

## КВАНТОВЫЙ КОМПЬЮТЕР ОТ ТЕОРИИ К ПРАКТИКЕ

Ганин С.А.

г. Ставрополь, МБОУ «СОШ №11», 11 класс

Руководители: Газимагомедова К.А., г. Ставрополь, МБОУ «СОШ №11», учитель физики, высшей квалификационной категории;

Белоус О.Н., г. Ставрополь, МБОУ «СОШ №11», учитель математики высшей квалификационной категории

*«Мы сделаем свои биты. С суперпозицией и запутанностью».*

Ричард Фейнман 1981

Обычные компьютеры вошли в нашу повседневную жизнь. С каждым годом они становятся все лучше и лучше. Но наступит момент, когда компьютеры достигнут пика. Настанет время, когда обычные компьютеры перестанут улучшаться в связи с физическими параметрами. И на смену им придут квантовые компьютеры. На данный момент разработкой квантового компьютера занимаются такие компании как: D-WAVE (Канадская компания), IBM (Американская компания), Google (Американская компания), Intel (Американская компания) и другие. Квантовый компьютер сможет решать многие задачи в сотни раз быстрее чем обычный компьютер. Например, разложения простых чисел на множители. Обычный компьютер с этой задачей способен справиться за большой промежуток времени, порой превышающий время существования вселенной.

Многие опасаются квантовых компьютеров, так как они будут способны взломать любой пароль и смогут узнать любую закодированную информацию. Но, с приходом квантовых компьютеров, придет новая система безопасности.

Развития квантовых технологий можно разделить на два этапа. Благодаря первому этапу были изобретены такие предметы как лазер, CD, флеш-память и магнитно-резонансный томограф. Сейчас идет второй этап развития квантовых технологий. Главным изобретением второго этапа должен стать мощный квантовый компьютер. На данный момент существуют квантовые компьютеры, но их производительная мощность пока мала. Самый мощный квантовый компьютер (51-кубитный) был разработан в июле 2017 года физиками из Российского квантового центра под руководством Михаила Лукина. В настоящее время компания Google работает над 49-кубитным квантовым компьютером.

Существует очень много проблем в создании квантового компьютера. Одна из самых главных – это взаимодействие с окру-

жающей средой. Квантовый компьютер не устойчив к электромагнитным волнам, радио волнам, он работает только при низких температурах.

**Цель проекта.** Изучить основные проблемы создания квантового компьютера.

**Гипотеза.** Квантовый компьютер – машина, которая объединяет в себе достижения компьютерной науки и квантовой физики.

**Актуальность.** Потребности человечества в производительности компьютерных процессоров уже сейчас обгоняют развитие классической электроники. Квантовый компьютер – это вероятность сделать скачок на более высокий уровень развития всего человечества. И создание квантового компьютера, способного решать некоторые важные вычислительные задачи гораздо быстрее обычного, – одно из возможных направлений развития.

**Задачи:**

1. Определить, какие внешние факторы влияют на работу квантового компьютера.
2. Выяснить, где может применяться квантовый компьютер.
3. Проанализировать, какие существуют преимущества квантового компьютера перед обычным компьютером.

### История возникновения квантовых компьютеров

Первым, кто предложил использовать квантовые вычисления был Ю.И. Манин. В 1980 он публикует свою работу «Вычислимое и невычислимое», в которой предлагает использовать квантовые вычисления. В 1982 году Ричард Фейнман публикует свою статью, в которой говорит о том, что определённые квантово-механические операции нельзя в точности переносить на классический компьютер. Дэвид Дойч в 1985 предложил математическую модель квантового компьютера. Квантовые вычисления до середины 90-х годов развивались очень слабо. На практике оказалась довольно сложно реализовать квантовый компьютер. Но в 1994 Питер Шор предложил алгоритм разложения  $n$ -значного числа на простые множители за время по-

линомиально зависящее от  $n$ . Этот алгоритм называют квантовым алгоритмом факторизации. Благодаря этому открытию началось стремительно развитие квантовых вычислений. В 2000 году продемонстрирован первый работающий пяти кубитный квантовый компьютер в Мюнхенском техническом университете. 2007 канадская компания D-WAVE продемонстрировала первый 16-кубитный и 28-кубитный квантовый компьютер. В 2011 году они выпустили квантовый компьютер с 128-битным чипом. В 2013 с 512-битным чипом. На самом деле эти компьютеры способны справиться только с одной определенной задачей. Из-за этого на данный момент самым мощным квантовым компьютером считается 51-кубитный квантовый компьютер, который разработали Русские ученые в 2017 году.

### Устройство

Квантовый компьютер состоит из:

- 1 – классическая быстродействующая ЭВМ;
- 2 – квантовый процессор;
- 3, 4 – устройства записи информации в квантовые регистры;
- 5 – устройство управления квантовыми операциями;
- 6 – устройство считывания информации с кубитов. (См. Приложение 1)

Основы функционирования

Для того чтобы разобраться как работает квантовый компьютер давайте в начале разберёмся на каких основах он работает.

1. Квантовая суперпозиция.
2. Квантовая запутанность.
3. Квантовый параллелизм. Основным элементом квантового компьютера является
4. Кубит.

1) Квантовая суперпозиция – это способность атома находится в нескольких местах одновременно. К примеру, бит состоит из 1 и 0, то есть он может принимать только одно значение один или ноль. Кубит тоже состоит из 1 и 0. Но он может принимать эти два значения одновременно. Такое состояние кубита и называется суперпозицией.

2) Квантовая запутанность – это квантовое состояние двух частиц, которые оказываются взаимозависимыми друг от друга. К примеру, поляризация фотона, когда фотон проходит через кристалл и разделяется на две части и обе эти части проходят через фильтр. Оба этих фотона могут пройти через фильтр либо не пройти. Причем фотоны принимают решение мгновенно, то есть, быстрее, чем скорость света. Они находятся на расстоянии, но при этом связаны между собой.

3) Квантовый параллелизм. В основе квантового параллелизма лежит исполь-

зование при вычислениях суперпозиций базовых состояний, что позволяет одновременно производить большое количество вычислений с различными исходными данными. К примеру, 54-разрядный квантовый регистр может хранить до  $2^{54}$  значений одновременно, а квантовый компьютер может все эти значения обрабатывать.

4) Кубит является основной ячейкой квантового компьютера и квантовой частицей, имеющей два базовых состояния 1 и 0 или оба этих состояния одновременно.

### Принцип работы

Мы сами разобрали четыре основных базиса, благодаря которым функционирует квантовый компьютер. Теперь давайте разберем принцип работы квантового компьютера. Квантовый компьютер – это вычислительное устройство, которое работает за счет квантовой суперпозиции и квантовой запутанности для передачи и обработки данных. Зная, что кубит может принимать сразу два состояния 0 и 1, можно сказать, что это позволяет проводить несколько вычислений одновременно.

Существует множество алгоритмов, за счет которых работает квантовый компьютер. Алгоритм Шора был разработан в 1994 году Питером Шором. Этот алгоритм позволяет разложить простые числа на множители. В 2001 году с помощью этого алгоритма на квантовом компьютере разложили число 15 на множители 3 и 5. Алгоритм Залки-Визнера предназначен для моделирования квантовых систем. Алгоритм Гровера предназначен для решения уравнений. Алгоритм Дойча – Йожи был предложен Давидом Дойчем и Ричардом Йожей в 1992 году. Алгоритм Дойча – Йожи стал одним из первых алгоритмов, предназначенных для выполнения на квантовых компьютерах. Задача которую может решить алгоритм Дойча – Йожи заключается в определении, является ли функция нескольких двоичных переменных  $f(x_1), f(x_2), \dots, f(x_n)$ , постоянной (при любых аргументах принимает значение либо 1 либо 0) или сбалансированной (для одной половины области определения принимает 1, а для другой половины 0). При этом мы знаем, функция является либо постоянной, либо сбалансированной.

### Классификация

Можно выделить два типа квантовых компьютеров. Они основываются на квантовых явлениях, только разного порядка.

В основе первого типа квантовых компьютеров лежит квантование магнитного потока на нарушениях сверхпроводимости. На этих эффектах делают аналого-цифровые преобразователи, линейные усилители.

Для второго типа квантовых компьютеров требуется постоянное поддержание когерентности волновых функций используемых кубитов в течение всего времени вычислений. Их ещё называют квантовые когерентные компьютеры. Для некоторых вычислительных задач мощность когерентных квантовых компьютеров равна  $2^N$ .  $N$  – это число кубитов в компьютере. Когда говорят о квантовых компьютерах, имеют в виду последний тип устройств.

### Проблемы и пути решения созданий квантовых компьютеров

При разработке квантового компьютера возникло множество проблем, которые требуется решить для того, чтобы квантовый компьютер эффективно работал.

Можно выделить несколько наиболее важных проблем:

1. Неустойчивость квантовой суперпозиции.
2. Взаимодействие квантовых компьютеров с внешней средой.
3. Квантово-механическая стабильность физической системы.

1) Неустойчивость квантовой суперпозиции. В момент, когда кубит находится в суперпозиции, на него может повлиять любое взаимодействие с внешней средой. Из-за чего он принимает одно единственное значение и теряет свои вычислительные свойства. Во время квантовых вычислений кубит должен быть полностью изолирован от внешней среды.

2) Взаимодействие квантовых компьютеров с внешней средой. Из первой проблемы как следствие вытекает вторая. Для того, чтобы кубит «мог долго находится в суперпозиции», ему нужен ряд условий:

а) Полный вакуум, то есть отсутствие других каких-либо частиц.

б) Очень низкие температурные условия. Квантовый 5-кубитный компьютер IBM Quantum Experience работает при 0,024K (–273,126 градуса Цельсия). При такой низкой температуре замедляются движения молекул.

3) Нужно уметь воздействовать на отдельные кубиты. А также иметь возможность измерить состояние квантовой системы на входе.

Область применения квантовых компьютеров

1. Медицина. Молекулярное моделирование может создать новые лекарства и моделировать свойства химических веществ. Например, Google уже смогли симулировать энергию молекулы водорода.

2. Финансовые услуги. Квантовый компьютер сможет моделировать разные фи-

нансовые ситуации и предотвращать риски при большом количестве случайных сценариев.

3. Прогноз погоды. Создание модели климата для предотвращения стихийных бедствий и моделирования влияния человека на окружающую среду.

4. Квантовая криптография. Создание новых надежных алгоритмов шифрования. Например, чтобы взломать алгоритм классическим компьютером, нужно перебрать все возможные варианты. Это требует огромного количества времени, что делает эту операцию дорогостоящей и не практичной. А квантовые компьютеры могут выполнять такое разложение гораздо быстрее и эффективнее. И это не весь список, ведь по мере развития квантовых компьютеров будут расширяться возможности и сферы их применений.

5. Моделирование других квантовых систем. Например, моделирование молекулы сложных химических соединений (белков).

### Заключение

Вместе с квантовым компьютером наступит новая эра вычислений и научных открытий. Если создать квантовый компьютер из 200 кубитов, то мощность этого компьютера будет равна больше чем число атомов во всей вселенной. Что позволит моделировать различные физические системы.

На данный момент я работаю над созданием макета квантового компьютера, который будет показывать основной принцип работы квантовых вычислений. Он будет работать на фотонах (Приложение 2). Эта схема моего квантового компьютера на фотонах. На этом макете я планирую проверить работу алгоритма Дойча – Йожи.

Также я проверил работу алгоритма Дойча – Йожи на настоящем 2-кубитном квантовом компьютере компании IBM (См. Приложение 3). По результатам этого опыта можно сказать, что функция является сбалансированной (См. Приложение 4). Квантовый компьютер это прорыв в науке.

### Выводы

Пока квантовые компьютеры способны выполнять простые задачи. Но в дальнейшем, с развитием квантовых технологий и вычислений, они будут способны выполнять очень сложные задачи, которые не способен выполнить простой компьютер. В квантовом компьютере скрыт большой потенциал.

Если говорить о конкретных темах физики из раздела «Квантовая физика», применяемых для создания и работы квантового компьютера, то это:

Полупроводники. Твердотельные квантовые точки на полупроводниках: в качестве кубитов используются зарядовые состояния электронного и ядерного спина в данной квантовой точке. Управление через внешние потенциалы или лазерным импульсом.

Сверхпроводники. Сверхпроводящие элементы. В качестве логических кубитов используются присутствие или отсутствие куперовской пары в определённой пространственной области. Управление: внешний потенциал, т.е. магнитный поток.

Фотоны. Смешанные технологии: использование заранее приготовленных запутанных состояний фотонов для управления атомными группами или как элементы управления классическими вычислительными сетями.

Проведя данные исследования, я пришел к выводу, что квантовый компьютер объединяет в себе достижения компьютерной науки и квантовой физики, следовательно, гипотеза подтвердилась.

#### Список литературы

1. Feynman R. Int. J. Theor. Phys. 21, 1982.
2. Манин Ю.И. Вычислимое и невычислимое. – М.: Советское радио, 1980.
3. Feynman R. Quantum mechanical computers // Optics News, February 1985, 11, p.11.

4. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. – Proc. R. Soc. London A 400, 97, 1985.

5. Deutsch D. Quantum computational networks. – Proc. R. Soc. London A 425, 73, 1989.

6. Yao A. C.-C. Quantum circuit complexity // Proceedings of the 34th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1993, p. 352.

7. Shor P.W. Algorithms for Quantum Computation: Discrete log and Factoring. // Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, CA, 1994, p.124.

8. Китаев А.Ю. Квантовые вычисления: алгоритмы и исправление ошибок. // Успехи математических наук.

9. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 212–219.

10. Kitaev A.Y. Quantum measurements and the Abelian stabilizer problem. – LANL e-print quant-ph/9511026. – <http://xxx.lanl.gov>.

11. Shor P.W. Fault-Tolerant Quantum Computation. – LANL e-print quant-ph/9005011. – <http://xxx.lanl.gov>.

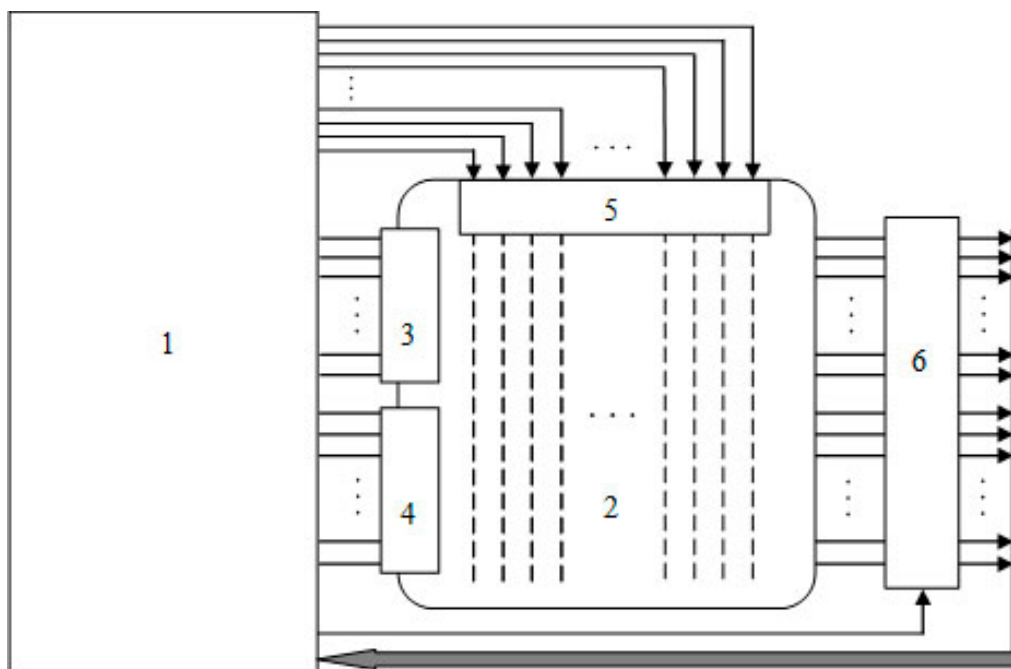
12. Bennett C.H., Bernstein E., Brassard G., Vazirany U. Strengths and Weaknesses of Quantum Computing. – LANL e-print quant-ph/9701001, <http://xxx.lanl.gov>, to appear in SIAM J. On Computing.

13. <https://meduza.io/cards/suschestvuyut-li-kvantovye-kompyutery-na-samom-dele>.

14. <https://www.research.ibm.com/ibm-q/>.

15. <https://ru.wikipedia.org>.

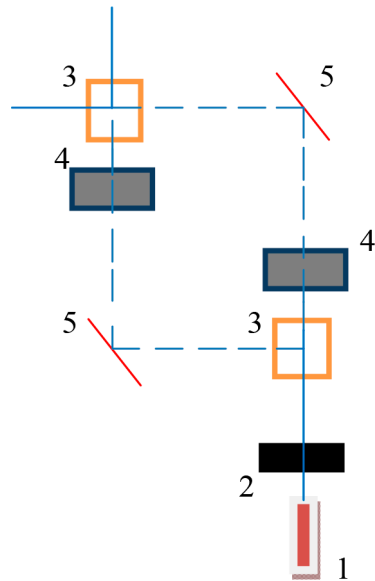
## Приложение 1



Функциональная схема аппаратуры для квантовых вычислений:

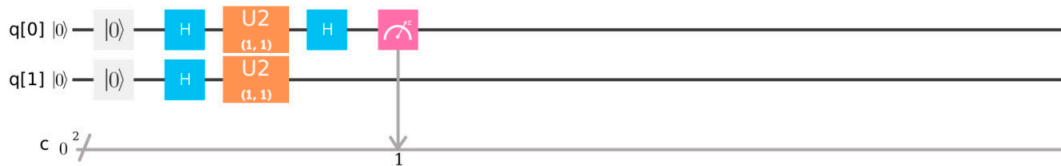
1 – классическая быстродействующая ЭВМ; 2 – квантовый процессор; 3, 4 – устройства записи информации в квантовые регистры; 5 – устройство управления квантовыми операциями; 6 – устройство считывания информации с кубитов

Приложение 2



Модель квантового компьютера на фотонах:  
 3, 5, 1 – лазер; 4 2 – линейный поляризатор; 4 3 – светоделительный кубик; 5 3 4 – полуволновая  
 пластина; 5 – зеркало

Приложение 3



Алгоритм Дойча – Йोजи

Приложение 4



Результат алгоритма Дойча – Йोजи