Министерство образования и науки РФ

Федеральное государственное бюджетное образовательное учреждение

"Тверской государственный технический университет"

(ФГБОУВПО "ТвГТУ")

Кафедра "Программное обеспечение"

Отчет по курсовой работе

Выполнили:

студенты группы ПИН.РИС.-17.06

Астахова М. А.

Верховская П. С.

Проверил: Новиков И. В.

Тверь, 2019

**Оглавление**

Зачем нужны квантовые вычисления?..........................................................3

Схема квантового компьютера……………………………………………..4

Схема Блоха………………………………………………………………….6

Проблема измерений………………….……………………………………..7

Искусственный интеллект……………..……………………………………7

Вывод…………………………………………………………………….......10

Список литературы………………………………………………………….11

**Зачем нужны квантовые вычисления?**

1. Современные компьютеры все еще неспособны решать ряд важных задач: • Криптография • Моделирование квантово-механических систем 2. Хотя классические компьютеры становятся все мощнее и мощнее, имеются физические ограничения на рост их производительности. Зачем нужны квантовые вычисления? Моделирование физических систем ”I’m not happy with all the analyses that go with just classical theory, because Nature isn’t classical, dammit, and if you want to make a simulation of Nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem!” Richard Feynman 1981 Может ли универсальный классический компьютер точно промоделировать квантовомеханические системы ? Может ли классический компьютер эффективно моделировать квантовомеханические процессы ? Ограничения классических компьютерных технологий (H.Wiedman) • Закон Мура: – Gordon E. Moore – Сформулирован в 1965. – Предсказывает, что число транзисторов в чипе будет удваиваться каждые – 18-24 месяца. • Проблема: – Транзистор станет 10-8 см – Большинство фирм ожидают что это произойдет в ближайшие 20 лет.

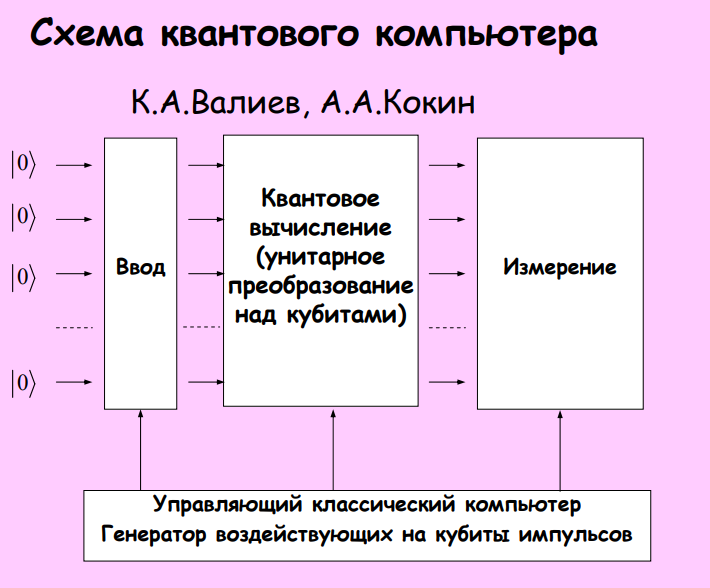
Что значит «вычисление»? Тезис Черча -Тюринга: алгоритмический процесс или вычисление это то, что можно сделать на машине Тюринга

Дойч (1985): Вытекает ли этот тезис из законов физики ?

Квантовомеханические системы очень трудно моделировать на классических компьютерах Дойч (1985): Вытекает ли этот тезис из законов физики ? Кандидат на универсальный компьютер: квантовый компьютер Может быть компьютеры, основанные на квантовой механике невозможно эффективно моделировать на машине Тюринга ? Возможно ли, что такие компьютеры могут решать некоторые задачи быстрее, чем выроятностная машина Тюринга ? Нарушение тезиса!

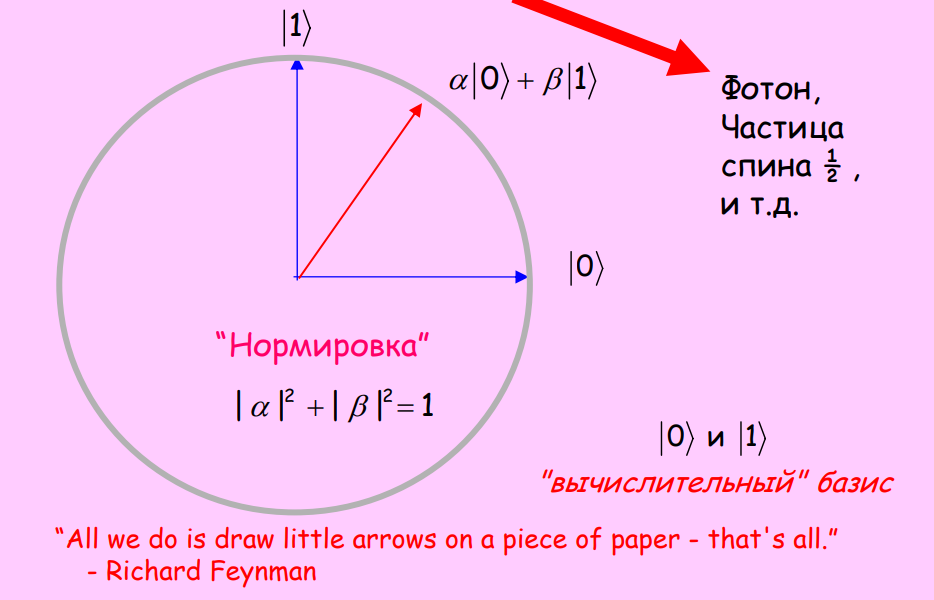
Тезис Черча-Тюринга-Дойча Любой физический процесс может быть эффективно Промоделирован на квантовом компьютере.

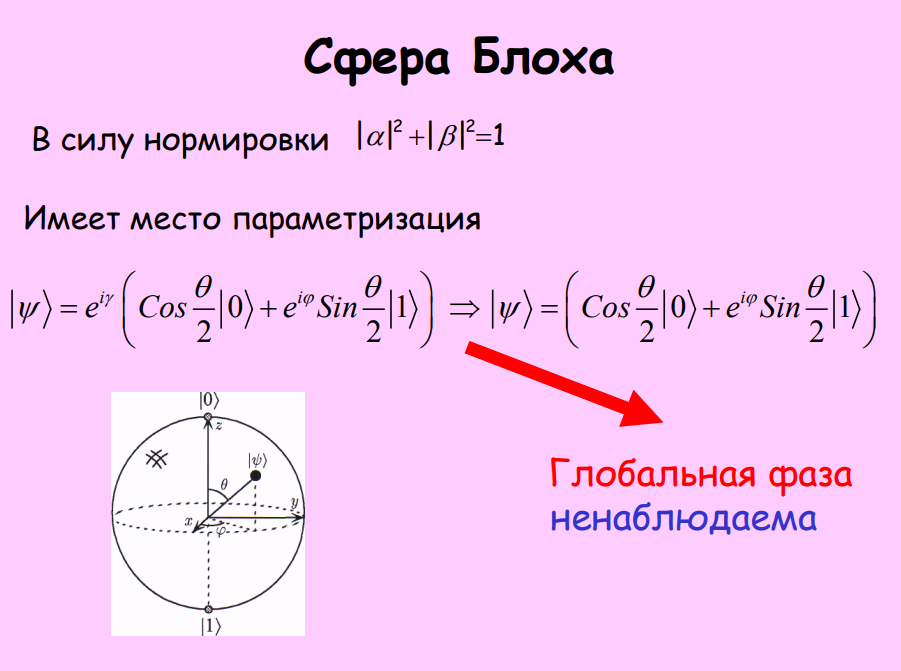
Что такое квантовый компьютер ? Квантовый компьютер – это вычислительный прибор, который основан на использовании для вычислений таких квантовомеханических явления как суперпозицию и перепутывание состояний для преобразования входных данных в выходные. В классическом компьютинге количество данных измеряется битами, а в квантовом компьютинге – кубитами. Основополагающий принцип квантовых вычислений состоит в использовании квантовомеханических объектов для представления данных и их обработки.

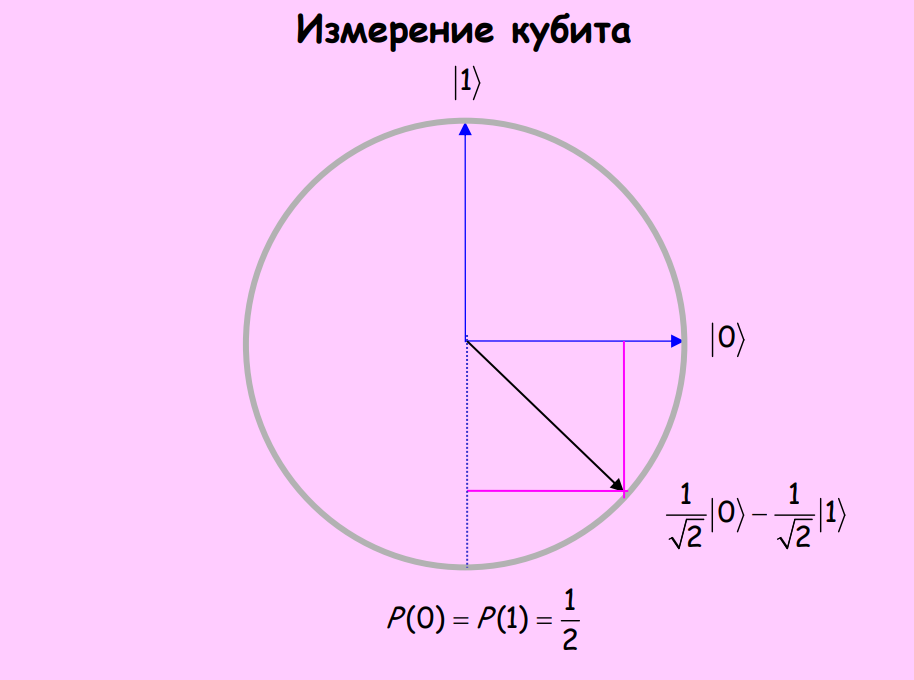


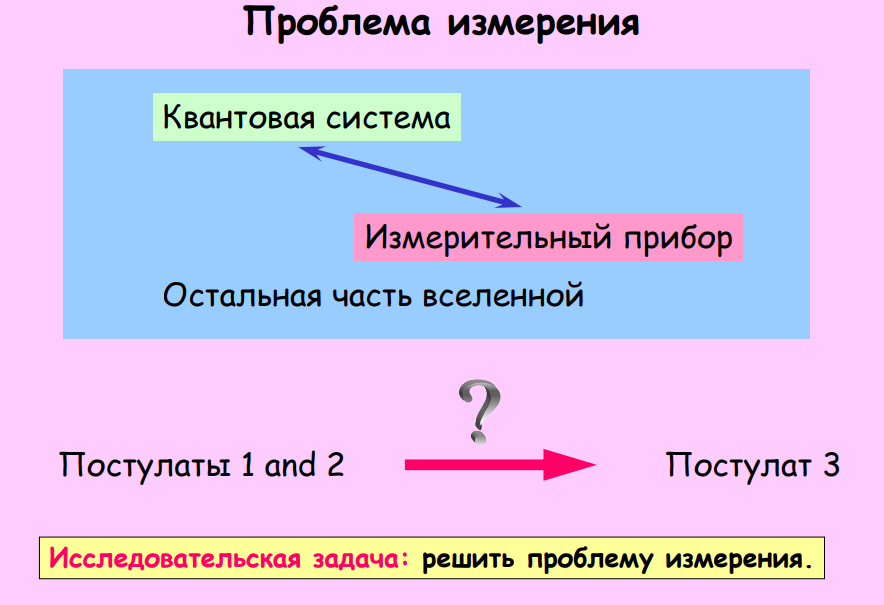
Постулаты квантовой механики Постулат 1: Состояние замкнутой квантовой системы задается единичным вектором в комплексном гильбертовом пространстве, образующим пространство состояний. Постулат 2: Эволюция замкнутой квантовой системы описывается унитарным преобразованием. ψψ ψ ( ) (0) exp( ) (0) t U= =− iHt ψ = ψ 1 2 Измерение в ортонормальном базисе ,..., дает результат с вероятност ь Постул ю ( ) . ат 3: d j e e j Pj e Измерение переводит систему в состояние , соотвествующее результату ej j Постулат 4: Пространство состояний составной системы является тензорным произведением пространств состояний ее компонент

Постулат 1 С каждой квантовой системой ассоциируется комплексное векторное пространство – пространство состояний. Пример: мы будем иметь дело, главным образом, с кубитами, которым соответствует пространство состояний C2. 0 1 α α β β ⎡ ⎤ + ≡ ⎢ ⎥ ⎣ ⎦ Состояние замкнутой квантовой системы описывается единичным вектором в пространстве состояний. Пример: кубит (двухуровневая квантовая система)









Многокубитные системы α00 00 01 10 11 ααα 01 10 11 +++ = α 2 (,)| | Измерение в вычислительном базисе: Pxy xy Общее состояние из n кубит: { } α ∑ ∈ 0,1 x n x x ( ) Для классического представления этого состояния требуется 2 бит. n O “Hilbert space is a big place” - Carlton Caves “Возможно […] нам недостает математической теории квантовых автоматов. […] квантовое пространство состояний обладает гораздо большей емкостью, чем классическое: […] там, где в классике имеется N дискретных состояний, в квантовой теории, допускающей их суперпозицию, имеется C N […] ячеек. […] Эти […] подсчеты показывают большую потенциальную сложность квантового поведения по сравнению с его классической имитацией.” – Ю.И. Манин (1980)

Постулат 4 Пространство состояний составной физической системы является тензорным произведением пространств состояний ее составляющих. Пример: ⊗ = 224 Двухкубитное пространство состояний CCC ⊗ ⊗⊗ ⊗ Вычислительные базисные состояния: 0 0 ; 0 1 ; 1 0 ; 1 1 Альтернативные обозначения: 0 0 ; 0,0 ; 00 .

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ Основное применение квантовым вычислениям — это искусственный интеллект. ИИ основан на принципах обучения в процессе извлечения опыта, становится все точнее по мере работы обратной связи, пока, наконец, не обзаводится «интеллектом», пусть и компьютерным. То есть самостоятельно обучается решению задач определенного типа. Эта обратная связь зависит от расчета вероятности для множества возможных исходов, и квантовые вычисления идеально подходят для такого рода операций. Искусственный интеллект, подкрепленный квантовыми компьютерами, перевернет каждую отрасль, от автомобилей до медицины, и говорят, что ИИ станет для двадцать первого века тем, чем электричество стало для двадцатого.  
  
Например, Lockheed Martin планирует использовать свой квантовый компьютер D-Wave для испытаний программного обеспечения для автопилота, которое слишком сложное для классических компьютеров, а Google использует квантовый компьютер для разработки ПО, которое сможет отличать автомобили от дорожных знаков. Мы уже достигли точки, за которой ИИ создает больше ИИ, и его сила и величина будет только расти. МОЛЕКУЛЯРНОЕ МОДЕЛИРОВАНИЕ Другой пример — это точное моделирование молекулярных взаимодействий, поиск оптимальных конфигураций для химических реакций. Такая «квантовая химия» настолько сложная, что с помощью современных цифровых компьютеров можно проанализировать только простейшие молекулы. Химические реакции квантовые по своей природе, поскольку образуют весьма запутанные квантовые состояния суперпозиции. Но полностью разработанные квантовые компьютеры смогут без проблем рассчитывать даже такие сложные процессы. Google уже совершает набеги в эту область, моделируя энергию водородных молекул. В результате получаются более эффективные продукты, от солнечных батарей до фармацевтических препаратов, и особенно удобрения; поскольку на удобрения приходится до 2% глобального потребления энергии, последствия для энергетики и окружающей среды будут колоссальными. КРИПТОГРАФИЯ Большая часть систем кибербезопасности полагается на сложность факторинга больших чисел на простые. Хотя цифровые компьютеры, которые просчитывают каждый возможный фактор, могут с этим справиться, длительное время, необходимое для «взлома кода», выливается в дороговизну и непрактичность. Квантовые компьютеры могут производить такой факторинг экспоненциально эффективнее цифровых компьютеров, делая современные методы защиты устаревшими. Разрабатываются новые методы криптографии, которые, впрочем, требуют времени: в августе 2015 года NSA начало собирать список устойчивых к квантовым вычислениям криптографических методов, которые могли бы противостоять квантовым компьютерам, и в апреле 2016 Национальный институт стандартов и технологий начал публичный процесс оценки, который продлится от четырех до шести лет. В разработке находятся также перспективные методы квантового шифрования, которые задействуют односторонний характер квантовой запутанности. Сети в пределах города уже продемонстрировали свою работоспособность в нескольких странах, и китайские ученые недавно объяснили, что успешно передали запутанные фотоны из орбитального «квантового» спутника на три отдельные базовые станции на Земле. ФИНАНСОВОЕ МОДЕЛИРОВАНИЕ Современные рынки являются одними из самых сложных систем в принципе. Хотя мы разработали много научных и математических инструментов для работы с ними, им по-прежнему недостает условия, которым могут похвастать другие научные дисциплины: нет контролируемых условий, в которых можно было бы провести эксперименты. Чтобы решить эту проблему, инвесторы и аналитики обратились к квантовым вычислениям. Непосредственным их преимуществом является то, что случайность, присущая квантовым компьютерам, конгруэнтна стохастическому характеру финансовых рынков. Инвесторы зачастую хотят оценивать распределение результатов при очень большом количестве сценариев, генерируемых случайным образом. Другое преимущество, которое предлагают квантовые компьютеры, состоит в том, что финансовые операции вроде арбитража иногда могут требовать множества последовательных шагов, и число возможностей их просчета сильно опережает допустимое для обычного цифрового компьютера. ПРОГНОЗИРОВАНИЕ ПОГОДЫ Главный экономит NOAA Родни Вейер утверждает, что почти 30% от ВВП США (6 триллионов долларов) прямо или косвенно зависит от погодных условий, влияющих на производство продуктов питания, транспорт и розничную торговлю, среди прочего. Способность лучше предсказывать погоду будет иметь огромное преимущество для многих областей, не говоря уж о дополнительном времени, которое понадобится для восстановления от стихийных бедствий. Хотя ученые давно ломают голову над процессами погодообразования, уравнения, стоящие за ними, включают множество переменных, сильно усложняя классическое моделирование. Как отметил квантовый исследователь Сет Ллойд, «использование классического компьютера для такого анализа займет столько времени, что погода успеет измениться». Поэтому Ллойд и его коллеги из MIT показали, что уравнения, управляющие погодой, имеют скрытую волновую природу, которую вполне удастся разрешить с применением квантового компьютера. Хартмут Невен, директор по разработкам в Google отметил, что квантовые компьютеры могут также помочь в создании более совершенных климатических моделей, которые могли бы дать нам более глубокое представление о том, как люди влияют на окружающую среду. На основе этих моделей мы выстраиваем наши представления о будущем потеплении, и они помогают нам определять шаги, которые требуются для предотвращения стихийных бедствий. ФИЗИКА ЧАСТИЦ Как ни странно, глубокое изучение физики с применением квантовых компьютеров может привести… к изучению новой физики. Модели физики элементарных частиц зачастую чрезвычайно сложные, требуют пространных решений и задействуют много вычислительного времени для численного моделирования. Они идеально подойдут для квантовых компьютеров, и ученые уже положили на них глаз. Ученые Университета Инсбрука и Института квантовой оптики и квантовой информации (IQOQI) недавно использовали программируемую квантовую систему для подобных манипуляций с моделями. Для этого они взяли простую версию квантового компьютера, в котором ионы производят логические операции, базовые шаги в любом компьютерном расчете. Моделирование показало прекрасное соглашение с реальными, описанными физикой, экспериментами. «Два этих подхода идеально дополняют друг друга», говорит физик-теоретик Питер Цоллер. «Мы не можем заменить эксперименты, которые проводятся на ускорителях частиц. Но развивая квантовые симуляторы, мы можем однажды лучше понять эти эксперименты». Теперь инвесторы стараются внедриться в экосистему квантовых вычислений, и не только в компьютерной индустрии: банки, аэрокосмические компании, кибербезопасность — все они выходят на гребень вычислительной революции. В то время как квантовые вычисления уже оказывают влияние на поля выше, этот список не является исчерпывающем ни в коем случае, и это самое интересное. Как бывает со всеми новыми технологиями, в будущем будут появляться совершенно немыслимые приложения, в такт с развитием аппаратных средств.

**Вывод**

Построение квантового компьютера в виде реального физического прибора является фундаментальной задачей физики XXI века. По состоянию на начало 2018 года построены только ограниченные варианты квантового компьютера (самые большие сконструированные квантовые регистры имеют несколько десятков связанных кубитов.

**Список литературы**

[**http://spkurdyumov.ru/uploads/2017/09/kvantovye-vychisleniya-i-funkcionalnoe-programmirovanie.pdf**](http://spkurdyumov.ru/uploads/2017/09/kvantovye-vychisleniya-i-funkcionalnoe-programmirovanie.pdf)

[**https://habr.com/ru/company/piter/blog/474528/**](https://habr.com/ru/company/piter/blog/474528/)

[**https://www.linux.org.ru/forum/talks/8129018**](https://www.linux.org.ru/forum/talks/8129018)