DOI: 10.17117/na.2015.08.761

Поступила (Received): 26.08.2015

<http://ucom.ru/doc/na.2015.08.761.pdf>

Гузик В.Ф., Гушанский С.М., Потапов В.С. Модель квантовых вычислений

Guzik V.Ph., Gushansky S.M., Potapov V.S.
The model of quantum computing

В данной статье выделены основные понятия теории квантовых вычислителей, такие как кубит, квантовый регистр или суперпозиция. Также предложена схематическая структура модели квантовых вычислений и взаимосвязь составляющих ее элементов с их подробным описанием и функциональностью. Выделены основные методы измерения состояния квантовой системы в определенный период ее работы

Ключевые слова: квантовые вычисления, кубит, суперпозиция, квантовый регистр

This article identified the main concepts of the theory of quantum calculators, such as the qubit, the quantum superposition or register. Also offered is a schematic structure of the model of quantum computation and the relationship of its constituent elements with their detailed description and functionality. The basic methods of measuring the state of a quantum system in a certain period of its operation

Key words: quantum computing, qubit, superposition, quantum register

Гузик Вячеслав Филиппович
Доктор технических наук, профессор, заведующий кафедрой
Южный федеральный университет

Guzik Vyacheslav Philipovich
Doctor of Engineering Sciences, Professor, Head of Department
Southern federal university

Гушанский Сергей Михайлович
Кандидат технических наук, доцент
Южный федеральный университет

Gushansky Sergey Mikhailovich
Candidate of Engineering Sciences, Associate Professor
Southern federal university

Потапов Виктор Сергеевич
Магистр
Южный федеральный университет

Potapov Victor Sergeevich
Master
Southern federal university

Работа выполнена при финансовой поддержке РФФИ, грант № НК 15-01-01270\15.

Что такое квантовые вычисления?

Квантовые вычисления – это вычислительная модель, которая отличается от модели Тьюринга и фон Неймана, и для ряда задач она является более эффективной. Также определены задачи, для которых модель квантовых вычислений даёт полиномиальную сложность, по сравнению с экспоненциальной сложностью классических алгоритмов.

Рис. 1. Схематическая структура модели квантовых вычислений (МКВ)

В основе модели квантовых вычислений (МКВ) лежит понятие кубита. Он может одновременно принимать несколько значений. Кубит[1] может находиться в суперпозиции своих базисных состояний, то есть значение кубита есть линейная комбинация его базовых состояний, а коэффициенты при этих состояниях – комплексные числа. Суперпозиция одного кубита

$$A * |0\rangle + B * |1\rangle,$$

где A и B – комплексные числа. Два кубита имеют 4 возможных значения: 00, 01, 10 и 11. Соответственно: $A|00\rangle + B|01\rangle + C|10\rangle + D|11\rangle$. Другими словами, квантовый регистр[2] из N кубитов одновременно хранит в себе 2^N комплексных чисел.

В рамках МКВ функция представляет собой эрмитову матрицу. При ее умножении на эрмитово-сопряжённую получается единичная матрица. Эрмитово-сопряжённая матрица выводится путем транспонирования начальной матрицы и заменой её членов на их комплексно-сопряжённые. Если такую матрицу умножить на вектор квантового регистра, то получится новый квантовый регистр.

Квантовый алгоритм представляет собой умножение матрицы на вектор, в результате чего получается новый вектор. Этот вектор можно измерить и вследствие такого измерения, получить из него конкретное значение кубита. В данном случае суперпозиция сворачивается в определенное значение.

Суть квантового алгоритма заключается в создании равновероятностной суперпозиции всех возможных значений входного параметра. Эта суперпозиция подаётся на вход функции. Далее по результатам её выполнения делается вывод о свойствах этой функции.

Измерение состояния квантовой системы

На классическом компьютере считывание значений переменных не представляет сложности. В квантовых же системах ситуация обстоит несколько сложнее. Такого рода системы должны работать изолировано – вмешательство в работу приводит к изменению ее состояния и, как следствие, результатов вычислений. Несмотря на то, что кубиты могут находиться в нескольких состояниях одновременно, информация об этих состояниях доступна только путем измерения. Этот процесс носит вероятностный характер, то есть при измерении суперпозиции $|\varphi\rangle = \sum_i \alpha_i * |i\rangle$, выделим некоторое состояние $|i\rangle$ с вероятностью $|\alpha_i|^2$. Это один из вариантов извлечения значения (информации) кубита. Другой метод – многократное копирование результатов вычислений и статический анализ. Опишем метод квантового измерения, называемый проектным. Для выполнения такого измерения необходимо выделить весь набор ортогональных проекторов P_m , удовлетворяющих условию $\sum_m P_m = I$ и

$$P_m * P_{m'} = \begin{cases} P_m, & \text{если } m = m' \\ I, & \text{иначе} \end{cases}$$

Тогда вероятность результата m :

$$\text{Pr}(m) = \|\tilde{P}_m |\varphi\rangle\|_2^2 = \langle \varphi | \tilde{P}_m * P_m * |\varphi\rangle$$

а состояние квантовой системы после измерения

$$|\varphi'\rangle = \frac{P_m * |\varphi\rangle}{\sqrt{\text{Pr}(m)}}$$

Структура модели квантового вычислителя

Для простоты процессов разработки, модификации, переносимости вычислителя, связи с различными языками программирования и средами разработки он должен иметь многослойную структуру:

– Ядро вычислителя

Ядро – это компонент, который содержит в себе всё необходимое для моделирования кубит (квантового регистра) и набора операций (гейтов), которые применяются к данным кубита. Для облегчения работы с ядром имеются функции, реализующие конкретные, одно- и двухкубитовые вентили.

// гейт Адамара

```
private void hadamardButtonActionPerformed(java.awt.event.ActionEvent evt)[3]
```

// гейт CNOT

```
private void cNOTButtonActionPerformed(java.awt.event.ActionEvent evt)
```

// гейт NOT

```
private void xButtonActionPerformed(java.awt.event.ActionEvent evt)
```

// Тоффоли гейт

```
private void toffoliButtonActionPerformed(java.awt.event.ActionEvent evt)
```

// Обратное квантовое преобразование Фурье

```
private void invQftButtonActionPerformed(java.awt.event.ActionEvent evt)
```

// Квантовое преобразование Фурье

```
private void qftButtonActionPerformed(java.awt.event.ActionEvent evt)
```

// Оператор вычисления функции

private void U_fButtonActionPerformed(java.awt.event.ActionEvent evt)

// Оператор Гровера

private void groverButtonActionPerformed(java.awt.event.ActionEvent evt)

Реализация указанных функций упрощает задачу разработки математического ядра. Но также перед разработчиками встает другая, не менее сложная задача: взаимодействие всех этих функций между собой.

– Квантовые вентили

Ядро эмулятора осуществляет эмуляцию одного квантового регистра с помощью его вектора состояния, реализацию произвольных одно- и двухкубитовых вентилей, предоставляет функции для чтения и записи как для регистра, так и для его отдельных кубитов. В отладочных целях имеется доступ непосредственно к вектору состояния.

В настоящее время реализованы все функции ядра и основные квантовые вентили. Библиотека написана на языке Си и допускает как статическую, так и динамическую компоновку с программами пользователя.

– Библиотека базовых квантовых алгоритмов

Библиотека базовых квантовых алгоритмов включает реализацию наиболее часто используемых рутинных квантовых алгоритмов, например квантового фурье-преобразования (QFT). Она будет использовать ядро и реализацию конкретных одно- и двухкубитовых вентилей. Имеется возможность динамической компоновки (DLL).

– Интерфейсы для языков программирования и сред разработки

Интерфейсы для языков программирования дают возможность использования ядра эмулятора с уже существующими языками, средами разработки и библиотеками без его доработки и перекомпиляции.

– Интерфейс пользователя

Интерфейс пользователя – это разновидность интерфейсов, в котором одна сторона представлена человеком (пользователем), другая – машиной/устройством (моделью квантового вычислителя).

Заключение

Вычисления квантового характера представляют собой контролируемые классическим управляющим компьютером последовательности унитарных операций простого вида. Идея о квантовых вычислениях была высказана Юрием Маниным в 1980 году [4], одна из первых моделей квантового компьютера была предложена Ричардом Фейнманом в 1981 году. Измерение есть единственная возможность получения информации о квантовом состоянии, так как значения α_i непосредственно недоступны. В ходе написания статьи были описаны основные понятия, связанные с квантовыми вычислениями. Также была предложена структура моделей квантовых вычислителей и набор элементов, входящих в ее состав.

Список используемых источников:

1. Кубит. URL: <https://ru.wikipedia.org/wiki/Кубит>
2. Гузик В.Ф., Гушанский С.М., Потапов В.С. Модель квантового вычислителя, архитектура и программная реализация // Сборник трудов XII Всероссийской научной конференции молодых ученых, аспирантов и студентов. Таганрог. 2014. Т. 1. С. 110-118.

3. Гузик В.Ф., Гушанский С.М., Потапов В.С. Реализация компонентов для построения открытой модульной модели квантовых вычислительных устройств // Информатизация и связь. Москва, 2015. С. 44-48.

4. Квантовый компьютер. URL: https://ru.wikipedia.org/wiki/Квантовый_компьютер

© 2015, Гузик В.Ф., Гушанский С.М., Потапов В.С.
Модель квантовых вычислений

© 2015, Guzik V.Ph., Gushansky S.M., Potapov V.S.
The model of quantum computing