МОДЕЛИРОВАНИЕ КВАНТОВОГО АЛГОРИТМА САЙМОНА НА КЛАССИЧЕСКОМ КОМПЬЮТЕРЕ

М.А. Шемякина, *магистрант*
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты (Россия, г. Шахты)

DOI: 10.24411/2500-1000-2019-11335

Аннотация. *Статья посвящена анализу фундаментальных принципов квантовых вычислений: квантовый бит, суперпозиция, основные квантовые элементы. Актуальность работы обоснована тем, что ряд задач не может быть решен с помощью классических вычислительных машин. В результате поиска решения данной проблемы возникла квантовая информатика. В данной статье рассматривается возможность создания программы, позволяющей моделировать квантовые вычисления, а именно, квантовый алгоритм Саймона на классическом компьютере. Квантовый алгоритм Саймона, позволяет определить период некоторой функции за линейное количество вызовов этой функции.*

Ключевые слова: *квантовая информатика, квантовые вычисления, квантовый бит, квантовые элементы, квантовый алгоритм Саймона.*

Сложившаяся современная тенденция повышения сложности математических расчетов привела к появлению новой парадигмы вычислений – квантовой парадигме вычислений. К данному моменту было доказано, что на квантовых компьютерах можно эффективно решать задачи, для которых ещё не существует эффективных алгоритмов в классической вычислительной парадигме. Например, используя классические вычисления, невозможно эффективно решить задачу факторизации. В квантовых же вычислениях используется алгоритм Шора, который позволяет за полиномиальное время решить задачу факторизации. Одновременно с этим были обнаружены и другие задачи, которые решаются эффективней на квантовых компьютерах. Именно поэтому квантовая информатика переживает такой бурный рост.

Основные теоретические сведения

Фундаментальным понятием в области квантовых вычислений и квантовой информации является понятие квантового бита (далее - кубита) [1]. Кубит может находиться в состоянии $|0\rangle$, $|1\rangle$ или суперпозиции состояний, являющейся линейной комбинацией состояний кубита.

Изменения, происходящие с кантовыми состояниями, описываются при помощи квантовых вычислений. Можно выделить следующие принципы квантовых вычислений [2]:

– *Обратимость вычислений.* Согласно квантовой механике, ее законы обратимы во времени. Значит квантовые преобразования должны быть также обратимы во времени.

– *Избыточность.* Для восстановления исходных данных количество выходов в квантовых логических элементах должно равняться количеству входов.

– *Отсутствие циклов.* Обратимость вычислений приводит к тому, что в квантовых преобразованиях не может быть циклов и возвратов назад.

– *Квантовый параллелизм.* Квантовый параллелизм позволяет вычислять функцию f(x) для многих различных значений X одновременно. Благодаря тому, что квантовые биты находятся в суперпозиции состояний, одна и та же задача решается параллельно для большого количества данных.

– *Квантовая запутанность.* Запутанным состоянием пары кубитов называется такое состояние, в котором имеется постоянная связь между физическими величинами, относящимися к разным кубитам.

2. Алгоритм Саймона

Для решения задачи компьютеру необходимо выполнить определенную последовательность операций. Описание этой

последовательности называют алгоритмом решения задачи [3]. 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 [4].

Рассмотрим квантовый алгоритм Саймона, который позволяет определить период некоторой функции. Для классических вычислений поиск периода функции является сложной задачей. В среднем случае потребуется $O(2^n)$ вызовов функции, прежде чем определить период этой функции. А квантовый алгоритм, в отличии от классического, способен найти период функции за линейное количество вызовов функции.

Задачу Саймона можно сформулировать следующим образом: дана двоичная функция $f:\{0, 1\}^n \rightarrow \{0, 1\}^n$. Известно, что существует некоторое число a, которое называется периодом, такое, что для любой пары различных входных значений x и y функция f возвращает одинаковое значение, если $y = x \oplus a$. Необходимо найти период a [5].

Задача, которую решает алгоритм Саймона не имеет большого прикладного значения, однако данный алгоритм стал основой других важных квантовых алгоритмов, например, алгоритмы Шора: факторизации и нахождения дискретного логарифма.

3. Реализация квантового алгоритма Саймона

Для реализация квантового алгоритма Саймона была выбрана сервис-ориентированная архитектура. Под сервис-ориентированной архитектурой (SOA) понимается модульный подход к разработке программного обеспечения, использующий слабо связанные и легко заменяемые компоненты. В данной архитектуре подразумевается, что клиент имеет минимум функций, он может только вызывать сервисы и отображать данные. Вся бизнес-логика реализуется набором слабо связанных сервисов. Сервисы взаимодействуют с клиентами и между собой, используя SOAP, HTTP и другие Internet-протоколы. 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.

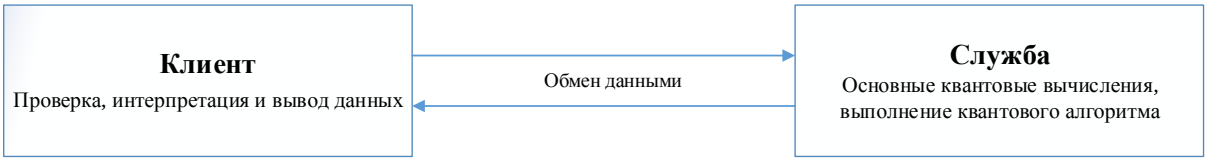

Рис. 1. Сервис-ориентированная архитектура

При реализации алгоритма Саймона было использовано два класса: *StartSimon и Simon*. В *StartSimon* происходит проверка и подготовка входных данных, а также вывод результатов в виде графика. *Simon* выполняет квантовую часть алгоритма Саймона.

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

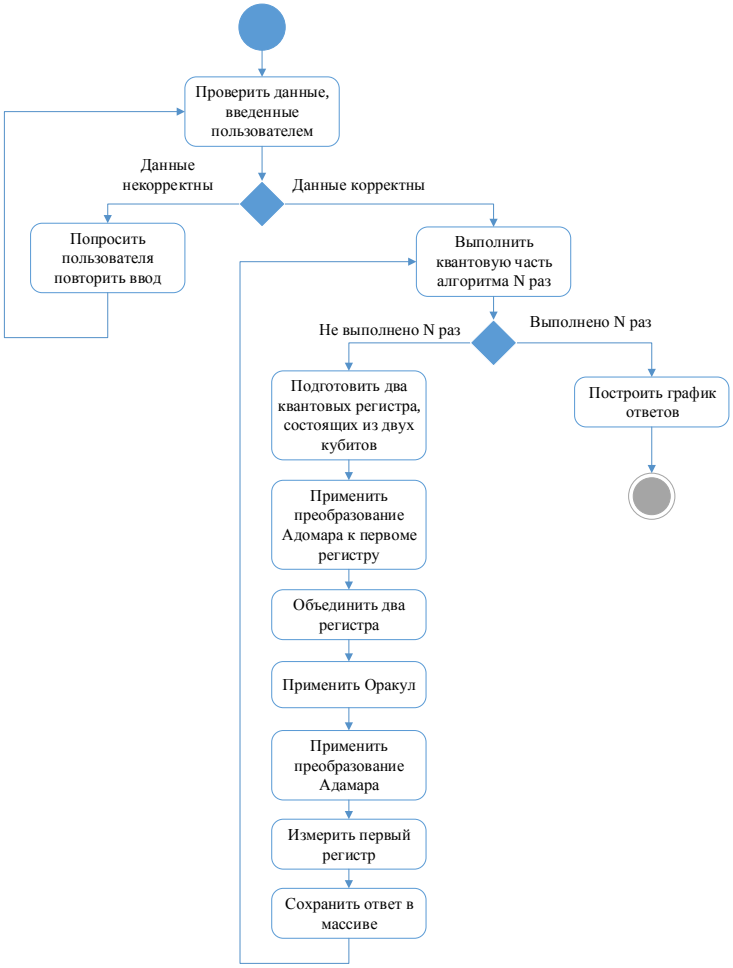

Рис. 2. Алгоритм Саймона

Выполнение алгоритма Саймона начинается с проверки данных, которые были введены пользователем. Если данные некорректны, тогда система должна попросить пользователя повторить ввод.

Если введенные данные корректны, тогда система переходит к выполнению квантовой части алгоритма Саймона. Квантовая часть должна быть выполнена N раз, где N указывается пользователем.

После квантовых преобразований система переходит к построению графика, на основе полученного массива ответов (рисунок 3).

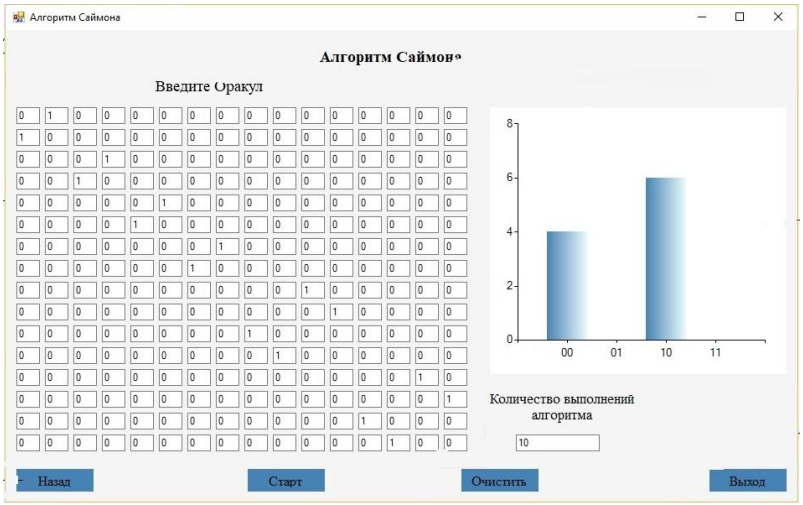

Рис. 3. Тестирование алгоритма Саймона

Заключение. В данной статье представлено моделирование квантового алгоритма Саймона 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.

В результате проведенного исследования были сделаны следующие выводы:

1. В рамках квантовых вычислений для некоторых задач можно реализовывать более эффективные алгоритмы, чем в классических вычислениях.
2. Создание квантовых компьютеров позволит решить проблему экспоненциального роста сложности алгоритмов.
3. Эмуляция алгоритмов возможна на классических компьютерах, но при этом не было обнаружено никакой выгоды по сравнению с классической вычислительной моделью.
4. Квантовые алгоритмы эффективны только на квантовых компьютерах и на больших входных данных.

Библиографический список

1. *Калачев А.А.* Квантовая информатика в задачах: учеб.-метод. пос. / А.А. Калачев. – Казань: Казан. ун-т, 2012. – 48 с.

2. *Нильсен М.,* Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. – М.: Мир, 2006. – 824 с.

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

4. *Stephen Jordan.* Quantum algorithms zoo. URL:https://math.nist.gov/quantum/zoo/ (дата обращения: 17.02.2018).

5. *Душкин Р. В.* Квантовые вычисления и функциональное программирование. – 2014. – 318 с.

SIMULATION OF QUANTUM ALGORITHM OF SIMON ON A CLASSICAL COMPUTER

M.A. Shemyakina, *graduate student*
Institute of service and entrepreneurship (branch) of DSTU in Shakhty
(Russia, Shakhty)

Abstract*. The article is devoted to the analysis of the fundamental principles of quantum computing: quantum bits, superposition, basic quantum elements. The relevance of the work is justified by the fact that a number of tasks cannot be solved with the help of classical computers. As a result of the search for a solution to this problem, quantum computer science has emerged. This article discusses the possibility of creating a program that allows you to simulate quantum computing, namely, the Simon quantum algorithm on a classical computer. Simon's quantum algorithm allows to determine the period of a certain function a linear number of function calls.*

Keywords*: quantum informatics, quantum computing, quantum bit, quantum elements, Simon's quantum algorithm.*