

Lapshin Vyacheslav Sergeevich – e-mail: lapshin@sfedu.ru; phone: +79525690073; the department of system analysis and telecommunications; cand. of eng. sc.; senior lecturer.

Lipko Yuliya Yur'evna – e-mail: ylipko@sfedu.ru; phone: +79185566893; the department of system analysis and telecommunications; cand. of eng. sc.; associate professor.

Sviridov Alexandr Slav'evich – e-mail: asviridov@sfedu.ru; phone: +79185567529; the department of system analysis and telecommunications; cand. of eng. sc.; associate professor.

УДК 004.032

DOI 10.18522/2311-3103-2022-5-141-151

С.М. Гушанский, В.С. Потапов

ИССЛЕДОВАНИЕ КВАНТОВОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ И РЕАЛИЗАЦИЯ КВАНТОВОГО ЯДРА НА ПЛИС

Метод квантового ядра является одним из важнейших методов в квантовом машинном обучении. Однако количество признаков, используемых для квантовых ядер, ограничено несколькими десятками признаков. Используется структура состояния блочного продукта в качестве карты квантовых признаков и демонстрируется реализация программируемых вентиляционных матриц. Актуальность данных исследований заключается в математическом и программном моделировании и реализации квантовой вычислительной системы в рамках разработки реализации квантового ядра на ПЛИС для решения классов задач классического характера. Научная новизна данного направления исследований заключается в разработке гибридного симулятора квантового ядра центрального процессорного устройства (ЦПУ) и программируемой логической интегральной схемы (ПЛИС) на несколько порядков быстрее, чем обычный симулятор квантовых вычислений. Эта совместная разработка реализованного квантового ядра и его эффективная реализация ПЛИС позволили выполнить численное моделирование квантового ядра на основе вентилях с точки зрения входных признаков, вплоть до 780-мерных признаков с использованием 4000 выборок. Применили квантовое ядро к задачам классификации изображений с использованием набора данных Fashion-MNIST и показали, что квантовое ядро сравнимо с ядрами Гаусса с оптимизированной пропускной способностью. Проведенный анализ работ данной области показал, что в настоящее время достигнут новый качественный уровень, открывающий перспективные возможности по реализации многокубитовых квантовых вычислений. Перспективы реализации и развития связаны не только с технологическими возможностями, но и с решением вопросов построения эффективных квантовых систем решения актуальных математических задач, задач криптографии и задач управления (оптимизации).

Моделирование; квантовый алгоритм; кубит; модель квантового вычислителя; запутывание; суперпозиция; квантовый оператор.

S.M. Gushanskiy, V.S. Potapov

STUDY OF A QUANTUM COMPUTING SYSTEM AND IMPLEMENTATION OF A QUANTUM CORE ON FPGA

The quantum core method is one of the most important methods in quantum machine learning. However, the number of features used for quantum nuclei is limited to a few dozen features. The block product state structure is used as a quantum feature map and the implementation of programmable gate matrices is demonstrated. The relevance of these studies lies in the mathematical and software modeling and implementation of a quantum computing system as part of the development of the implementation of a quantum core on FPGA for solving classes of problems of a classical nature. The scientific novelty of this research area is the development of a hybrid simulator of the quantum cores of a central processing unit (CPU) and a programmable logic integrated circuit (FPGA) several orders of magnitude faster than a conventional quantum computing simulator. This joint development of the implemented quantum core and its efficient FPGA imple-

mentation allowed numerical simulation of the quantum core based on gates in terms of input features, up to 780-dimensional features using 4000 samples. We applied the quantum kernel to image classification problems using the Fashion-MNIST dataset and showed that the quantum kernel is comparable to Gaussian kernels with optimized throughput. The analysis of the work in this field has shown that a new qualitative level has now been reached, opening up promising opportunities for the implementation of multi-qubit quantum computing. The prospects for implementation and development are connected not only with technological capabilities, but also with solving the issues of building effective quantum systems for solving actual mathematical problems, cryptography problems and control (optimization) problems.

Modeling; quantum algorithm; qubit; model of a quantum computer; entanglement; superposition; quantum operator.

Введение. Квантовые вычисления [1] – перспективная технология, способная трансформировать многие области промышленности и научных исследований, включая финансы, химию и машинное обучение [2] (МО). В то время как ранние отказоустойчивые квантовые вычисления были продемонстрированы недавно [3], поиски практического использования существующих шумных квантовых процессоров (ШКП) были активной областью исследований [4]. В настоящее время процессоры ШКП доступны через различные облачные платформы квантовых вычислений [5] с ~ 10 –100 физических кубитов [6]. Устройства ШКП по своей природе подвержены ошибкам, и ряд алгоритмов ШКП был предложен в рамках гибридного квантово-классического подхода [7, 8]. Метод квантового ядра является одним из наиболее важных алгоритмов КМО и подходит для устройств ШКП с неглубокими квантовыми схемами [9]. Недостатком вычисления квантового ядра является необходимость проведения ряда измерений для получения элементов квантового ядра [10] с помощью $O(N^4 / \epsilon^2)$ операций, где N обозначает количество выборок данных, а ϵ максимальную ошибку. Такая вычислительная сложность становится недопустимой при разработке и проверке квантовых ядер по мере роста N . Кроме того, количество запутывающих кубитов с различной связностью в ранее предложенных квантовых ядрах увеличивается с увеличением количества кубитов, что требует дополнительных вычислительных ресурсов. Чтобы преодолеть вышеуказанные проблемы, введем неглубокую квантовую схему с фиксированной глубиной, которую можно применить к квантовому ядру для большего количества входных функций.

1. Схематическое представление квантового симулятора с использованием гибридного подхода. В настоящее время большинство исследователей используют симуляторы квантовых вычислений на классических платформах; по этой причине были предприняты значительные усилия по разработке симуляторов квантовых вычислений [11]. Среди аппаратных реализаций программируемые вентильные матрицы являются одной из желательных платформ, поскольку ПЛИС обладает свойствами эффективного параллелизма, малой задержки и модификации блоков. Такие свойства особенно подходят для нашего квантового ядра, состоящего из неглубокой квантовой цепи. Здесь совместно разрабатываем нашу архитектуру ПЛИС [12] и квантовое ядро с неглубокой квантовой схемой, что позволяет проводить эффективные численные эксперименты с квантовым ядром. ПЛИС успешно применяется к отказоустойчивым квантовым алгоритмам [13], таким как алгоритм Гровера [14], квантовое преобразование Фурье [15] и алгоритм Дойча [16]. Однако реализация ПЛИС, разработанная для конкретного алгоритма ШКП, в значительной степени не исследована, и настоящее исследование является первой демонстрацией симулятора квантового ядра на основе вентилей с использованием платформы ПЛИС, что позволяет проверить применимость модели КМО с помощью сотни входных функций. Оставшаяся часть теста организована следующим образом. Предоставляем краткое введение в машину опорных векторов и описываем нашу кар-

ту квантовых признаков, основанную на неглубокой квантовой схеме с фиксированной глубиной. В дополнение к такой структуре разрабатываем квантовый симулятор, используя гибридный подход ЦПУ – ПЛИС. Затем реализация квантового ядра ПЛИС проверяется с точки зрения численной точности и ускорения. Применяем симулятор квантового ядра для бинарной и многоклассовой классификации [17] для ряда входных функций с использованием набора данных Fashion-MNIST.

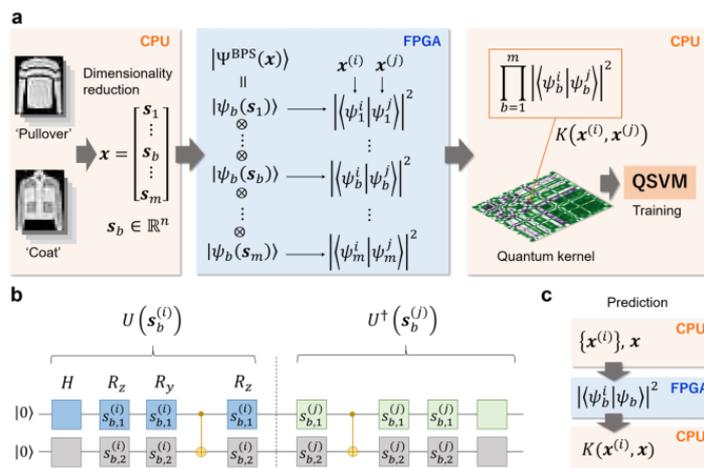


Рис. 1. Схематическое представление квантового симулятора с использованием гибридного подхода

На рис. 1 отображено схематическое представление квантового симулятора. ПК используется для уменьшения размерности исходных данных из Fashion-MNIST, ряд признаков от $d = 4$ до $d = 780$ можно использовать для машинного обучения. Затем функции, уменьшенные с помощью ПК, отправляются из ЦП в ПЛИС. Вычисляем квадрат нормы скалярных произведений для каждой блочной волновой функции $|\psi_b\rangle$ карты квантовых признаков. Этот процесс повторяется для всех пар точек данных (т.е. $N^2 / 2$ раза). Затем данные отправляются обратно в ЦП. Значение матрицы ядра можно получить путем умножения блоков m . После того, как все элементы квантового ядра вычислены, алгоритм выполняется на процессоре. Для запутывающего вентиля используется вентиль CNOT.

2. Квантовое ядро, использующее структуру состояния блочного произведения. Метод квантового ядра является одним из наиболее важных алгоритмов в методах квантового машинного обучения [18]. В классическом методе ядра скалярное значение карты признаков представлен функциями ядра, которые неявно используют гильбертово пространство; с другой стороны, квантовое ядро явно определяет карту квантовых признаков с помощью квантового состояния $|\phi(x)\rangle$ для d -мерных входных векторов $x \in R^d$. Матрица квантового ядра $K(x, x')$ может быть оценена путем вычисления скалярного произведения карты квантовых признаков:

$$K(x, x') = |\langle \phi(x) | \phi(x') \rangle|^2. \quad (1)$$

Для бинарной классификации можно получить классификатор опорных векторов, который оценивает метку для новых данных x :

$$y = \text{sgn}\left(\sum y_i \alpha_i^* K(x^{(i)}, x) + b^*\right), \quad (2)$$

где $y_i \in \{+1, -1\}$, а параметры $\{\alpha_i^*\}$ и b^* – оптимальные параметры, полученные на этапе обучения. В гибридном квантово-классическом алгоритме фаза обучения [19] может выполняться на классических компьютерах, тогда как элементы квантового ядра могут быть вычислены компьютерами или симуляторами квантовых вычислений. Вычисление квантового ядра требует ряда квантовых измерений [20], чтобы получить запись квантового ядра со статистически достоверной точностью. Такая вычислительная сложность не позволяет разрабатывать и проверять квантовые ядра по мере роста количества выборок данных. Чтобы решить эти проблемы, введем неглубокую квантовую схему с фиксированной глубиной, которую можно применить к квантовому ядру для большего количества входных функций. В ранее предложенных квантовых ядрах [21], основанных на мгновенном квантовом полиноме, количество размерных признаков обычно устанавливается равным количеству квантовой запутанности. Это приводит к ухудшению производительности обобщения по мере увеличения количества кубитов. Цель подхода – упростить карту квантовых признаков, ограничить степень запутанности кубитов и контролировать емкость модели, увеличивая при этом количество входных признаков. Эта структура может обрабатывать несколько сотен входных функций. Для n -мерного входа вектор $x = [s_1, s_2, \dots, s_m]^T \in R^{mn}$, где s_b – m -мерный вектор $s_b = [s_{b,1}, s_{b,2}, \dots, s_{b,m}]^T$. Рассмотрим волновую функцию состояния блочного произведения:

$$|\Psi^{BPS}(x)\rangle = |\psi_1(s_1)\rangle \otimes |\psi_2(s_2)\rangle \otimes \dots \otimes |\psi_m(s_m)\rangle. \quad (3)$$

3. Симулятор квантового ИИ с использованием гибридного подхода ЦПУ-ПЛИС. Совместно разработав архитектуру ПЛИС и квантовое ядро, заданное неглубокой квантовой схемой, реализовали быстрый и эффективный симулятор, используя подход гетерогенных вычислений [22] (рис. 1,а). Для начала с помощью метода главных компонент провели уменьшение размерности данных изображения 28×28 из набора данных Fashion-MNIST, количество входных признаков можно варьировать от $d = 4$ до $d = 780$. После получения редуцированных входных векторов $x^{(i)} \in R^d$ входные данные отправляются из процессора во внутреннюю память аппаратной части ПЛИС. Затем для каждой блочной волновой функции $|\psi_b(s_b)\rangle$ ($b = 1, \dots, m$) карты квантовых признаков вычисляем квадрат

нормы скалярных произведений $|\langle \psi_b^i | \psi_b^j \rangle|^2$ (что изображено на рис. 1,б) на архитектуре ПЛИС в следующей процедуре: во-первых, синус и косинус входных углов для квантовых вентилях вычисляются с использованием алгоритма COordinate Rotational DIgital Computer (CORDIC) [23]. Во-вторых, квадрат нормы скалярного произведения можно вычислить, используя унитарные матрицы в уравнении (4) вместе с эффективной реализацией n -кубитной запутанности. Этот процесс можно повторить для всех пар выборок данных, а именно для $N^2/2$ циклов. Обработанные, действительные данные отправляются обратно в ЦП. Таким образом, матричный элемент ядра будет вычисляться путем умножения m блоков. После того, как все записи ядра будут получены, этап обучения может быть выполнен на платформе ЦП.

4. Разработка квантового ядра на ПЛИС. Начнем со сравнения значений квантового ядра, полученных платформой ПЛИС, и значений, полученных платформой ЦПУ (рис. 2,а–с). В силу ортонормированности волновых функций нормы скалярных произведений $|\langle \psi_b^i | \psi_b^j \rangle|^2$ имеют значения от 0 до 1. Такое свойство

наряду с малой глубиной схемы поддается использование 16-битной арифметики с фиксированной запятой в архитектуре ПЛИС, что, в свою очередь, ускоряет вычисления при эффективном использовании аппаратного обеспечения. Чтобы проверить реализацию ПЛИС, также использовали 64-битную арифметику с плавающей запятой на платформе ЦП. График четности указывает на успех нашей реализации квантового ядра ПЛИС (рис. 2с). Численное отклонение между двумя аппаратными платформами составляло $\pm\sim 0,095\%$, что указывает на незначительную потерю числовой точности.

Далее сравниваем время выполнения, вычисленное платформой ПЛИС, с временем, полученным реализацией ЦП, а также со временем, полученным Qiskit Aer [24], симулятором квантовых вычислений (рис. 2,d). В реализации после отправки данных в архитектуру ПЛИС используем только внутреннюю память оборудования ПЛИС без использования внешней памяти, что позволяет избежать связанных с этим коммуникационных издержек. В архитектуре ПЛИС все записи ядра вычислялись за 4,1 мс при $N = 1000$; а время выполнения, включая накладные расходы на связь между ЦП и ПЛИС, составило 15,4 мс при $N = 1000$. Другими словами, реализация ПЛИС достигла улучшения в 1784 раза по сравнению с аналогом на ЦП.

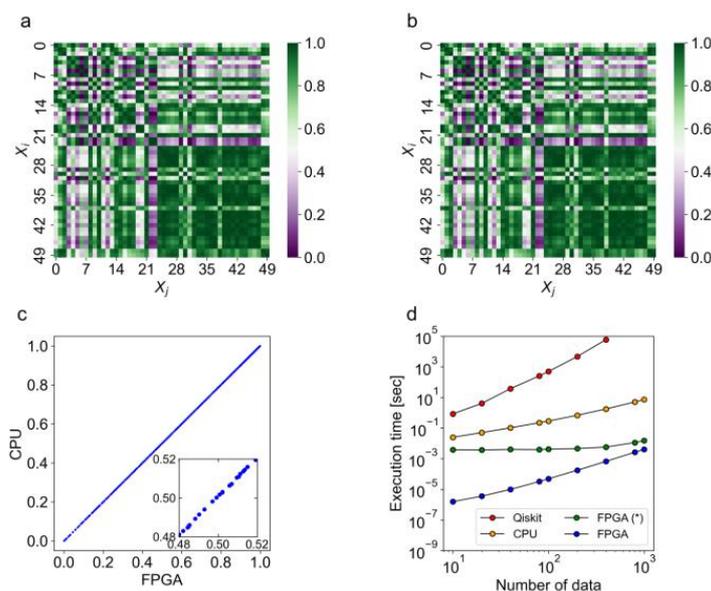


Рис. 2. ПЛИС реализация квантового ядра и время его выполнения. Численное моделирование было выполнено на квантовой схеме с 6 кубитами, которая оценивает элемент квантового ядра

А также время выполнения, включая коммуникационные накладные расходы, было в 472 раза быстрее (рис. 2,г); к тому же по сравнению с выполнением на симуляторе Qiskit Aer (где стоимость вычислений растет как $O(N^4 / \epsilon^2)$ операций) ускорение в 10 млн. раз было достигнуто при $N = 400$ (рис. 2,г). Результаты показывают, что реализация ПЛИС очень эффективна с точки зрения количества выборок данных, при этом в карте квантовых признаков используется небольшое количество запутывающих кубитов (до 6 кубитов). Симулятор на основе ПЛИС ускоряет численное моделирование с использованием квантового ядра и позволяет проверить его применимость к гораздо более крупным функциям методов квантового ядра.

а) Матрица квантового ядра, полученная платформой ПЛИС (16-битная арифметика с фиксированной точкой); б) Матрица квантового ядра, полученная процессором; с) График четности для значений квантового ядра, полученных ЦП и платформы ПЛИС. На вставке показаны небольшие различия между ними: ошибка между двумя аппаратными платформами составила $\pm \sim 0,095\%$; д) Время выполнения по количеству данных N для разных платформ: ПЛИС, синий; ПЛИС (включая накладные расходы на связь между ЦП и ПЛИС; обозначено звездочкой), зеленый; процессор, оранжевый; Qiskit Aer (квантовый симулятор), красный. Опишем подход для эффективного моделирования квантового ядра, специально разработанного для архитектуры ПЛИС. Квантовое ядро задается внутренним произведением карты квантовых признаков, что в принципе требует $O(2^{3n})$ операций из-за умножения матриц $2^n \times 2^n$ для создания карты квантовых признаков. Такая вычислительная сложность становится непосильной для эффективной реализации квантовых ядер ПЛИС, поскольку архитектура ПЛИС привязана к памяти, а количество сложных множителей ограничено. По этой причине эффективное использование ресурсов ПЛИС имело решающее значение для расчета нашего квантового ядра. В работе использовали неглубокую квантовую схему, чтобы иметь возможность вычислить квантовое ядро с помощью $O(2^n)$ операций, как увидим ниже. Это позволило эффективно распараллелить и использовать внутреннюю память в ПЛИС. Рассмотрим следующее квантовое состояние:

$$|\psi\rangle = (V_1 \otimes V_2 \otimes \dots \otimes V_n) U_{2^n}^{ent} (U_1 \otimes U_2 \otimes \dots \otimes U_n) |0^{\otimes n}\rangle, \quad (4)$$

где U_1, U_2, \dots, U_n и V_1, V_2, \dots, V_n – однокубитные вентили, а $U_{2^n}^{ent} = \prod_{q=1}^{n-1} CNOT_{q,q+1}$

представляет n-операция запутывания кубитов. Для нашего обсуждения удобно переписать $|\psi\rangle$ как $f = V U_{2^n}^{ent} U f_0$, где f_0 – вектор $[1, 0, \dots, 0]^T$, где $U = U_1 \otimes \dots \otimes U_n$ и $V = V_1 \otimes \dots \otimes V_n$. Во-первых, отметим, что при вычислении $U f_0$ нужен только первый столбец U ; следовательно, $U f_0$ можно получить без необходимости полностью проводить тензорные операции. Обозначим первый вектор-столбец каждой 2×2 унитарная матрица U_q как $[\chi_1^{(q)}, \chi_2^{(q)}]^T$ имеют первый вектор-столбец U как $u = [u_1, u_2, \dots, u_{2^n}]^T \in C^{2^n}$.

$$U f_0 = u = \begin{bmatrix} \chi_1^{(1)} \cdot \dots \cdot \chi_1^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_1^{(n)} \\ \chi_1^{(1)} \cdot \dots \cdot \chi_1^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_2^{(n)} \\ \chi_1^{(1)} \cdot \dots \cdot \chi_1^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_1^{(n)} \\ \chi_1^{(1)} \cdot \dots \cdot \chi_1^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_2^{(n)} \\ \chi_2^{(1)} \cdot \dots \cdot \chi_2^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_1^{(n)} \\ \chi_2^{(1)} \cdot \dots \cdot \chi_2^{(n-2)} \cdot \chi_1^{(n-1)} \cdot \chi_2^{(n)} \\ \chi_2^{(1)} \cdot \dots \cdot \chi_2^{(n-2)} \cdot \chi_2^{(n-1)} \cdot \chi_1^{(n)} \\ \chi_2^{(1)} \cdot \dots \cdot \chi_2^{(n-2)} \cdot \chi_2^{(n-1)} \cdot \chi_2^{(n)} \end{bmatrix}. \quad (5)$$

Это вычисление можно выполнить с помощью $4 \cdot (2^{n-1} - 1)$ операций с использованием комплексных множителей в ПЛИС. Таким образом, карту признаков можно переписать как $f = VU_{2^n}^{ent} u$. Далее отметим, что V – диагональная матрица в квантовой схеме, а U^{ent} – разреженная матрица, в которой каждый вектор-строка содержит только один ненулевой элемент. Обозначая диагональные элементы $\{V_{kk}\}$ как $v = [v_1, v_2, \dots, v_{2^n}]^T \in \mathbb{C}^{2^n}$, можем вычислить f как $f_k = v_k u_{\xi_k}$. Здесь ξ_k – индекс ненулевого элемента в k -й строке U^{ent} (например, при $n = 2$ $\xi_1 = 1, \xi_2 = 2, \xi_3 = 4, \xi_4 = 3$). Индексы $\{\xi_k\}$ в уравнении (5) можно определить после получения U^{ent} . Наконец, внутренний продукт $\langle \psi^i | \psi^j \rangle$ можно рассчитать как $\sum_k f_k^*(s^{(i)}) f_k(s^{(j)})$. Квантовый симулятор на основе гибридной системы реализован на облачной платформе Amazon Web Services (AWS) [25], в которой доступны экземпляры Amazon EC2 F1 оборудования Xilinx FPGA [26].

5. Сравнение вычислительной сложности пяти классических и квантовых методов для решения транспортной задачи коммивояжера. Сравним сложность пяти классических методов и пяти квантовых методов для решения алгоритма оптимизации. Все изученные алгоритмы были основаны на стандартном подходе дискретизации уравнений с помощью метода конечных разностей, приводящего к системе линейных уравнений. В частности, мы использовали простой метод “прямое время, центральное пространство” (FTCS) с равномерной прямоугольной сеткой. Мы оценили следующие классические алгоритмы:

- ◆ Решение системы линейных уравнений с использованием метода сопряженных градиентов.
 - ◆ Итерация вперед во времени от начального условия.
 - ◆ Использование быстрого преобразования Фурье для решения линейной системы.
 - ◆ Метод случайного блуждания, основанный на связи между уравнением теплопроводности и случайным блужданием по сетке.
- Ускоренная версия метода случайного блуждания, использующая эффективную выборку из биномиального распределения.
- Мы также оценили следующие квантовые алгоритмы:
- ◆ Решение линейной системы с использованием самых быстрых квантовых алгоритмов для решения линейных уравнений.
 - ◆ Диагонализация линейной системы с использованием квантового преобразования Фурье и последующего выбора.
 - ◆ Когерентное ускорение случайного блуждания по сетке.
 - ◆ Применение оценки амплитуды к классическому случайному блужданию по сетке.
 - ◆ Применение оценки амплитуды к быстрому классическому алгоритму случайного блуждания.

Эти методы различаются по своей гибкости. Например, методы квантовых и классических линейных уравнений могут быть применены к гораздо более общим граничным условиям и пространственным областям, тогда как методы быстрого преобразования Фурье и когерентной диагонализации непосредственно применимы только к решению уравнения теплопроводности в простой области. Результаты обобщены в табл. 1, где показываем время выполнения в терминах ϵ , хотя вычислена сложность различных алгоритмов с точки зрения других параметров, подробно описанных ниже.

Таблица 1

Время выполнения алгоритмов для решения транспортной задачи коммивояжера с точностью ϵ в пространственном измерении d , только в терминах ϵ и d . O обозначение скрывает полилогарифмические множители

	Метод	$d = 1$	$d = 2$	$d = 3$	$d \geq 4$
Квантовые аналоги	Линейные уравнения	$O(e^{-2})$	$O(e^{-2.5})$	$O(e^{-3})$	$O(e^{-d/2-1.5})$
	Пошаговое управление временем	$O(e^{-1.5})$	$O(e^{-2})$	$O(e^{-2.5})$	$O(e^{-d/2-1})$
	Быстрое преобразование Фурье	$O(e^{-0.5})$	$O(e^{-1})$	$O(e^{-1.5})$	$O(e^{-d/2})$
	Случайное блуждание	$O(e^{-3})$	$O(e^{-3})$	$O(e^{-3})$	$O(e^{-3})$
	Быстрое случайное блуждание	$O(e^{-2})$	$O(e^{-2})$	$O(e^{-2})$	$O(e^{-2})$
Разработанное квантовое ядро	Линейные уравнения	$O(e^{-2.5})$	$O(e^{-2.5})$	$O(e^{-2.75})$	$O(e^{-d/4-2})$
	Ускорение когерентного случайного блуждания	$O(e^{-1.75})$	$O(e^{-2})$	$O(e^{-2.25})$	$O(e^{-d/4-1.5})$
	Когерентная диагонализация	$O(e^{-1.25})$	$O(e^{-1.5})$	$O(e^{-1.75})$	$O(e^{-d/4-1})$
	Оценка амплитуды случайного блуждания	$O(e^{-2})$	$O(e^{-2})$	$O(e^{-2})$	$O(e^{-2})$
	Быстрая оценка амплитуды	$O(e^{-1})$	$O(e^{-1})$	$O(e^{-1})$	$O(e^{-1})$

При $d = 1$ все квантовые методы на разработанном квантовом ядре превосходят квантовый метод быстрого преобразования Фурье. Для $d \geq 2$ самым быстрым методом является квантовый алгоритм, основанный на применении амплитудного усиления на разработанном квантовом ядре к “быстрому” квантовому случайному блужданию. Для произвольного d наибольшее квантовое ускорение при использовании этого метода составляет от $O(e^{-2})$ до $O(e^{-1})$.

Алгоритмы быстрого преобразования Фурье и быстрой оценки амплитуды случайного блуждания специфичны для прямоугольной области. Учитывая алгоритмы, которые также могут быть применены к более общим областям, самым быстрым квантовым методом для $d \leq 3$ является повторение начального условия вперед по времени на разработанном квантовом ядре. Это превосходит все квантовые методы при $d = 1$, выполняет примерно так же хорошо, как (стандартная) оценка амплитуды случайного блуждания при $d = 2$, и превосходит оценку амплитуды случайного блуждания при $d \geq 3$.

Заключение. В настоящее время активно развивается теория квантовых вычислений. Результаты, полученные в работе, имеют значение для разработки квантовых алгоритмов и проектирования квантовых ядер. Хотя квантовые вычисления еще не готовы к переходу от теории к практике, тем не менее, можно обоснованно догадываться какую форму, возможно, квантовая вычислительная система примет, или, что более важно для дизайна языка программирования, по какому интерфейсу можно будет взаимодействовать с таким квантовым компьютером. Естественно применить уроки, извлеченные из программирования классических вычислений к квантовым вычислениям.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-07-00916.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Квантовая криптография // Википедия. Дата обновления: 05.11.2022. – URL: <http://ru.wikipedia.org/?oldid=82377595> (дата обращения: 05.11.2022).
2. Трубицын А.А. Расчет траектории движения материальной точки в двумерном (осесимметричном) консервативном поле // Журнал вычислительной математики и математической физики. – 1990. – Т. 30, № 7. – P. 1113-1115; U.S.S.R. Comput. Math. Math. Phys. – 1990. – 30:4. – P. 107-109.
3. Arthur Trew (ed.), Greg Wilson (ed.). Past, Present, Parallel: A Survey of Available Parallel Computer Systems. – Springer, 1991. – 392 p. – ISBN 9783540196648.
4. Quantum phase estimation algorithm (2022, Nov 03). In Wikipedia, The Free Encyclopedia. Retrieved: 05:15, Nov 3, 2022, from https://en.wikipedia.org/w/index.php?Title=Quantum_phase_estimation_algorithm&oldid=731732789.
5. Richard G. Milner. A Short History of Spin // Contribution to the XVth International Workshop on Polarized Sources, Targets, and Polarimetry. – Charlottesville, Virginia, USA, September 9-13, 2013. – arXiv:1311.5016.
6. Гушанский С.М., Потапов В.С. Методика разработки и построения квантовых алгоритмов // Информатизация и связь. – 2017. – № 3. – С. 101-104.
7. Гушанский С.М. Поленов М.Ю., Потапов В.С. Реализация компьютерного моделирования системы с частицей в одномерном и двухмерном пространстве на квантовом уровне // Известия ЮФУ. Технические науки. – 2017. – № 3 (188). – С. 223-233.
8. Hales S. Hallgren. An improved quantum Fourier transform algorithm and applications // Proceedings of the 41st Annual Symposium on Foundations of Computer Science. November 12–14, 2000. – P. 515.
9. Potapov V., Gushanskiy S., Polenov M. The Methodology of Implementation and Simulation of Quantum Algorithms and Processes // 2017 11th International Conference on Application of Information and Communication Technologies (AICT). – Institute of Electrical and Electronics Engineers, 2017. – P. 437-441.
10. Lukin M.D. Attractive photons in a quantum nonlinear medium // Ofer Firstenberg, Nature. – October 2013. – Vol. 502.
11. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация = Quantum Computation and Quantum Information. – М.: Мир, 2006.
12. Quantum mechanics. In Wikipedia, The Free Encyclopedia. Retrieved 15:50, March 30, 2022. – URL: https://en.wikipedia.org/w/index.php?title=Quantum_mechanics&oldid=772744105.
13. Boneh D., Zhandry M. Quantum-secure message authentication codes // In Proceedings of Eurocrypt. – 2013. – P. 592-608.
14. Chris Ferrie. Quantum Physics for Babies // Sourcebooks Jabberwocky. – Brdbk edition, 2017-05-02. – P. 23-24.
15. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн. Алгоритмы: построение и анализ = Introduction to Algorithms. – 2-е изд. – М.: Вильямс, 2006. – 1296 с. – ISBN 0-07-013151-1.
16. Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V. Entanglement-assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem // IEEE Transactions on Information Theory. – 2002. – Vol. 48. – P. 2637-2655.
17. Kleppner D., Kolenkow R. An Introduction to Mechanics (Second ed.). – Cambridge: Cambridge University Press, 2014. – 49 p.
18. Потапов В.С., Гушанский С.М. Квантовые типы ошибок и методы их устранения, зависимость ошибки от меры и чистоты запутанности // Сб. трудов XIV Всероссийской научной конференции молодых ученых, аспирантов и студентов ИТСАНУ-2016. – Ростов-на-Дону: Изд-во ЮФУ, 2016. – Т. 3. – С. 123-129.
19. Olukotun K. Chip Multiprocessor Architecture – Techniques to Improve Throughput and Latency. – Morgan and Claypool Publishers, San Rafael, 2007.
20. Raedt K.D., Michielsen K., De Raedt H., Trieu B., Arnold G., Marcus Richter, Th Lip-pert, Watanabe H., and Ito, N. Massively parallel quantum computer simulator // Computer Physics Communications. – Vol. 176. – P. 121-136.
21. Williams C.P. Explorations in Quantum Computing // Texts in Computer Science. Chapter 2. Quantum Gates. – P. 51-122. – Springer, 2011.

22. Potapov V., Gushanskiy S., Guzik V., Polenov M. The Computational Structure of the Quantum Computer Simulator and Its Performance Evaluation // Software Engineering Perspectives and Application in Intelligent Systems. Advances in Intelligent Systems and Computing. – Vol. 763. – P. 198-207. – Springer, 2019.
23. Потанов В.С., Гушанский С.М. Разработка и исследование методики построения вычислительной квантовой системы с использованием аппаратных средств оптимизации // Информационные технологии и вычислительные системы. – 2022. – № 1. – С. 26-32.
24. Milner R.G. A Short History of Spin. In: Contribution to the XV International Workshop on Polarized Sources, Targets, and Polarimetry. – Charlottesville, Virginia, USA, September 9–13, 2013. – arXiv:1311.5016. – 2013.
25. Hallgren H.S. An improved quantum Fourier transform algorithm and applications // Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA. – P. 515. – IEEE, 2000.
26. Boneh D., Zhandry M. Quantum-secure message authentication codes // Proceedings of Eurocrypt. – 2013. – P. 592-608.

REFERENCES

1. Kvantovaya kriptografiya [Quantum Cryptography], *Vikipediya* [Wikipedia]. Update date: 05.11.2022. Available at: <http://ru.wikipedia.org/?oldid=82377595> (accessed 05 November 2022).
2. Trubitsyn A.A. Raschet traektorii dvizheniya material'noy toчки v dvumernom (osesimmetrichnom) konservativnom pole [Calculation of the trajectory of a material point in a two-dimensional (axisymmetric) conservative field], *Zhurnal vychislitel'noy matematiki i matematicheskoy fiziki* [Journal of Computational Mathematics and Mathematical Physics], 1990, Vol. 30, No. 7, pp. 1113-1115; U.S.S.R. Comput. Math. Math. Phys., 1990, 30:4, pp. 107-109.
3. Arthur Trew (ed.), Greg Wilson (ed.). Past, Present, Parallel: A Survey of Available Parallel Computer Systems. Springer, 1991, 392 p. ISBN 9783540196648.
4. Quantum phase estimation algorithm (2022, Nov 03). In Wikipedia, The Free Encyclopedia. Retrieved: 05:15, Nov 3, 2022, from https://en.wikipedia.org/w/index.php?Title=Quantum_phase_estimation_algorithm&oldid=731732789.
5. Richard G. Milner. A Short History of Spin, *Contribution to the XVth International Workshop on Polarized Sources, Targets, and Polarimetry*. Charlottesville, Virginia, USA, September 9-13, 2013. arXiv:1311.5016.
6. Gushanskiy S.M., Potapov V.S. Metodika razrabotki i postroeniya kvantovykh algoritmov [Methodology of development and construction of quantum algorithms], *Informatizatsiya i svyaz'* [Informatization and communication], 2017, No. 3, pp. 101-104.
7. Gushanskiy S.M. Polenov M.Yu., Potapov V.S. Realizatsiya komp'yuternogo modelirovaniya sistemy s chastitsey v odnomernom i dvukhmernom prostranstve na kvantovom urovne [Implementation of computer simulation of a system with a particle in one-dimensional and two-dimensional space at the quantum level], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 3 (188), pp. 223-233.
8. Hales S. Hallgren. An improved quantum Fourier transform algorithm and applications, *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*. November 12–14, 2000, pp. 515.
9. Potapov V., Gushanskiy S., Polenov M. The Methodology of Implementation and Simulation of Quantum Algorithms and Processes, *2017 11th International Conference on Application of Information and Communication Technologies (AICT)*. Institute of Electrical and Electronics Engineers, 2017, pp. 437-441.
10. Lukin M.D. Attractive photons in a quantum nonlinear medium, *Ofer Firstenberg, Nature*. October 2013, Vol. 502.
11. Nil'sen M., Chang I. Kvantovye vychisleniya i kvantovaya informatsiya = Quantum Computation and Quantum Information [Quantum computing and quantum information = Quantum Computation and Quantum Information]. Moscow: Mir, 2006.
12. Quantum mechanics. In Wikipedia, The Free Encyclopedia. Retrieved 15:50, March 30, 2022. Available at: https://en.wikipedia.org/w/index.php?title=Quantum_mechanics&oldid=772744105.
13. Boneh D., Zhandry M. Quantum-secure message authentication codes, *Proceedings of Eurocrypt*, 2013, pp. 592-608.

14. *Chris Ferrie*. Quantum Physics for Babies, *Sourcebooks Jabberwocky*. Brdbk edition, 2017-05-02, pp. 23-24.
15. *Tomas Kh. Kormen, Charl'z I. Leyzerson, Ronal'd L. Rivest, Klifford SHtayn*. Algoritmy: postroenie i analiz = Introduction to Algorithms [Algorithms: Construction and analysis = Introduction to Algorithms]. 2nd ed. Moscow: Vil'yams, 2006, 1296 p. ISBN 0-07-013151-1.
16. *Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V.* Entanglement-assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem, *IEEE Transactions on Information Theory*, 2002, Vol. 48, pp. 2637-2655.
17. *Kleppner D., Kolenkow R.* An Introduction to Mechanics (Second ed.). Cambridge: Cambridge University Press, 2014, 49 p.
18. *Potapov V.S., Gushanskiy S.M.* Kvantovye tipy oshibok i metody ikh ustraneniya, zavisimost' oshibki ot mery i chistoty zaputannosti [Quantum types of errors and methods of their elimination, the dependence of error on the measure and purity of entanglement], *Sb. trudov XIV Vserossiyskoy nauchnoy konferentsii molodykh uchenykh, aspirantov i studentov ITSAiU-2016* [Proceedings of the XIV All-Russian Scientific Conference of Young Scientists, graduate Students and students of ITSAiU-2016]. Rostov-on-Don: Izd-vo YuFU, 2016, Vol. 3, pp. 123-129.
19. *Olukotun K.* Chip Multiprocessor Architecture – Techniques to Improve Throughput and Latency. Morgan and Claypool Publishers, San Rafael, 2007.
20. *Raedt K.D., Michielsen K., De Raedt H., Trieu B., Arnold G., Marcus Richter, Th Lip-pert, Watanabe H., and Ito, N.* Massively parallel quantum computer simulator, *Computer Physics Communications*, Vol. 176, pp. 121-136.
21. *Williams C.P.* Explorations in Quantum Computing, *Texts in Computer Science. Chapter 2. Quantum Gates*, pp. 51-122. Springer, 2011.
22. *Potapov V., Gushanskiy S., Guzik V., Polenov M.* The Computational Structure of the Quantum Computer Simulator and Its Performance Evaluation, *Software Engineering Perspectives and Application in Intelligent Systems. Advances in Intelligent Systems and Computing*, Vol. 763, pp. 198-207. Springer, 2019.
23. *Potapov V.S., Gushanskiy S.M.* Razrabotka i issledovanie metodiki postroeniya vychislitel'noy kvantovoy sistemy s ispol'zovaniem apparatnykh sredstv optimizatsii [Development and research of a methodology for constructing a computational quantum system using optimization hardware], *Informatsionnye tekhnologii i vychislitel'nye sistemy* [Information technologies and computing systems], 2022, No. 1, pp. 26-32.
24. *Milner R.G.* A Short History of Spin. In: Contribution to the XV International Workshop on Polarized Sources, Targets, and Polarimetry. Charlottesville, Virginia, USA, September 9–13, 2013. arXiv:1311.5016, 2013.
25. *Hallgren H.S.* An improved quantum Fourier transform algorithm and applications, *Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA*, pp. 515. IEEE, 2000.
26. *Boneh D., Zhandry M.* Quantum-secure message authentication codes, *Proceedings of Eurocrypt*, 2013, pp. 592-608.

Статью рекомендовал к опубликованию д.ф.-м.н. Г.В. Куповых.

Гушанский Сергей Михайлович – Южный федеральный университет; e-mail: smgushanskiy@sfedu.ru; г. Таганрог, Россия; тел.: 88634371656; кафедра вычислительной техники; к.т.н.; доцент.

Потапов Виктор Сергеевич – e-mail: vpotapov@sfedu.ru; тел.: 88634371656; кафедра вычислительной техники; ассистент.

Gushanskiy Sergey Mikhailovich – Southern Federal University; e-mail: smgushanskiy@sfedu.ru; Taganrog, Russia; phone: +78634371656; the department of computer engineering; cand. of eng. sc.; associate professor.

Potapov Viktor Sergeevich – e-mail: vpotapov@sfedu.ru; phone: +78634371656; the department of computer engineering; assistant.