

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 519.7

<https://doi.org/10.26907/2541-7746.2025.1.115-124>Квантовый поиск в словаре на основе функции
отпечатков

Н.М. Салихова

Казанский (Приволжский) федеральный университет, г. Казань, Россия

Аннотация

Рассмотрена задача поиска элемента в словаре. В последние десятилетия были предложены различные подходы к решению этой проблемы, в том числе классические и квантовые алгоритмы. Метод квантового усиления амплитуды, который лежит в основе хорошо известного алгоритма Гровера, квадратично ускоряет процесс поиска.

Мы представляем новый подход к поиску элемента w длиной m в словаре V размером n , основанный на квантовой функции отпечатков. Наш алгоритм имеет запросную сложность $O(\sqrt{n})$ и использует $O(\log n + \log m)$ кубитов, тогда как алгоритмы, представленные в работах других авторов, используют $O(\log n + m)$ кубитов.

Ключевые слова: квантовый алгоритм, поиск элемента в словаре, квантовый поиск, код исправляющий ошибки, функция отпечатков

Для цитирования: Салихова Н.М. Квантовый поиск в словаре на основе функции отпечатков // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2025. Т. 167, кн. 1. С. 115–124.
<https://doi.org/10.26907/2541-7746.2025.1.115-124>.

ORIGINAL ARTICLE

<https://doi.org/10.26907/2541-7746.2025.1.115-124>

Quantum search in a dictionary using fingerprinting function

N.M. Salikhova*Kazan Federal University, Kazan, Russia***Abstract**

The problem of searching for an element within a dictionary was considered. Over the past decades, various approaches, including classical and quantum algorithms, have been proposed to solve it. One possible solution is the method of quantum amplitude amplification, which underpins the well-known Grover algorithm and enables a quadratic speedup in the search process.

In this article, a new approach to searching for an element w of length m in a dictionary V of size n with the use of the quantum fingerprinting function was introduced. The developed algorithm has a query complexity of $O(\sqrt{n})$ and requires $O(\log n + \log m)$ qubits.

Keywords: quantum algorithm, searching for element in dictionary, quantum search, error-correcting code, fingerprinting function

For citation: Salikhova N.M. Quantum search in a dictionary using fingerprinting function. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2025, vol. 167, no. 1, pp. 115–124. <https://doi.org/10.26907/2541-7746.2025.1.115-124>. (In Russian)

Введение

Проблемы поиска информации в базах данных хорошо известны в теоретической и прикладной информатике. Классический поиск в неотсортированном списке представляет собой алгоритм последовательного перебора элементов. Квантовый алгоритм поиска, который квадратично ускоряет поиск по сравнению с классическими алгоритмами, был предложен Л. Гровером в 1996 году [1] и был модифицирован в ряде последующих работ (см., например, [2, 3]). Разработка квантовых алгоритмов для поиска информации в базах данных продолжается и сегодня (см. [4, 5]).

Идея использования методов хеширования (универсального семейства хеш-функций) для поиска информации в неупорядоченной базе данных была представлена в 2024 году в работе [6]. В ней предложен гибридный классико-квантовый (вероятностно-квантовый) алгоритм для поиска подстроки длиной m в тексте длиной N . Доказано, что использование методов хеширования может экспоненциально сократить количество требуемых кубитов. В настоящей работе мы расширяем подход, представленный в [6], и предлагаем “чистый” квантовый алгоритм $\mathcal{A}$ для поиска определенного элемента длиной m в неупорядоченной коллекции из n объектов, каждый из которых имеет длину m . Ключевым отличием

предлагаемого алгоритма от алгоритма, представленного в [6], является использование квантовой хеш-функции, которая обеспечивает эффективность работы алгоритма по памяти: алгоритму требуется $O(\log n + \log m)$ кубитов для решения задачи. Количество обращений к оракулу оценивается как $O(\sqrt{n})$. Отметим, что для других известных на сегодняшний день алгоритмов поиска элемента длины m в неупорядоченной коллекции из n объектов требуется $O(\log n + m)$ кубитов.

1. Квантовая функция отпечатков

Квантовая функция ψ , представленная ниже, рассматривалась в работе [7], где называлась “квантовой функцией отпечатков”.

Коды, исправляющие ошибки. Код, исправляющий ошибки, определяется отображением $E : \Sigma^m \rightarrow \Sigma^l$ со следующим условием: для любых двух слов $w, w' \in \Sigma^m$ их отображения $E(w), E(w') \in \Sigma^l$ таковы, что расстояние Хэмминга $d(E(w), E(w'))$ между ними не меньше d . Такой код E называется (l, m, d) -кодом. В случае, когда $\Sigma = \{0, 1\}$, код называется двоичным кодом, исправляющим ошибки.

Для произвольного $d > 1$ существует (l, m, d) -код, исправляющий ошибки E , где $l = cm$, $c > 1$.

Квантовая функция ψ_E . Функция ψ_E определяется на основе бинарного (l, m, d) -кода, исправляющего ошибки E . Для $s = \log l$ функция $\psi_E : \{0, 1\}^m \rightarrow (\mathcal{H}^2)^{\otimes(s+1)}$ определяется следующим образом:

$$|\psi_E(w)\rangle = \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w)\rangle, \quad (1)$$

где $E_i(w)$ – i -й бит кодового слова $E(w)$.

Реализация функции ψ_E . Пусть $|0\rangle = |0\rangle^{\otimes(s+1)}$. Преобразование

$$U_{\psi_E} : |0\rangle \xrightarrow{w} (\mathcal{H}^2)^{\otimes(s+1)}$$

воздействует на $(s+1)$ кубитов.

Определим преобразование $U_{\psi_E}(w) = U_E(w)(H^{\otimes s} \otimes I)$ унитарной матрицей $2^{s+1} \times 2^{s+1}$. Это композиция преобразования Адамара $H^{\otimes s}$, единичного оператора I и преобразования U_E . Удобно определить преобразование U_E , описав его действие на 2^{s+1} векторах $|b\rangle$ вычислительного базиса $B = \{(0, \dots, 1), \dots, (1, \dots, 0)\}$ пространства $(\mathcal{H}^2)^{\otimes(s+1)}$. Аргументами преобразования U_E являются слова $w \in \{0, 1\}^m$:

$$U_E : |b\rangle \xrightarrow{w} |b'\rangle.$$

U_E определяется кодовым словом $E(w)$, длина которого равна $l = 2^s$. Содержательно: преобразование U_E “изменяет” состояние последнего $(s+1)$ -го кубита $|a\rangle$ базисного состояния $|b\rangle = |i\rangle \otimes |a\rangle$ на $|b'\rangle = |i\rangle \otimes |a \oplus E_i(w)\rangle$.

Свойство 1. Преобразование $U_{\psi_E}(w) = U_E(w)(H^{\otimes s} \otimes I)$ определяет функцию ψ_E . А именно, для любого слова $w \in \{0, 1\}^m$ верно следующее:

$$|\psi_E(w)\rangle = U_{\psi_E}(w)|0\rangle^{\otimes(s+1)} = \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w)\rangle.$$

Свойство 2. Преобразование $U_{\psi_E}^{-1}(w) = (H^{\otimes s} \otimes I) \otimes U_E(w)$ является обратным к $U_{\psi_E}(w)$.

Доказательство. Действительно, для произвольного слова $w \in \{0, 1\}^m$ и $(s+1)$ -кубитного состояния $|\psi_E(w)\rangle$ верно, что $U_{\psi_E}^{-1}(w)|\psi_E(w)\rangle = |0\rangle$:

$$\begin{aligned} \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w)\rangle &\xrightarrow{U_E(w)} \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w) \oplus E_i(w)\rangle = \\ &= \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle \otimes |0\rangle \xrightarrow{H^{\otimes s} \otimes I} |0\rangle^{\otimes(s+1)}. \end{aligned}$$

□

2. Алгоритм $\mathcal{A}$

Постановка задачи. Дано неупорядоченное множество V из n бинарных слов w_j , каждое длины m :

$$V = \{w_0, \dots, w_{n-1}\},$$

где $w_j \in \{0, 1\}^m$, $0 \leq j \leq n-1$.

Дано бинарное слово w длины m , где $m < n$. Требуется найти индекс вхождения слова w в множество V , а именно, такой индекс k , для которого $w = w_k$.

Алгоритм $\mathcal{A}$ состоит из двух частей:

А. Первая часть: подготовка начального состояния на основе V .

В. Вторая часть: считывание искомого слова w и поиск его позиции во множестве.

Описание алгоритма $\mathcal{A}$.

Входные данные. Для первой части: множество $V = \{w_0, \dots, w_{n-1}\}$ бинарных строк длины m . Для второй части: бинарная строка w длины m .

Выходные данные: индекс k , обозначающий номер элемента во множестве и такой, что $w = w_k$.

Таким образом, алгоритм $\mathcal{A}$ реализует отображение $\mathcal{A} : V, w \mapsto k$.

А. Первая часть алгоритма включает в себя подготовку начального состояния $|V, \psi_E\rangle$ на основе множества V с помощью преобразования U_{ψ_E} , определяющего квантовую функцию ψ_E :

$$|V, \psi_E\rangle = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |j\rangle \otimes |\psi_E(w_j)\rangle \otimes |1\rangle,$$

где

$$|\psi_E(w_j)\rangle = \frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w_j)\rangle.$$

В. Вторая часть алгоритма $\mathcal{A}$ состоит из считывания искомого слова w и поиска такой его позиции k , что $w = w_k$.

- Оператор $I^{\otimes \log n} \otimes U_{\psi_E}^{-1}(w) \otimes I$ применяется к состоянию $|V, \psi_E\rangle$:

$$\begin{aligned} |V, \psi_E, w\rangle &= \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |j\rangle \otimes \left(\frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle |E_i(w_j) \oplus E_i(w)\rangle \right) \otimes |1\rangle = \\ &= \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |j\rangle \otimes \left(\frac{1}{\sqrt{2^s}} \sum_{i=0}^{2^s-1} |i\rangle \otimes \left(\sum_{i: E_i(w_j)=E_i(w)} |0\rangle + \sum_{i: E_i(w_j) \neq E_i(w)} |1\rangle \right) \right) \otimes |1\rangle = \\ &= \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |j\rangle \otimes |\phi(w_j, w)\rangle \otimes |1\rangle, \end{aligned}$$

где $|\phi(w_j, w)\rangle = U_{\psi_E}^{-1}(w) |\psi_E(w_j)\rangle$ для $j \in \{0, \dots, n-1\}$.

- В состоянии $|V, \psi_E, w\rangle$ проводится поиск базовых состояний $|j\rangle |0\rangle^{\otimes s+1} |1\rangle$. Для этого применяется известная процедура “усиления амплитуды” (см., например, [2]). Процедура заключается в применении оператора QQ (4) — оператора итерации поиска. Число применений QQ определяется как запросная сложность алгоритма.
- Первые $\log n$ кубитов конечного состояния измеряются в вычислительном базисе. Результат измерения k объявляется позицией элемента w_k , для которого выполнено: $w_k = w$.

2.1. Характеристики алгоритма $\mathcal{A}$. Характеристики квантового алгоритма включают:

Вероятность успеха. Обозначим через $Pr_{success}(\mathcal{A})$ вероятность успешного завершения алгоритма $\mathcal{A}$.

Запросная сложность. Количество обращений $Q(\mathcal{A})$ к унитарному оператору QQ (оператор QQ итерации поиска, определяется в (4)) — это запросная сложность квантового алгоритма $\mathcal{A}$.

Сложность по памяти. Число $S(\mathcal{A})$ используемых кубитов является мерой сложности памяти квантового алгоритма $\mathcal{A}$.

3. Анализ алгоритма $\mathcal{A}$

Обозначим через $Pr_{success}(\mathcal{A})$ вероятность того, что результатом действия алгоритма $\mathcal{A}$ будет такое число k , что $w_k = w$.

Теорема 1. Для алгоритма $\mathcal{A}$, который ищет вхождение элемента длиной m в неупорядоченной последовательности из n элементов, верно

$$S(\mathcal{A}) = O(\log n + \log m), \quad Q(\mathcal{A}) = O(\sqrt{n}) \quad \text{и} \quad Pr_{success}(\mathcal{A}) \approx 1.$$

Теорема 1 основана на следующем формальном утверждении.

Теорема 2. Пусть $c > 0$, $t = O(\sqrt{n})$ и $a = \sin^2((2t+1)\theta)$, где $\sin \theta \in \left(\sqrt{1/n}, \sqrt{1/n+c}\right]$. Тогда

$$S(\mathcal{A}) \leq 2 \log n + \log m + \text{const}, \quad Q(\mathcal{A}) = O(\sqrt{n}) \quad \text{и} \quad Pr_{\text{success}}(\mathcal{A}) \geq a \frac{1}{1+c}.$$

3.1. Доказательство теоремы 2. В [7] доказано следующее утверждение, которое необходимо для анализа алгоритма, рассматриваемого нами. Представим это утверждение в следующем виде, удобном для нас.

Свойство 3. Пусть $\epsilon < 1$ и $E : \{0, 1\}^m \rightarrow \{0, 1\}^l$ – бинарный (l, m, d) -код с $d \geq (1 - \epsilon)l$. Тогда для функции ψ_E (1) и произвольной пары различных слов $w, w' \in \{0, 1\}^m$ верно неравенство

$$|\langle \psi_E(w) | \psi_E(w') \rangle| \leq \epsilon.$$

3.1.1. Оценка вероятности успеха $Pr_{\text{success}}(\mathcal{A})$ и запросной сложности алгоритма. Следующая лемма 1, основанная на свойстве 3, имеет решающее значение для оценки вероятности успеха $Pr_{\text{success}}(\mathcal{A})$ алгоритма $\mathcal{A}$.

Напомним, что $|\phi(w_j, w)\rangle = U_{\psi_E}^{-1}(w)|\psi_E(w_j)\rangle$.

Лемма 1. Пусть

$$|\phi(w_j, w)\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_{2^l-1}|2^s - 1\rangle.$$

Тогда для слова $w_j = w$ верно, что $\alpha_0 = 1$, $p_0 = 1$, а для слов $w_j \neq w$ верно, что $\alpha_0 = \epsilon_j \leq \epsilon$, $p_0 = \epsilon_j^2 \leq \epsilon^2$.

Доказательство. Преобразование $U_E^{-1}(w)$ является обратным к преобразованию $U_E(w)$. Применим $U_E^{-1}(w)$ к состоянию $|\psi_E(w_j)\rangle$ для получения $|\phi(w_j, w)\rangle$. Для слова $w_k = w$ имеем

$$|\phi(w_k, w)\rangle = |0\rangle = 1|0\rangle + 0|1\rangle + \dots + 0|2^s - 1\rangle.$$

Для всех других слов $w_j \in \{0, 1\}^m$ значения функции $|\psi(w_k)\rangle$ и $|\psi(w_j)\rangle$ попарно ϵ -ортогональны:

$$|\langle \psi(w_k) | \psi(w_j) \rangle| \leq \epsilon.$$

Унитарное преобразование $U_E^{-1}(w)$ состояний $|\psi(w_k)\rangle$ и $|\psi(w_j)\rangle$ сохраняет скалярное произведение. Это означает, что все состояния $|\phi(w_j, w)\rangle = U_E^{-1}(w)|\psi(w_j)\rangle$ для $w_j \in \{0, 1\}^m$ попарно ϵ -ортогональны:

$$|\langle \phi(w_k, w) | \phi(w_j, w) \rangle| \leq \epsilon.$$

Следовательно, для состояний

$$|\phi(w_j, w)\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_{2^l-1}|2^s - 1\rangle$$

и $w_j \neq w$ верно равенство $|\alpha_0| = \epsilon_j \leq \epsilon$. Последнее доказывает утверждение леммы. $\square$

Процедура усиления амплитуды соответствует процедуре, представленной в статье [2]. Мы будем следовать описанию процедуры в главе 8 книги [3].

Процедура усиления амплитуды реализуется путем многократного применения унитарного оператора QQ (оператора итерации поиска) (4) к состоянию $|V, \psi_E, w\rangle$. Ниже для простоты будем использовать $|\psi\rangle$ для обозначения состояния $|V, \psi_E, w\rangle$.

Разделим вектор $|\psi\rangle$ на части: $|\psi\rangle = |\psi_0\rangle + |\psi_1\rangle$. Согласно лемме 1,

$$|\psi_0\rangle = \frac{1}{\sqrt{n}} \left(|k\rangle|0\rangle^{\otimes(s+1)}|1\rangle + \sum_{j=0, j \neq k}^{n-1} \epsilon_j |j\rangle|0\rangle^{\otimes(s+1)}|1\rangle \right), \quad (2)$$

а вектор $|\psi_1\rangle$ включает в себя оставшиеся компоненты состояния $|\psi\rangle$. Обозначим

$$p_{good} = \frac{1}{n} \left(1 + \sum_{j=0, j \neq k}^{n-1} \epsilon_j^2 \right) \quad \text{и} \quad p_{bad} = 1 - p_{good};$$

p_{good} – это вероятность измерения n базовых состояний $|j\rangle|0\rangle^{\otimes(s+1)}|1\rangle$ для $j \in \{0, \dots, n-1\}$. Эти базовые состояния будем называть хорошими состояниями, а вероятность их получения – хорошей вероятностью p_{good} ; другие базовые состояния $|j\rangle|i\rangle|1\rangle$ – плохими состояниями, а вероятность их получения – плохой вероятностью p_{bad} . Перенормируем компоненты $|\psi_0\rangle$ и $|\psi_1\rangle$ и получим следующие состояния:

$$|\psi_{good}\rangle = \frac{1}{\sqrt{p_{good}}} |\psi_0\rangle \quad \text{и} \quad |\psi_{bad}\rangle = \frac{1}{\sqrt{p_{bad}}} |\psi_1\rangle. \quad (3)$$

Далее запишем

$$|\psi\rangle = \sqrt{p_{good}} |\psi_{good}\rangle + \sqrt{p_{bad}} |\psi_{bad}\rangle,$$

или

$$|\psi\rangle = \sin \theta |\psi_{good}\rangle + \cos \theta |\psi_{bad}\rangle,$$

где $\theta \in (0, \frac{\pi}{2})$ определяется уравнением $\sin^2 \theta = p_{good}$.

Определим оператор итерации поиска QQ следующим образом

$$QQ = U_\psi^\perp U_f. \quad (4)$$

Для произвольного действительного числа θ операция U_f осуществляется следующим образом:

$$U_f(\sin \theta |\psi_{good}\rangle + \cos \theta |\psi_{bad}\rangle) = -\sin \theta |\psi_{good}\rangle + \cos \theta |\psi_{bad}\rangle,$$

значит, U_f выполняет отражение относительно оси, определяемой вектором $|\psi_{bad}\rangle$. Точнее, оператор U_f изменяет знак амплитуды для базовых состояний вида $|j\rangle|0\rangle|1\rangle$.

Обозначим состояние

$$|\bar{\psi}\rangle = \cos \theta |\psi_{good}\rangle - \sin \theta |\psi_{bad}\rangle,$$

которое ортогонально к $|\psi\rangle$. $\{|\psi_{good}\rangle, |\psi_{bad}\rangle\}$ и $\{|\bar{\psi}\rangle, |\psi\rangle\}$ являются ортонормированными базисами для одного и того же двумерного пространства,

$$U_f|\psi\rangle = -\sin \theta |\psi_{good}\rangle + \cos \theta |\psi_{bad}\rangle = \cos(2\theta)|\psi\rangle - \sin(2\theta)|\bar{\psi}\rangle.$$

Оператор $U_\psi^\perp$ действует так:

$$U_\psi^\perp(\sin(\theta)|\psi\rangle + \cos(\theta)|\bar{\psi}\rangle) = \sin(\theta)|\psi\rangle - \cos(\theta)|\bar{\psi}\rangle,$$

таким образом, $U_\psi^\perp$ выполняет отражение относительно оси, определенной вектором $|\psi\rangle$. Действительно,

$$U_\psi^\perp U_f |\psi\rangle = U_\psi^\perp (-\sin(\theta)|\psi_{good}\rangle + \cos(\theta)|\psi_{bad}\rangle) = \cos(2\theta)|\psi\rangle + \sin(2\theta)|\bar{\psi}\rangle$$

и может быть описан в базисе $\{|\psi_{good}\rangle, |\psi_{bad}\rangle\}$ как

$$U_\psi^\perp U_f |\psi\rangle = \sin(3\theta)|\psi_{good}\rangle + \cos(3\theta)|\psi_{bad}\rangle.$$

Применение оператора QQ t раз приводит начальное состояние $|\psi\rangle$ к состоянию

$$|\psi^t\rangle = QQ^t |\psi\rangle = \sin((2t+1)\theta)|\psi_{good}\rangle + \cos((2t+1)\theta)|\psi_{bad}\rangle. \quad (5)$$

Пусть $a = \sin^2((2t+1)\theta)$. Отметим, что для малых θ имеем $\sin \theta \geq \theta - \delta$ для малых δ ($\sin \theta \approx \theta$). В частности, в нашем случае

$$\sin \theta = \sqrt{\frac{1}{n} \left(1 + \sum_{j=0, j \neq k}^{n-1} \epsilon_j^2 \right)}$$

и $\sin \theta \in \left(\sqrt{1/n}, \sqrt{1/n+c} \right]$ для малых $c > 0$. Выберем t таким образом, что $(2t+1)\theta \approx \frac{\pi}{2}$, имея в виду, что $t \in \Omega(\sqrt{n})$ ($t \in \Omega(\frac{1}{\theta})$). Выбор t обеспечивает $a \approx 1$.

$Pr_{success}(A)$ – вероятность измерения уникального базового состояния $|k\rangle|0\rangle^{\otimes(s+1)}|1\rangle$ среди всех базовых состояний $|j\rangle|0\rangle^{\otimes(s+1)}|1\rangle$, $j \in \{0, \dots, n-1\}$, части $\sin((2t+1)\theta)|\psi_{good}\rangle$ состояния $|\psi^t\rangle$ (5). Отсюда и из (2), (3) следует, что

$$Pr_{cussess}(A) = a \frac{1}{p_{good}} \frac{1}{n} = a \frac{1}{\left(\frac{1}{n}\right) \left(1 + \sum_{j, j \neq k} \epsilon_j^2\right) n} \geq a \frac{1}{1 + (n-1)\epsilon^2} \geq a \frac{1}{1 + c(\epsilon)}.$$

Таким образом, выбор $t \in \Omega(\sqrt{n})$ и $c > 0$ (в соответствии с ϵ), близкого к 0, обеспечивает $Pr_{cussess}(A) \approx 1$.

3.1.2. Оценка объема памяти $S(\mathcal{A})$. Размерность $S(\mathcal{A})$ алгоритма $\mathcal{A}$ определяется как количество кубитов в состоянии $|V, \psi_E\rangle$. Таким образом, имеем

$$S(\mathcal{A}) = \log n + s + 2.$$

Для некоторого выбранного $c > 0$ и $\epsilon = \sqrt{c/(n-1)}$ имеем

$$\begin{aligned} S(\mathcal{A}) &= \log n + \log m + \log(\epsilon^2(n-1)) + 2 = \\ &= \log n + \log m + \log \epsilon^2 + \log(n-1) + 2 \leq 2 \log n + \log m + const. \end{aligned}$$

Комментарий. Напомним, что ϵ является параметром кода E , исправляющего ошибки, а код E определяет квантовую функцию отпечатков ψ_E . Величина ϵ является важной компонентой, определяющей попарную “почти” ортогональность (ϵ -ортогональность) значений функции ψ_E . Последнее существенно в доказательстве высокой вероятности правильного результата действия алгоритма.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Conflicts of Interest. The authors declare no conflicts of interest.

Литература

1. Grover L.K. A fast quantum mechanical algorithm for database search // STOC'96: Proc. 28th Annu. ACM Symp. on Theory of Computing. Philadelphia, PA: ACM. 1996. P. 212–219. <https://doi.org/10.1145/237814.237866>.
2. Brassard G., Høyer P., Mosca M., Tapp A. Quantum amplitude amplification and estimation // Quantum Computation and Information. Ser.: Contemporary Mathematics. Providence, RI: Am. Math. Soc., 2002. V. 305. P. 53–74. <http://dx.doi.org/10.1090/conm/305/05215>.
3. Kaye P., Laflamme R., Mosca M. An Introduction to Quantum Computing. New York, NY: Oxford Univ. Press, 2007. 274 p.
4. Ablayev F., Ablayev M., Huang J.Z., Khadiev K., Salikhova N., Wu D. On quantum methods for machine learning problems. Part I: Quantum tools // Big Data Min. Anal. 2020. V. 3, No 1. P. 41–55. <https://doi.org/10.26599/BDMA.2019.9020016>.
5. Ablayev F., Ablayev M., Huang J.Z., Khadiev K., Salikhova N., Wu D. On quantum methods for machine learning problems. Part II: Quantum classification algorithms // Big Data Min. Anal. 2020. V. 3, No 1. P. 56–67. <https://doi.org/10.26599/BDMA.2019.9020018>.
6. Ablayev F., Salikhova N., Ablayev M. Hybrid classical–quantum text search based on hashing // Mathematics. 2024. V. 12, No 12. Art. 1858. <https://doi.org/10.3390/math12121858>.
7. Buhrman H., Cleve R., Watrous J., de Wolf R. Quantum fingerprinting // Phys. Rev. Lett. 2001. V. 87, No 16. Art. 167902. <https://doi.org/10.1103/PhysRevLett.87.167902>.

References

1. Grover L.K. A fast quantum mechanical algorithm for database search. *STOC'96: Proc. 28th Annu. ACM Symp. on Theory of Computing*. Philadelphia, PA, ACM, 1996, pp. 212–219. <https://doi.org/10.1145/237814.237866>.
2. Brassard G., Høyer P., Mosca M., Tapp A. Quantum amplitude amplification and estimation. In: *Quantum Computation and Information*. Ser.: Contemporary Mathematics. Vol. 305. Providence, RI, Am. Math. Soc., 2002, pp. 53–74. <http://dx.doi.org/10.1090/conm/305/05215>.
3. Kaye P., Laflamme R., Mosca M. *An Introduction to Quantum Computing*. New York, NY, Oxford Univ. Press, 2007. 274 p.
4. Ablayev F., Ablayev M., Huang J.Z., Khadiev K., Salikhova N., Wu D. On quantum methods for machine learning problems. Part I: Quantum tools. *Big Data Min. Anal.*, 2020, vol. 3, no. 1, pp. 41–55. <https://doi.org/10.26599/BDMA.2019.9020016>.
5. Ablayev F., Ablayev M., Huang J.Z., Khadiev K., Salikhova N., Wu D. On quantum methods for machine learning problems. Part II: Quantum classification algorithms. *Big Data Min. Anal.*, 2020, vol. 3, no. 1, pp. 56–67. <https://doi.org/10.26599/BDMA.2019.9020018>.
6. Ablayev F., Salikhova N., Ablayev M. Hybrid classical–quantum text search based on hashing. *Mathematics*, 2024, vol. 12, no. 12, art. 1858. <https://doi.org/10.3390/math12121858>.
7. Buhrman H., Cleve R., Watrous J., de Wolf R. Quantum fingerprinting. *Phys. Rev. Lett.*, 2001, vol. 87, no. 16, art. 167902. <https://doi.org/10.1103/PhysRevLett.87.167902>.

Информация об авторах

Наиля Маратовна Салихова, аспирант, Казанский (Приволжский) федеральный университет

E-mail: *nailyasalikhova66@gmail.com*

Author Information

Nailya M. Salikhova, Postgraduate Student, Kazan Federal University

E-mail: *nailyasalikhova66@gmail.com*

Поступила в редакцию 15.11.2024

Принята к публикации 18.01.2025

Received November 15, 2024

Accepted January 18, 2025