

УДК 621.315.375

**ПЕРСПЕКТИВЫ СОЗДАНИЯ
КВАНТОВЫХ КОМПЬЮТЕРОВ***Попова И. Г., Грицай И. П., Скворцова Н. С.*

Донской государственной технической,
университет, Ростов-на-Дону, Российская
Федерация

inna111109@rambler.rugritsay.irina@rambler.ruskvorcova16@rambler.ru

Рассматриваются перспективы организации вычислений нового типа — параллельных вычислений на квантовых компьютерах, единичными элементами которых являются кубиты, которые могут находиться в состояниях «0» и «1», но и в их суперпозиции.

Ключевые слова: квантовый компьютер, кубиты, вычислительное устройство, квантовые алгоритмы, вычислительная техника.

Введение. Современные электронные технологии стремительно развиваются, скорость вычислений удваивается каждые два года. То, что было фантастикой пару лет назад, на глазах становится реальностью. Информация стала незаменимой частью нашей жизни. Человеческое общество ищет все новые способы и механизмы ее обработки и передачи.

Сейчас перед человечеством стоят такие задачи, которые не сможет решить даже самый мощный классический компьютер, занимающий по своим габаритам целые здания. На помощь привычным приходят квантовые компьютеры, которые могут решать задачи любой сложности.

Квантовый компьютер — вычислительное устройство, которое использует квантовую природу микрообъектов: их способность находиться для передачи и обработки данных в состоянии «суперпозиции» и хранить не «0» или «1», а сразу несколько состояний одновременно. Микромир — одна из самых сложных областей, которые изучает физика. Цель данной работы — рассказать о компьютере будущего, истории его создания, проблемах, которые предстоит решить в ходе ожидаемого прорыва в технологиях, что позволит создать это пока гипотетическое устройство.

Обсуждение результатов исследований. На сегодняшний день полномасштабный квантовый компьютер — это чисто гипотетическое устройство. Создать подобный прибор человечество сможет только после нового ожидаемого прорыва в технологиях. Создание квантового компьютера и его внедрение в повседневную жизнь является одной из основных задач физики XXI века.

Первые идеи о создании квантовых компьютеров были высказаны еще в прошлом веке. Историю развития квантовой вычислительной техники можно разделить на несколько этапов. Первый этап начался в 1980 году. Советский математик Ю. И. Манин написал две знаменитые книги по логике, «Вычислимое и невычислимое» и «Доказуемое и недоказуемое», описав теорию квантовых вычислений [1–2]. Эта проблема стала активно обсуждаться после того, как американский физик-теоретик Р. Фейнман в 1981 году описал первую модель квантового компьютера [3]. Вскоре Пол Бенниофф описал теоретические основы построения такого компьютера, в которых он предложил использовать квантовые алгоритмы. Стивен Визнер в 1983 году опубликовал общую концепцию квантового компьютера [4]. В середине восьмидесятых годов Дэвид Дойч описал конкретную математику

UDC 621.315.375

**PROSPECTS FOR CREATING QUANTUM
COMPUTERS***Popova I. G., Gritsay I. P., Skvortsova N. S.*

Don State Technical University, Rostov-on-Don,
Russian Federation

inna111109@rambler.rugritsay.irina@rambler.ruskvorcova16@rambler.ru

The paper considers the prospects for organizing a new type of computing — parallel computing on quantum computers, the individual elements of which are qubits, which can be in states “0” and “1”, as well as in their superposition.

Keywords: quantum computer, qubits, computing device, quantum algorithms, computing

ческую модель квантового компьютера — квантовую машину Тьюринга. Все эти события дали толчок к развитию квантовой вычислительной техники. Однако в то время невозможно было создать этот прибор. Физическое построение такого компьютера тогда считалось фантастикой.

Ситуация в сфере квантовой вычислительной техники кардинально меняется и переходит на новый этап развития в 1994 году. Американский математик Питер Шор публикует статью, в которой построен квантовый алгоритм факторизации. В 1996 году Л. Гровер предложил квантовый алгоритм быстрого поиска в неупорядоченной базе данных. Все это привело к массовой публикации материалов, посвященных квантовым вычислениям. И уже в начале 2000 годов во многих научных лабораториях были созданы первые однокубитные квантовые процессоры (Q-бит, или кубит — многомерный аналог традиционного бита, наименьший элемент для хранения информации, одновременно может хранить «0» или «1» в отличие от бита) [5].

Третий этап характеризуется инновационной гонкой. Квантовые компьютеры активно изучают лучшие умы мира, в их разработку вкладываются крупнейшие корпорации: Google, IBM, Microsoft, Alibaba, Intel. Страны стремятся стать лидерами, спонсируя научно-технические лаборатории и квантовые центры. За 18 лет научного прогресса человечество далеко продвинулось в своих исследованиях. В январе 2018 года компания Intel заявили о создании сверхпроводящего квантового чипа под кодовым именем Tangle Lake, оперирующего 49 кубитами. А уже в марте 2018 года компании Google удалось построить 72-кубитный квантовый процессор Bristlecone, показавший низкий процент ошибок в вычислениях. Компания не раскрывает подробных характеристик своего устройства, но утверждает, что оно позволяет достичь «квантового превосходства». Однако лидерство одержала канадская компания D-Wave, которой удалось создать 128-кубитную машину D-Wave One, состоящую по меньшей мере из 1000 кубитов.

Квантовые компьютеры способны открыть для человечества новые горизонты и с тем же успехом разрушить все коммуникации и безопасность в целом. «Квантовый компьютер функционирующий гораздо страшнее атомной бомбы», — считает генеральный директор компании Acronis, сооснователь Российского квантового центра Сергей Белоусов. Квантовые компьютеры способны буквально поставить на колени тех, кто так или иначе зависит от интернета. Квантовый компьютер использует алгоритм Шора, который способен разложить огромное число на два простых множителя. Традиционный компьютер с подобным алгоритмом не справится, он постепенно будет перебирать все возможные комбинации и затратит на вычисления сотни лет. Таким недостатком классической вычислительной техники воспользовались криптографы для шифрования защищенных данных. Только представьте себе, что у кого-то появляется квантовый компьютер, он первым делом запустит алгоритм Шора, и все защищенные в мире данные станут ему доступны. Ученые довольно давно пытаются опередить квантовые вычисления и придумали квантовую криптографию, когда информация записывается в квантовое состояние отдельных фотонов и пересылается по оптическим каналам связи. Такой системой уже пользуются некоторые банки в Швейцарии, и она начитает активно внедряться по всему миру [6].

Несмотря на всю свою опасность квантовые компьютеры нам необходимы. Они способны решить ряд ключевых задач, актуальных для человечества, такие как взлом и шифрование информации, анализ больших неупорядоченных динамических баз данных, оптимизация процессов. Одной из возможных задач для квантового компьютера может являться задача поиска необходимых материалов или лекарств. Квантовый алгоритм позволит обрабатывать массив данных намного быстрее и дешевле. Например, таким способом можно найти высокотемпературные сверхпроводники, которые проводят электричество без каких-либо потерь при комнатной температуре и существенно сэкономят наши ресурсы и финансы.

Квантовый компьютер работает за счет квантового параллелизма, основным свойством которого является суперпозиция. Она заключается в том, что элементарные частицы могут находиться в двух взаимоисключающих состояниях одновременно. Для классических компьютеров минимальной единицей измерения информации являются биты, которые могут принимать значение «0» или «1», в квантовых компьютерах такой единицей измерения являются когерентные биты или кубиты, которые могут быть и нулем, и единицей одновременно [7].

Для сравнения классического и квантового компьютера можно рассмотреть математическую задачу. По условию нам необходимо найти маршрут через пять разных городов, который будет самым быстрым и экономичным. Обычный компьютер по очереди рассчитывает длину пути и затраты для каждого из возможных маршрутов, потом поэтапно проанализирует все полученные данные и выберет самый выгодный маршрут. Квантовый компьютер будет выполнять те же самые расчеты одновременно. Сейчас мы разницу между работой этих приборов проследить не сможем, но если мы изменим условие, и теперь нам будет необходимо проложить тот же самый маршрут только уже через 200 городов, то сразу сможем увидеть преимущество квантового компьютера. Поскольку кубиты могут обрабатывать значительно больше информации одновременно, то они найдут решение значительно быстрее.

Роль кубитов могут играть различные физические системы: атомы, ионы, электроны, фотоны. Весьма перспективными на сегодняшний день являются сверхпроводящие кубиты. Основное преимущество их заключается в массивности объекта. Электроны сложно удержать в определенной точке, со сверхпроводящими кубитами подобных проблем не возникает. Эти кубиты представляют собой кольца с джозефсоновскими переходами. Поскольку их выполняют из сверхпроводника, электроны в нем текут не беспорядочно, как в металлах, а объединяются в пары и таким образом упорядоченно перемещаются по кольцу. Также электроны могут туннелировать в переходах без затрат энергии как в самих переходах, так и в кольце в целом. Чтобы работать с кубитами, их необходимо изолировать от окружающего мира, так как они по своей природе очень хрупкие и любые воздействия из внешней среды разрушают любую квантовость. Для того чтобы измерить кубиты, их необходимо максимально охладить до температуры 10 мКл. Охлаждение осуществляется криостатами, которые работают на смеси жидкого гелия.

Заключение. Создание полноценного квантового компьютера — фундаментальная проблема физики, тесно связанная как с математическим формализмом, так и с алгоритмами. И сейчас человечество стоит на пороге решающих открытий, за которыми начнется эра квантовой информации.

Библиографический список

1. Манин, Ю. И. Вычислимое и невычислимое / Ю. И. Манин. — Москва : Советское радио, 1980. — 128 с.
2. Манин, Ю. И. Доказуемое и недоказуемое / Ю. И. Манин. — Москва : Советское Радио, 1979. — 88 с.
3. Фейнман, Р. Ф. Внизу полным-полно места: приглашение в новый мир физики / Р. Ф. Фейнман // Российский химический журнал. — 2002. — Т. XLVI, № 5. — С. 4–7.
4. Weisner, S. Conjugate coding. / S. Weisner // Association for Computing Machinery, Special Interest Group in Algorithms and Computation Theory. — 1983. — Т. 15. — С. 78–88.
5. Холево, А. С. Квантовая информатика : прошлое, настоящее, будущее / А. С. Холево // В мире науки. — 2008. — № 7. С. 68–75.
6. Biggest quantum computer [Электронный ресурс] / Geek.com. — Режим доступа : <https://www.geek.com/chips/biggest-quantum-computer-to-date-544054/> (дата обращения: 11.08.2019).
7. Физическая энциклопедия. Том 4. Пойнтинга–Робертсона стримеры. — Москва : Большая Российская энциклопедия, 1994. — 704 с.