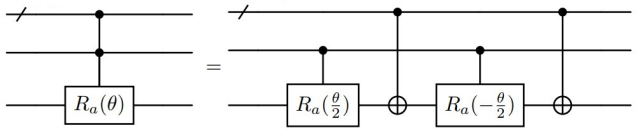

Рис. 3: Декомпозиция контролируемого поворота вокруг оси a.

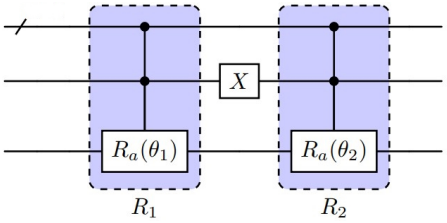

Рис. 4: Фрагмент схемы, реализующей UCR_a^{n-1}.

Нами предлагается применить к исходному гейту UCR_a^{n-1} рекурсивно k раз схему, изображенную на рисунке 2. После k итераций получаем схему, содержащую 2^k CNOT-гейтов и 2^k UCR_a^{n-k-1} гейтов. Точность углов поворота при этом возрастает до $O\left(\frac{1}{2^{d+k}}\right)$. Далее для гейта UCR_a^{n-k-1} строим разложение, в котором осуществляем перебор контролируемых поворотов, используя код Грея. Использование кода Грея удобно тем, что соседние кодовые слова отличаются ровно в одной позиции, поэтому переход из одного состояния контролирующих кубитов в другой осуществляется путём применения одного отрицания. Различающаяся позиция определяет номер кубита, к которому применяется отрицание.

Далее в получившейся схеме можно выделить 2^{n-k-2} фрагментов, изображенных на рисунке 4. Здесь мы для гейта R_1 применяем декомпозицию, представленную на рисунке 3, а для гейта R_2 зеркальное отображение этой же декомпозиции. В итоге получаем схему, которая представлена на рисунке 5. Легко заметить, что обрамленные в рамку контролируемые отрицания гасят друг друга.

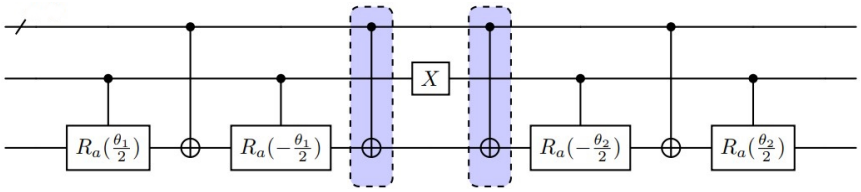

Рис. 5: Декомпозиция схемы на рис. 4.

Таким образом, общее число CNOT-гейтов равно $2^k + 2^{n-1}(24(n-k)-97)$ или $2^k + d(24(\log d - k) - 73)$. Отметим, что $k \leqslant n - 5 = \log d - 4$. При увеличении k глубина схемы уменьшается от $O(\log q \log\log q)$ до $O(\log q)$, однако точность углов повышается от $O\,(1/q)$ до $O\,(1/(q \log q))$.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00406, `https://rscf.ru/project/24-21-00406/`.

Список литературы

[1] Ablayev F. M., Vasiliev A. V. Cryptographic quantum hashing // Laser Physics Letters. 2013. Vol. 11, no. 2. P. 753–757.

[2] Vasiliev A. Quantum hashing for finite abelian groups // Lobachevskii Journal of Mathematics. 2016. Vol. 37, no. 6. P. 753–757.

[3] Quantum circuits for general multiqubit gates / M. Möttönen, J. J. Vartiainen, V. Bergholm, M. M. Salomaa // Physical Review Letters. 2004. Vol. 93, no. 13. P. 130502.

[4] Elementary gates for quantum computation / A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter // Physical Review A. 1995. Vol. 52, no. 5. P. 3457.

Выбор оптимального корня для корневых ориентированных деревьев

Иорданский Михаил Анатольевич
Нижегородский государственный педагогический университет имени Козьмы Минина;
Нижегородский государственный университет имени Н. И. Лобачевского; iordanski@mail.ru

Постановка задачи

Пусть $t(V, E)$ — дерево, содержащее n вершин, $A = \{1, 2, \ldots, n\}$ — множество из n натуральных чисел. Взаимно однозначное отображение $\varphi : V(t) \to A$ называется *нумерацией* вершин дерева $t(V, E)$. При этом каждой вершине $v_i \in V(t)$ ставится в соответствие номер $\varphi(v_i) \in A$, каждому ребру $e = (v_i, v_j)$ — число $\Delta_e^{\varphi} = \mid \varphi(v_i) - \varphi(v_j) \mid$, а всему дереву $t(V, E)$ соответствует сумма $\Delta^{\varphi}(t) = \sum_{(v_i, v_j) \in E(t)} \mid \varphi(v_i) - \varphi(v_j) \mid$, где суммирование производится по всем ребрам дерева $t(V, E)$. Величина $\Delta^{\varphi}(t)$ задает *длину* дерева $t(V, E)$ на