УДК 004.82 + 004.832.34

О КВАНТОВЫХ ВЫЧИСЛЕНИЯХ

Сафаев Руслан Васылович
Студент
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Россия, г. Владимир

Safaev Ruslan Vasylovich
Student
Vladimir State University named after Alexander and Nikolay Stoletovs, Russia, Vladimir

Озерова Марина Игоревна
Кандидат технических наук, доцент кафедры информационные системы и программная инженерия, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Россия, г. Владимир

Ozerova Marina Igorevna
Candidate of Technical Sciences, Associate Professor of the Department of Information Systems and Software Engineering, Vladimir State University named after Alexander and Nikolay Stoletovs, Russia, Vladimir

Аннотация

Рассматривается парадигма квантовых вычислений. Особенности квантовых вычислений. В каких областях применяются и какие задачи решают данные вычисления. Квантовый компьютер и квантовый симулятор

Ключевые слова: *квантовые вычисления, квантовый компьютер.*

Abstracts

The paradigm of quantum computing is considered. Features of quantum computing. In what areas are applied and what tasks are solved by these calculations. Quantum computer and quantum simulator.

Keywords: *quantum computing, quantum computer, quantum simulator.*

Известно, что законы квантовой физики имеют различия по сравнению с законами классической физики. Если привести пример, выяснится, что согласно явлению суперпозиции с точки зрения квантовой физики, система может быть представлена в двух возможных состояниях, даже если эти состояния взаимоисключающие. На языке двоичной логики принцип квантовой суперпозиции означает, что квантовые биты, они же кубиты, могут быть в одно и тоже время и «0» и «1». Между тем, квантовые системы могут показывать сильную корреляцию параметров, даже находясь на приличном состоянии друг от друга, в силу феномена квантовой запутанности.

Кубиты – необходимая составляющая квантовых вычислений, реализующая физические свойства квантовых объектов. Как уже было написано, кубит может находиться в одно и тоже время в двух состояниях, поэтому его принято обозначать выражением $a|0\rangle + b|1\rangle$*, где A и B – комплексные числа, удовлетворяющие условию*

$$|A|^2 + |B|^2 = 1 \qquad (1)$$

Одно из свойств кубита гласит, что он может быть введен в состояние, при котором результатом измерения могут быть 1 или 0 с одинаковой вероятностью. Это состояние описывается следующим образом

$$1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle \qquad (2)$$

Иногда приходиться сравнивать классические вычисления с квантовыми. Например, имея восемь классических бит, можно представить ровно одно число в диапазоне от 0 до 255, при этом значение каждого из 8 бит будут равны 0 или 1. Имея же 8 кубит, можно представить уже все числа от 9 до 255.

Устройства для реализации квантовых вычислений принято разделять на два больших класса: (универсальные) квантовые компьютеры и квантовые симуляторы.

Универсальные квантовые компьютеры — это аналоги классических процессоров общего назначения в том смысле, что они могут решать любую алгоритмическую задачу, при этом их функционирование существенно базируется на использовании квантовых эффектов.

Например, давно известен так называемый алгоритм Шора, позволяющий быстро раскладывать большие числа на простые множители (задача, необходимая для взлома современных шифров). Обычные компьютеры решают эту задачу перебором возможных делителей, поэтому длинные числа современные компьютеры могут обрабатывать годами. Квантовый компьютер справился бы с такой задачей за считанные минуты и даже секунды, в зависимости от производительности.

Одной из важнейших частей компьютера, от которой напрямую зависит его мощность, является процессор, который, в свою очередь, состоит из огромного числа транзисторов. Транзисторы — это простейшие части системы, они чем-то похожи на переключатели и могут находиться только в двух положениях: либо «включен», либо «выключен». Именно из комбинаций этих положений складывается двоичный код, состоящий из нулей и единиц, на котором базируются все языки программирования. Соответственно, чем мощнее компьютер, тем больше транзисторов необходимо для его работы.

Транзисторы, из которых будет состоять квантовый компьютер, могут находиться одновременно в двух положениях:« включен» и «выключен» и, соответственно, сразу быть и единицей, и нулем, это называется «суперпозиция».

Рассмотрим, например, квантовый компьютер от компании Microsoft

Квантовый компьютер Microsoft состоит из трех основных уровней: первый уровень — собственно, квантовый компьютер, содержащий кубиты и постоянно находящийся при температуре, близкой к абсолютному нулю; следующий уровень — криогенный компьютер — это тоже совершенно новый тип компьютера, который управляет квантовым и работает при температуре–268° С; последний уровень — компьютер, за которым уже может работать человек, и управляющий всей системой.

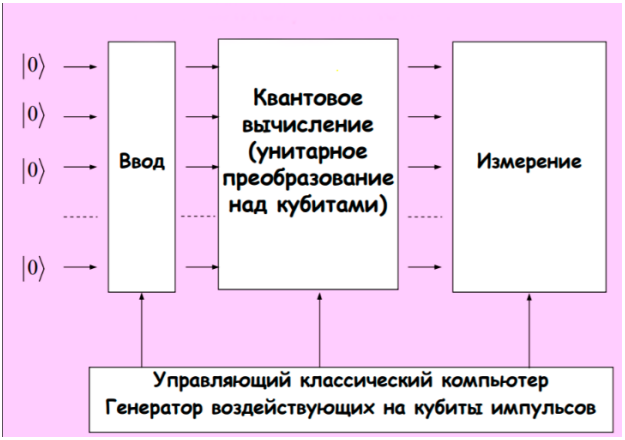

Рис.1 Схема квантового компьютера

Проблемы создания квантового компьютера - необходимо научиться приводить кубиты в определенные исходные состояния, объединять их в запутанные системы, изолировать эти системы от влияния внешних помех, считывать результаты квантового расчета.

Квантовые симуляторы — это узкоспециализированные аналоговые квантовые компьютеры, которые создаются с целью решения определенного класса задач.

Области применения квантовых вычислений и компьютеров -оптимизация, моделирование сложных систем, обработка данных, машинное обучение и информационная безопасность.

Задачи квантовых систем

— поиск в массивах неструктурированных данных (радикальное ускорение обработки больших данных);

— разложение чисел на простые множители (алгоритм Шора, важен для преодоления криптозащиты данных — квантовый компьютер за секунды способен сделать то, на что у суперкомпьютера уйдут миллиарды лет);

— быстрое генерирование последовательности подлинно случайных чисел (практическое применение — одноразовые ключи для гарантированно защищенной передачи данных по открытому каналу связи; очевидно, о решении именно этой задачи и сообщил Google);

— моделирование квантовых систем — молекул и материалов(практическое применение — фармакология, средства защиты от биологического оружия), причем для решения таких задач достаточен« маломощный» квантовый компьютер с регистром до 100 кубит.

СПИСОК ЛИТЕРАТУРА

1. Р.Ф. Фейнман. Квантово-механические ЭВМ // Успехи физических наук, УФН 149. — 1986. — С. 671–688. URL: **https://ufn.ru/ru/articles/1986/8/c/**(дата обращения 03.09.2019).
2. M.M. Waldrop. The chips are down for Moore's law // Nature. — 2016. — Vol. 530. — P. 144.
3. P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. — 1997. — N. 26. — P. 1484.
4. J. Preskill. Quantum Computing in the NISQ era and beyond // Quantum. — 2018. — N. 2. — P. 79.
5. Сергей Авдошин, Александра Савельева. Криптоанализ: вчера, сегодня, завтра // Открытые системы.СУБД. — 2009. — № 3. — С. 22–25. URL: **www.osp.ru/os/2009/03/8120956**(дата обращения: 12.09.2019).