

УДК 004

КВАНТОВЫЕ КОМПЬЮТЕРЫ: ПРЕДПОСЫЛКИ, ЗАДАЧИ, ПЕРСПЕКТИВЫ

Хачай Д. С., Кабанов А. С., студенты гр. ССб – 201, II курс
Колокольников А.И., к.т.н., доцент
Кузбасский государственный технический университет
имени Т. Ф. Горбачева
г. Кемерово

Ученые Института науки Вейцмана разработали одну из примерно 30 квантовых систем в мире и одну из менее десятка, в которых используется передовая технология захвата ионов, когда ионы удерживаются в небольшом пространстве при помощи магнитных и/или электрических полей. По расчетам израильских ученых потребуется примерно год, чтобы из устройства на 5 кубит создать квантовую машину WeizQC на 64 кубита [1].

Зарождению квантовых компьютеров способствовал физик-теоретик Ричард Филлипс Фейнман, который доказал, что термодинамических ограничений в вычислительных способностях компьютера нет. Этот факт свидетельствует о том, что вычисления можно совершить обратимым образом. Это любопытно, ведь вычисления на классических компьютерах необратимо: вся информация может находиться только в одном состоянии — в виде нулей и единиц (бит).

С середины 1980-х годов в работах таких ученых, как Дэвид Дойч, Итан Бернштейн, Умеш Вазрани были описаны модели квантовых компьютеров. Одной из них являлась квантовая машина Тьюринга. В основе создания транзисторов и лазера лежат явления квантовой физики.

В отличие от обычного в квантовом компьютере используются квантовые биты (кубиты). Кубит — квантовый разряд, наименьший элемент для хранения информации в квантовом компьютере. Кубитом может быть любой объект, проявляющий квантовое поведение. Если 3 бита — это 8 состояний, то 3 кубита — это одно состояние всех 8 состояний [2, 3].

В квантовых решениях для передачи и обработки данных используются явления квантовой механики. Следует напомнить, что именно квантовой механике мы обязаны появлением компьютеров, ноутбуков и смартфонов.

При рассмотрении математических основ функционирования квантовых компьютеров важно понимать, что законы квантового мира существенно отличаются от законов нашего мира. Стандартным образом, кванты ведут себя лишь при постоянном измерении состояния, в каком они находятся. При прекращении измерений квантовые частицы переходят сразу в несколько положений. Например, если электрон частично находится сразу в трех точках, это не означает, что он делится на несколько частей. После измерения электрон оказывается в единственной точке несмотря на то, что с точки зрения

квантовой статистики он успел побывать в нескольких местах. Такое состояние называют суперпозицией. Особенность квантовых частиц, когда они могут находиться во многих состояниях, называют квантовым параллелизмом.

С увеличением числа кубитов количество состояний, в которых находится квантовый процессор, возрастает за счет их возможности связываться между собой. Это позволяет квантовым компьютерам решать задачи во много раз быстрее обычных и суперкомпьютеров.

Для выполнения квантовых вычислений используются коллективные свойства квантовых состояний, такие как суперпозиция и запутанность.

Устройства для реализации квантовых вычислений принято разделять на квантовые компьютеры и квантовые симуляторы. Функционирование универсальных квантовых компьютеров базируется на использовании квантовых эффектов. Существует два типа квантовых компьютеров. В основе работы квантовых компьютеров первого типа лежит квантование магнитного потока на нарушение сверхпроводимости. На эффекте протекания сверхпроводящего тока через разделяющий два сверхпроводника тонкий слой диэлектрика делают линейные усилители, аналого-цифровые преобразователи, СКВИДы и корреляторы. Известны проект создания RISC-процессора на RSFQ-логике и проект создания петафлопного компьютера. Экспериментально достигнута тактовая частота 370 ГГц. Второй тип квантовых компьютеров основан на поддержании когерентности волновых функций используемых кубитов на протяжении всего времени вычислений. Часто именно такой тип устройств называют квантовым компьютером.

При помощи суперпозиции, в которой единица измерения информации существует в нескольких состояниях одновременно, квантовая машина может сохранять и обрабатывать в один момент намного больше данных, чем любое другое вычислительное устройство, существующее в настоящее время. При этом огромными объемами данных можно управлять при помощи квантового параллелизма. Вычислять и анализировать разные состояния одновременно квантовые системы могут с высокой скоростью.

С помощью квантовых систем стало возможным решение проблемы коммивояжера – задачи, требующей нахождения кратчайшего маршрута. Решение такой задачи позволит рационально выстраивать маршруты по всему миру, что упростило бы перемещения грузов и людей. Подобного рода исследования уже проводят такие экономические гиганты, как Volkswagen, совместно с D-Wave и Google.

Специалисты швейцарской фармацевтической компании Roche надеются, что квантовое моделирование ускорит разработку вакцин для защиты от инфекций, подобных COVID-19, лекарств от гриппа, рака и даже болезни Альцгеймера.

Существование квантового компьютера позволит как находить новые методы шифрования, так и взламывать новые уровни шифров различного уровня сложности [4]. В скором времени есть вероятность распространения квантовых криптографических систем. Квантовая криптография дает

возможность обмениваться сообщениями незаметно. При попытке перехвата данного сообщения, оно будет искажено так, что восстановить его будет невозможно.

Классической системе, реализующей квантовый компьютер, можно предъявить ряд обязательных требований. Степень изоляции от внешней среды и последовательность преобразований фазового пространства являются сложными задачами на пути создания полноценного квантового компьютера. Хотя и измерить состояние отдельной частицы тоже непростая задача.

Квантовые компьютеры фактически среди нас. Их разработкой занимаются Google, Intel, IBM, Microsoft и другие компании поменьше. В каждом более-менее крупном институте мира есть исследовательские группы, которые ведут эксперименты по разработке квантового компьютера, так что появление сверхмощных вычислительных машин — это вопрос нескольких лет. Так, компания IBM, выпускающая электронную аппаратуру и программное обеспечение, уже анонсировала выпуск первого коммерческого квантового компьютера к 2023 году мощностью в 1121 кубит. Уже ведутся работы по созданию компьютера на миллионы кубитов, именно эти мощные вычислительные машины раскроют истинный потенциал квантовых компьютеров.

С применением квантового компьютера в наукоемких сферах производства, в области криптографических алгоритмов, связи, медицины появится возможность в кратчайшие сроки создавать сложные модели различных объектов, повысить эффективность производства. В социальной сфере внедрение квантовых компьютеров позволит разрабатывать новые лекарственные соединения для оказания больным эффективного лечения. Таким образом, разработка квантового компьютера окажет эффективное влияние на многие сферы деятельности человека.

Список литературы:

1. В Израиле создали первый в стране квантовый компьютер // SberPress : [сайт]. — 2022. — URL: https://news.rambler.ru/tech/48363479/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 19.03.2022).
2. Глушков Е. Просто о сложном: что такое квантовый компьютер и зачем он нужен // Хайтек : сайт. — URL: <https://theoryandpractice.ru/posts/13588-kvantovyy-komputer> (дата обращения 27.03.2022)
3. Проць С. Квантовый процессор: описание, принцип работы // FB.ru: сайт. — URL: <http://fb.ru/article/321935/kvantovyyi-protssor-opisaniie-printsip-raboty> // (дата обращения 26.03.2022).
4. Авельсник Н. Криптография не устоит перед мощью квантовых компьютеров // hightech.fm: сайт. — URL: https://hightech.fm/2016/05/11/quantum_computing_cryptography#! (дата обращения 25.03.2022).