УДК 519.688, 510.52

Шемякина М.А.,
студент магистратуры
1 курс, факультет «Техника и технологии»
Институт сферы обслуживания и предпринимательства (филиал)
ДГТУ в г. Шахты
Россия, г. Шахты

АЛГОРИТМ МОДЕЛИРОВАНИЯ КВАНТОВОГО АЛГОРИТМА ГРОВЕРА

Аннотация: *Статья посвящена исследованию квантового алгоритма Гровера. Данный алгоритм предназначен для поиска значения некоторого параметра в заданном неупорядоченном пространстве. Как показало исследование, использование алгоритма Гровера позволяет получить квадратичное ускорение по сравнению с классическими алгоритмами поиска. Также проведен анализ фундаментальных принципов квантовых вычислений: квантовый бит, суперпозиция, основные квантовые элементы.*

Ключевые слова: *квантовый бит, квантовый компьютер, квантовый алгоритм Гровера.*

Annotation: *The article is devoted to the study of Grover's quantum algorithm. This algorithm is designed to search for the value of some parameter in a given unordered space. As research has shown, the use of Grover's algorithm allows one to obtain quadratic acceleration in comparison with classical search algorithms. The analysis of the fundamental principles of quantum computing is also carried out: quantum bits, superposition, basic quantum elements.*

Key words: *quantum bit, quantum computer, Grover's quantum algorithm.*

Квантовая вычислительная модель в последние десятилетия привлекает к себе пристальное внимание ученых, а именно ее реализация в качестве

квантового компьютера. На данный момент известно, что квантовый компьютер способен вычислять сложные задачи, для которых не существует эффективных алгоритмов решения на классическом компьютере. Например, используя классические вычисления невозможно эффективно решить задачу факторизации. В квантовых же вычислениях используется алгоритм Шора, который позволяет за полиномиальное время решить задачу факторизации [1]. Одновременно с этим были обнаружены и другие задачи, которые решаются эффективней на квантовых компьютерах.

1. Основные теоретические сведения

Основой квантовой вычислительной модели является квантовый бит (кубит), который является аналогом классического бита. Кубит, как и бит может находиться в состоянии $|0\rangle$, $|1\rangle$. Однако в отличие от бита он также может находиться в суперпозиции состояний, которая представляет собой линейную комбинацию состояний квантового бита. Для квантовой системы, состоящей из одного кубита суперпозицию можно представить следующим образом:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \qquad (1)$$

где числа α и β - комплексные коэффициенты, удовлетворяющие условию $|\alpha|^2+|\beta|^2=1$ [2].

Еще одним отличием кубита от бита является невозможность его измерения для определения состояния. Можно получить лишь более ограниченную информацию о его квантовом состоянии. При измерении кубита будет получен 0 с вероятностью $|\alpha|^2$ или 1 с вероятностью $|\beta|^2$ [3]. После проведения измерения кубит переходит в состояние, которое соответствует измерению, т.е. он коллапсирует из суперпозиции в определенное состояние [4].

В квантовом компьютере состояние кубита изменяется под действием различных квантовых элементов В качестве стандартных квантовых элементов можно выделить следующие: квантовый элемент NOT и преобразование Адамара.

Квантовый элемент NOT является аналогом классического логического элемента NOT. Его действие заключается в переводе состояния $\alpha|0\rangle + \beta|1\rangle$ в состояние, в котором $|0\rangle$ и $|1\rangle$ меняются местами.

Преобразование Адамара позволяет переводить базисное состояние в равновероятное, т.е. при измерении с равной вероятностью можно получить любой результат. Во многих квантовых алгоритмах в качестве начального и конечного шага используют преобразование Адамара.

2. Алгоритм Гровера

Для решения задачи компьютеру необходимо выполнить определенную последовательность операций. Описание этой последовательности называют алгоритмом решения задачи [5]. Для решения задачи на квантовом компьютере создают квантовые алгоритмы, которые в отличие от классических учитывают законы квантовой физики. На данный момент было разработано около шестидесяти квантовых алгоритмов [6].

Рассмотрим квантовый алгоритм Гровера предназначенный для поиска значения некоторого параметра в заданном неупорядоченном пространстве. Пусть задана булева функция $f(x)$, $x \in \{0,1\}^n$, которая представлена в виде черного ящика. Цель алгоритма Гровера найти x такой, что $f(x)=1$ (функция дана в виде оракула).

Алгоритм Гровера можно представить следующим образом:

– Инициализация начального состояния. На данном этапе необходимо подготовить равновероятную суперпозицию состояний всех входных кубитов.

– Применение итерации Гровера. Итерация Гровера состоит из оракула и оператора диффузии Гровера (условный сдвиг фазы). Данный этап повторяется $\sqrt{N}$ раз.

– Измерение. На данном этапе производят измерение выходного регистра кубитов.

Основной частью рассматриваемого алгоритма является итерация Гровера, которая разбита на четыре шага: применение оракула (гейт, осуществляющий вычисление заданной функции.); применение преобразования Адамара;

применение к регистру условного сдвига фазы; применение преобразования Адамара. Три последних шага объединяются в оператор диффузии Гровера [7].

В анализируемом алгоритме оракул предназначен для распознавания решения задачи поиска. Когда на вход функции f подается значение x, при котором $f(x)=1$ оракул помечает данное решение, сдвигая фазу у того квантового состояния, которое соответствует значению x.

Как можно заметить, классический алгоритм решает задачу поиска методом перебора, т.е. в лучшем случае x будет найден с первой попытки, а в худшем придётся перебрать 2^n вариантов. Следовательно, x можно найти таким методом за O(N) операций, где $N=2^n$. Алгоритм Гровера позволяет ускорить метод поиска – до $O(\sqrt{N})$ операций.

Таким образом, на основе выше сказанного можно сделать вывод о том, что квантовый алгоритм Гровера позволяет найти значение некоторого параметра в заданном неупорядоченном пространстве за $O(\sqrt{N})$ обращений к оракулу, т.е. дает квадратичное ускорение по сравнению с классическим алгоритмом.

3. Реализация квантового алгоритма Гровера

Для реализация квантового алгоритма Гровера была выбрана сервис-ориентированная архитектура. Вся бизнес-логика, которая представляет собой квантовые вычисления, реализуется набором сервисов, а проверка введенных данных, их интерпретация и вывод осуществляются на стороне клиента. Введенные пользователем данные по протоколу передаются сервису, который выполняет квантовые вычисления. Полученный результат передается клиенту.

На рисунке 1 представлена архитектура проектируемой системы.

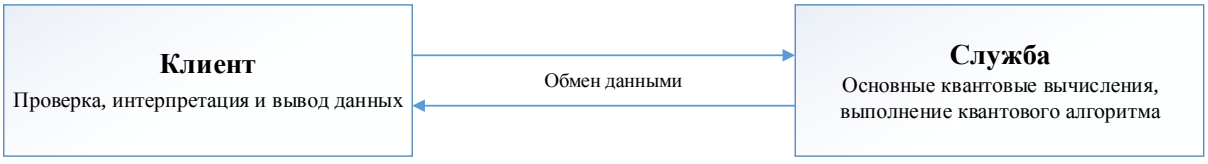

Рисунок 1 –Сервис-ориентированная архитектура

При реализации алгоритма Гровера, было использовано два класса: *StartGrover и Grover*. В StartGrover происходит проверка и подготовка входных

данных, а также вывод результатов в виде графика. *Grover* выполняет квантовую часть алгоритма Гровера

На рисунке 2 показана последовательность действий, необходимых для выполнения алгоритма Гровера.

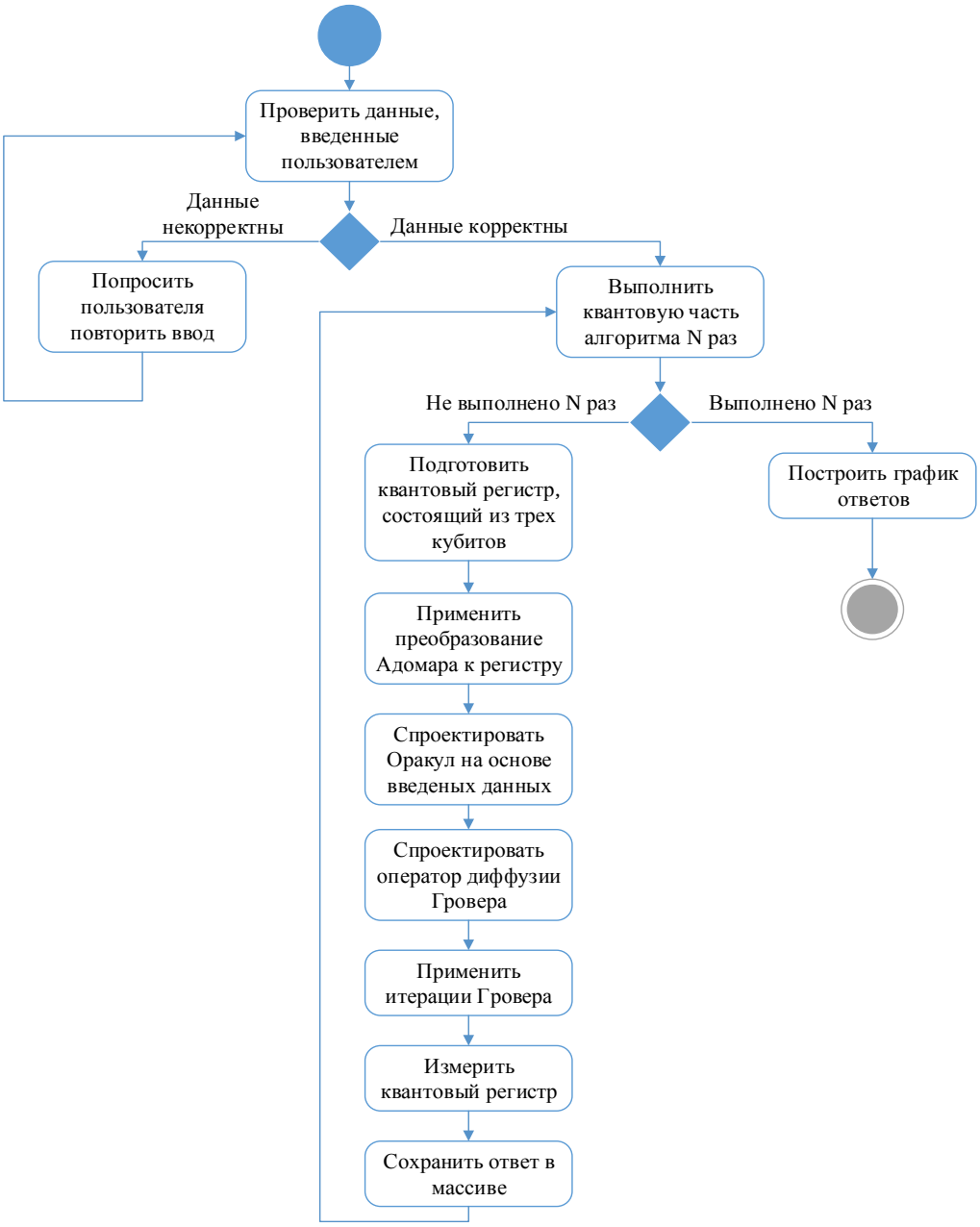

Рисунок 2 – Алгоритм Гровера

Выполнение алгоритма Гровера начинается с ввода данных. Затем система подготавливает квантовый регистр, который должен состоять из трех кубитов, над которыми выполняется преобразование Адамара.

Следующий этап начинается с проектирование оракула и оператора диффузии Гровера, которые строятся на основе данных, которые были введены

пользователем. Затем поток управления переходит к выполнению итерации Гровера.

Заключительным этапом квантовой части алгоритма является измерение квантового регистра и сохранение ответа в массиве. Когда квантовая часть алгоритма Гровера будет выполнена N раз, система переходит к построению графика, на котором отображаются все ответы (рисунок 3).

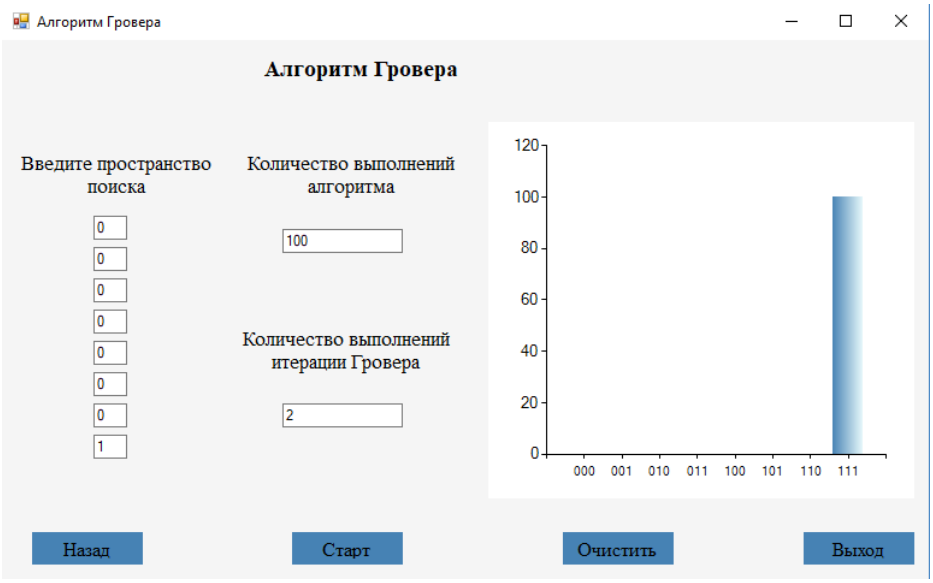

Рисунок 3 – Тестирование алгоритма Гровера

Заключение

В данной статье представлено моделирование квантового алгоритма Гровера на классическом компьютере. Для реализации алгоритма была использована библиотека квантовых вычислений на C# - Quantum.NET, которая была выпущена в 2017 году. Данная библиотека позволяет манипулировать кубитами и моделировать квантовые цепи. Она значительно упрощает проектирование регистров и оракулов.

Таким образом, можно сделать вывод о том, что несмотря на отсутствие полноценного квантового компьютера, квантовые алгоритмы поддаются описанию, изучению и моделированию и на классическом компьютере.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Душкин Р.В. Квантовые вычисления и функциональное программирование. — 2014 г. — 318 с., ил.

2. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ - М: Мир, 2006 г. — 824 с, ил

3. Гуц А.К. Основы квантовой кибернетики. – Омск: Полиграфический центр КАН, 2008. – 204 с.

4. Калачев А.А. Квантовая информатика в задачах: учеб.-метод. пос. / А.А. Калачев. — Казань: Казан. ун-т, 2012 г. — 48 с.: ил.

5. Дасгупта С., Пападимитриу Х., Вазирани У. Алгоритмы. Пер. с англ. под ред. А. Шеня. — М.: МЦНМО, 2014. — 320 с.

6. Stephen Jordan. Quantum algorithms zoo. [Электронный ресурс]. URL:https://math.nist.gov/quantum/zoo/ (дата обращения: 08.01.2019).

7. Гуц А.К. Архитектура, процессор и работа квантового компьютера// Математические структуры и моделирование. - 2010. - Вып. 21. - С. 55-64: рис. - Библиогр.: С. 64.