Салпагарова Ш.Х., Байкулова Ф.А.

Принципы работы квантового компьютера и круг решаемых задач в современном мире

ФГБОУ ВО «Северо-Кавказская Государственная Академия»
(Россия, Черкесск)

doi: 10.18411/lj-11-2019-46

idsp: ljjournal-11-2019-46

Аннотация

Постоянная актуализация информации о последних достижениях и современных разработках позволяет более качественно прогнозировать развитие направлений фундаментальной и прикладной наук, корректировать область научных изысканий. В статье проводится обобщение информации о новейшей области электронно-вычислительных машин квантовом компьютере. Рассматриваются основные принципы, отличающие квантовую вычислительную машину от классического компьютера. Приводится пример коммерческого производства квантовых компьютеров. Описываются продолжающиеся фундаментальные исследования в области совершенствования квантовых компьютеров. Материал статьи позволит, не вдаваясь в подробное изучение квантовой физики, составить представление о работе квантового компьютера и проблематике этой области и ознакомиться со всеми последними достижениями в рамках разработки мощнейшей вычислительной машины, в основе работы которой лежат принципы квантовых вычислений.

Ключевые слова: квантовый компьютер, кубит, вычисления, информационная безопасность, физика.

Abstract

Constant updating of information about the latest achievements and modern developments allows to predict the development of fundamental and applied Sciences, to correct the field of scientific research. The article summarizes the information about the latest field of electronic computers quantum computer. The basic principles that distinguish a quantum computer from a classical computer are considered. An example of commercial production of quantum computers is given. The article describes the ongoing fundamental research in the field of quantum computers improvement. The material of the article will allow, without going into a detailed study of quantum physics, to get an idea about the work of a quantum computer and the problems of this area and get acquainted with all the latest achievements in the development of a powerful computer, which is based on the principles of quantum computing.

Keywords: quantum computer, qubit, computing, information security, physics.

Сейчас много говорят о новых технологиях вычисления — в частности, то и дело звучат слова «квантовые вычисления», «квантовый интернет» и даже «квантовая криптография». Посмотрим, что это такое и нужно ли оно нам. Начнём с квантового компьютера.

В обычном компьютере все вычисления основаны на понятии «бит». Это такой элемент, который может принимать значения 0 или 1. Физически это реализовано так:

1. В компьютере есть деталь под названием транзистор. Представим, что это кран на трубе: если его включить, вода польётся, если выключить — остановится.
2. В транзисторе вода — это электричество, и включение-выключение крана тоже зависит от электричества. Представьте, что краны соединены между собой так, что вода из одного крана включает или выключает другой кран, — и так каскадом по цепочке.

3. Транзисторы соединены таким хитрым образом, что когда они включаются и выключаются, на них можно производить математические вычисления.
4. Из-за того, что транзисторов очень много (миллиарды), а работают они очень быстро (близко к скорости света), транзисторные компьютеры могут очень быстро совершать математические вычисления.
5. Всё, что вы видите в компьютере, — это производные от вычислений. Вы видите окно, буквы, картинки, а где-то в самой-самой глубине это просто сложение и вычитание, а ещё глубже — включение-выключение кранов с электричеством на скорости света [5].

Транзистор в компьютере может принимать значение 1 или 0, то есть «включён» или «выключен». С точки зрения компьютерной логики, этот транзистор называется битом. Это минимальная единица информации в компьютере. Физически бит может быть в процессоре, на чипе памяти, на магнитном диске, но суть одна: это какое-то физическое пространство, которое определённо либо включено, либо выключено.

Ключевое слово здесь — «определённо». Программист и инженер может точно узнать, в каком состоянии находится тот или иной бит. Заряд в нём либо есть, либо нет, никаких промежуточных состояний там не существует.

В квантовом компьютере вместо битов — кубиты. Кубиты — это квантовые частицы, у которых есть интересная особенность: кроме стандартных 0 и 1 кубит может находиться между нулём и единицей — это называют суперпозицией. Нагляднее это видно на рисунке 1:

Рис. 1 - Кубит может принимать все значения, которые видны на цветной сфере

Ещё одна особенность кубитов — зависимость значения от измерения. Это значит, что программист не узнает значение кубита до тех пор, пока его не измерит, а сам факт измерения тоже влияет на значение кубита. Звучит странно, но это особенность квантовых частиц [2].

Именно благодаря тому, что кубит находится во всех состояниях одновременно до тех пор, пока его не измерили, компьютер мгновенно перебирает все возможные варианты решения, потому что кубиты связаны между собой. Получается, что решение становится известно сразу, как только введены все данные. Суперпозиция и даёт ту параллельность в вычислениях, которая ускоряет работу алгоритмов в разы.

Вся сложность в том, что результат работы квантового компьютера — это правильный ответ с какой-то долей вероятности. И нужно строить алгоритмы таким образом, чтобы максимально приблизить вероятность правильного ответа к единице.

Как делают кубиты и в чём сложность?

Максимально упрощённо: чтобы получить рабочий кубит, нужно взять один атом, максимально его зафиксировать, оградить от посторонних излучений и связать с другим атомом специальной квантовой связью.

Чем больше таких кубитов связано между собой, тем менее стабильно они работают. Для достижения «квантового превосходства» над обычным компьютером нужно не менее 49 кубитов — а это очень неустойчивая система.

Основная сложность — декогеренция. Это когда много кубитов зависят друг от друга и на них может повлиять всё что угодно: космические лучи, радиация, колебания температуры и все остальные явления окружающего мира [1].

Такой «фазовый шум» — катастрофа для квантового компьютера, потому что он уничтожает суперпозицию и заставляет кубиты принимать ограниченные значения. Квантовый компьютер превращается в обычный — и очень медленный.

С декогеренцией можно бороться разными способами. Например, компания D-Wave, которая производит квантовые компьютеры, охлаждает атомы почти до абсолютного нуля, чтобы отсечь все внешние процессы. Поэтому они такие большие — почти всё место занимает защита для квантового процессора.

Рис.2 - Квантовый процессор на девяти кубитах от Google

Зачем нужны квантовые компьютеры?

Одно из самых важных применений квантового компьютера сейчас — разложение на простые числа. Дело в том, что вся современная криптография основана на том, что никто не сможет быстро разложить число из 30–40 знаков (или больше) на простые множители. На обычном компьютере на это уйдёт миллиарды лет. Квантовый компьютер сможет это сделать примерно за 18 секунд [3].

Это означает, что тайн больше не будет, потому что любые алгоритмы шифрования можно будет сразу взломать и получить доступ к чему угодно. Это касается всего — от банковских переводов до сообщений в мессенджере. Возможно, наступит интересный момент, когда обычное шифрование перестанет работать, а квантовое шифрование ещё не изобретут.

Ещё квантовые компьютеры отлично подходят для моделирования сложных ситуаций, например, расчёта физических свойств новых элементов на молекулярном уровне. Это, возможно, позволит быстрее находить новые лекарства или решать сложные ресурсоёмкие задачи.

Сейчас квантовые компьютеры всего этого не умеют — они слишком сложные в производстве и очень нестабильные в работе. Максимум, что можно пока сделать, — заточить квантовый компьютер под единственный алгоритм, чтобы получить на нём

колоссальный выигрыш в производительности. Как раз для этих целей их и закупают крупнейшие компании — чтобы быстрее решать одну-две самые важные для себя задачи.

1. Душкин Р.В. Квантовые вычисления и функциональное программирование. Москва, 2014. 33 с.
2. Малыхина М.П., Герасимов Д.А. Симуляция квантовых вычислений. Краснодар: КГТУ, 2016. 9 с.
3. Сасскинд Л., Фридман А. Квантовая механика. Санкт-Петербург: Питер, 2015. С. 225-227.
4. Федотов И.Е. Модели параллельного программирования. Москва: Солон-Пресс, 2012. С. 182-183.
5. Флейгин О. Парадоксы квантового мира. Москва: Эксмо, 2012. С. 129 -131.
6. Дойч Д. Структура реальности. Наука параллельных вселенных. Москва: Альпина нон-фикшн, 2015. С. 114-117.
7. Reiffel, E., Polak, W. Quantum Computing: A Gentle Introduction. Cambridge, Massachusetts: TheMITpress, 2011. pp. 67-69.
8. Wichert, A. Principles of Quantum Artificial Intelligence. Hackensack: World Scientific Publishing Co, Pte. Ltd., 2014. pp. 77-78.
9. Кучма Н.А. Биокомпьютер в реальных процессах. Инженерный вестник Дона, 2013, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2013/2129.
10. Филатов В. А., Козырь О.Ф. Модель поведения автономного сценария в задачах управления распределенными информационными ресурсами. Инженерный вестник Дона, 2013, № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1771.

Салпагарова Ш.Х., Боташева З.А.

Применение платформы 1с:Предприятие 8.3 в системе высшего образования

*ФГБОУ ВО «Северо-Кавказская Государственная Академия»
(Россия, Черкесск)*

doi: 10.18411/lj-11-2019-47

idsp: lj-11-2019-47

Аннотация

В данной статье рассматриваются наиболее перспективные направления развития комплексных систем автоматизации вузов. За счет возможности доработки конфигураций и широких интеграционных возможностей платформы "1С: Предприятие 8" в целом решения на этой платформе позволяют успешно автоматизировать основную деятельность образовательной организации, повысить качество и доступность данных, оперативность получения информации, обеспечить взаимодействие с государственными информационными системами.

Ключевые слова: конфигурация, платформа, информационные технологии, «1С:Предприятие», автоматизация, ВУЗ, АИС.

Abstract

This article considers the most promising directions of development of complex automation systems of universities. Due to the possibility to refine configurations and wide integration capabilities of the platform "1C: Enterprise 8" as a whole, solutions on this platform allow to successfully automate the main activity of the educational organization, improve the quality and accessibility of data, speed of obtaining information, ensure interaction with state information systems.

Keywords: configuration, platform, information technology, "1C: Enterprise", automation, university, AIS.

Тенденция к изменению организационных форм взаимодействия, приводящая к росту слияний и поглощений крупных компаний, в последние годы дополнительно усиливается активной государственной политикой по укрупнению целого ряда отраслей путем создания объединенных отраслевых корпораций, а в образовательном