КВАНТОВЫЕ ЭЛЕКТРОННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Яковчик Н.В.

Навойчик В.В. – полковник кафедры РЭТ ВВС и войск ПВО

Современные универсальные цифровые электронные компьютеры базируются на полупроводниковой технологии. Беспрецедентные успехи в развитии полупроводниковой микроэлектроники, непрерывно продолжающиеся начиная с изобретения первого планарного транзистора в 1959 году, наиболее наглядно выражаются так называемым "законом Мура" (G.Moore), согласно которому число транзисторов а следовательно и вычислительная мощность в кристалле одной интегральной схемы в течение первых 15 лет удваивалось каждый год, а затем и до сих пор такое удвоение происходит за 1,5 года. Но на сегодняшний момент размер транзистора в процессоре достиг 20нм, что очень близко к пределу. Дальнейшее движение по этому пути увеличения производительности не возможно в связи с тем, что нельзя сделать транзистор меньше размеров атома, а также в потребности использования громоздких систем охлаждения. Другой способ увеличения производительности, создание компьютер на принципиально новых технологиях, одна из ни квантовые компьютеры.

Идея использования квантовых вычислений впервые была высказана советским математиком Ю.И. Маниным в 1980 году в его знаменитой монографии «Вычислимое и невычислимое». Правда, интерес к его труду возник лишь два года спустя, в 1982 году, после опубликования статьи на ту же тему американского физика-теоретика нобелевского лауреата Ричарда Фейнмана. Он заметил, что определенные квантово-механические операции нельзя в точности переносить на классический компьютер. Это наблюдение привело его к мысли, что подобные вычисления могут быть более эффективными, если их осуществлять при помощи квантовых операций.

Основная идея квантового вычисления состоит в том, чтобы хранить данные в ядрах атомов, изменяя их ориентацию в пространстве. Элементарная ячейка такого компьютера получила название квантовый бит (quantum bit = кубит). В отличие от привычной нам единицы информации – бита (binary digits = bits), который может принимать только два значения или «0» или «1», квантовый бит в соответствии с принципом неопределенности, постулируемым квантовой механикой, может находиться одновременно в состоянии и «0», и «1».

Таким образом, если классическое вычислительное устройство, состоящее из L вычислительных ячеек способно выполнять одновременно L операций, то для квантового устройства размером L кубит количество выполняемых параллельно операций будет равно 2 в степени L.

Для практического применения пока не создано ни одного квантового компьютера, который бы удовлетворял всем вышеперечисленным условиям. Однако во многих развитых странах разработке квантовых компьютеров уделяется пристальное внимание и в такие программы ежегодно вкладываются десятки миллионов долларов.

На данный момент наибольший квантовый компьютер составлен всего из семи кубитов. Этого достаточно, чтобы реализовать алгоритм Шора и разложить число 15 на простые множители 3 и 5.

В будущем квантовые компьютеры будут обладать огромными вычислительными мощностями что позволит использовать их в разных сферах жизни. Например, криптографический алгоритм RSA на данный момент считается одним из самых надежных и даже самый современный компьютер не в состоянии его взломать за и за сотни лет, но это сможет сделать квантовый компьютер. Возможно в связи с этим появится квантовая криптография для создания более надежных алгоритмов шифрования.

Список использованных источников литературы:

1. *Валиев К. А.* Квантовая информатика: компьютеры, связь и криптография // Вестник российской академии наук. — 2000. — Том 70. — № 8. — С. 688—6957

2. *К.А.Валиев, А.А.Кокин.* Квантовые компьютеры: надежды и реальность // Регулярная и хаотическая динамика – 2001