

РАЗВИТИЕ КВАНТОВЫХ КОМПЬЮТЕРОВ И ИХ ПЕРСПЕКТИВЫ В БУДУЩЕМ

Аракелян П. А., Галяк И. П., Лаптева А. С.

*Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь*

Чаевский В.В. – канд. физ.-мат. наук, доцент
кафедры физики

Аннотация. Квантовые компьютеры представляют собой революционное направление в вычислительной технологии. Обзорная статья кратко рассматривает основные принципы работы таких компьютеров, включая квантовую механику и концепцию кубитов, а также оценивает текущие достижения в этой области и их применение в научных исследованиях. Обсуждаются перспективы развития квантовых компьютеров, их возможное влияние на повседневную жизнь и промышленность, а также вызовы и проблемы, стоящие перед их разработкой. В заключении рассматривается влияние квантовых компьютеров на науку и технологии, включая область искусственного интеллекта и машинного обучения.

Ключевые слова. Квантовые компьютеры, биты, когерентность, вычисления, параллелизм, квантовая запутанность.

Работа квантовых компьютеров основана на принципах квантовой механики. Основные принципы, связанные с работой квантовых компьютеров:

– Квантовые состояния и кубиты [1]: вместо использования классических битов, квантовые компьютеры используют кубиты (quantum bits) как основные единицы информации, которые превосходят, как показано на рисунке 1, один бит классической единицы измерения количества информации практически на порядок величины.

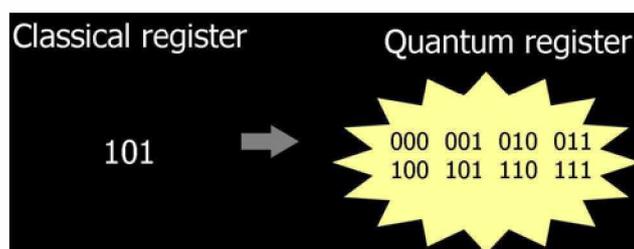


Рисунок 1 – 3 бита обычного регистра против 3 кубитов квантового

Как показано на рисунке 2, кубиты могут находиться в состоянии 0, состоянии 1 или в суперпозиции, когда они находятся в линейной комбинации состояний 0 и 1.

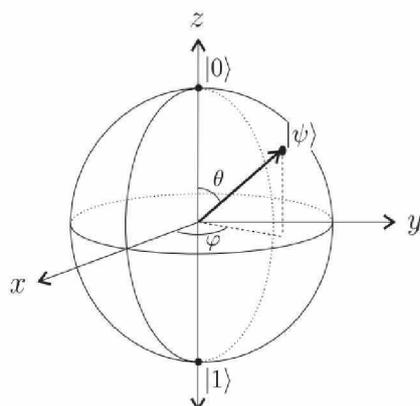


Рисунок 2 – Схема кубита

– Принцип суперпозиции [1]: квантовые системы могут существовать одновременно во всех возможных состояниях суперпозиции до тех пор, пока не производится измерение. Это означает, что кубит в суперпозиции может быть в состоянии 0 и 1 одновременно с определенной вероятностью.

– Принцип квантового параллелизма [2]: квантовые компьютеры могут выполнять операции над всеми возможными комбинациями состояний кубитов одновременно. Это позволяет квантовым компьютерам эффективно обрабатывать большие объемы данных за счет параллельной обработки.

– Квантовые взаимодействия: кубиты могут быть связаны друг с другом, образуя квантовые системы с более чем одним кубитом. Взаимодействие между кубитами позволяет осуществлять операции, такие как квантовые вентили [3] и квантовые измерения.

– Принцип измерения: измерение квантовой системы приводит к коллапсу суперпозиции в одно конкретное состояние. Результат измерения будет одним из возможных состояний кубита с вероятностью, определенной амплитудой этого состояния.

Эти принципы позволяют квантовым компьютерам выполнять определенные вычисления и решать задачи, которые классические компьютеры могут выполнять значительно медленнее или вообще не могут решить. Однако, квантовые компьютеры также сталкиваются с рядом сложностей, таких как шумы, декогеренция и ошибки квантовых операций, которые требуют разработки специальных алгоритмов и методов коррекции ошибок для достижения надежной работы.

Существуют следующие концепции кубитов и квантовых состояний:

1. Кубит может быть представлен на квантовом уровне частицы со свойствами спина или поляризации [4].

2. Различные операции переводят кубит из одного квантового состояния в другое, изменяя его внутреннее состояние.

3. Квантовое состояние описывает систему с точки зрения квантовой механики и позволяет системе находиться во всех возможных состояниях.

4. Квантовые состояния характеризуются суперпозицией и интерференцией [2], что приводит к уникальным свойствам квантовых систем.

5. Примерами квантовых состояний являются состояния поляризации фотона, спин электрона и другие квантовые системы.

6. Кубит может быть реализован, например, как атом, ион или квантовая точка [3], которые обладают квантовыми свойствами.

7. Измерение кубита приводит к коллапсу в одно определенное квантовое состояние.

8. Квантовые состояния обладают вероятностными характеристиками, что отличает их от классических состояний.

9. Операции с кубитами осуществляются с помощью квантовых гейтов [5], которые меняют их состояние в зависимости от входных данных.

10. Квантовые состояния могут быть использованы для квантовых вычислений, криптографии, симуляций и других задач.

11. Среди типов квантовых состояний можно выделить базисные состояния, суперпозиции, квантовое запутывание [1] и другие.

12. Квантовая суперпозиция позволяет существовать кубиту во всех возможных состояниях, что придает квантовым вычислениям выразительность.

13. Квантовые системы способны обрабатывать большие объемы информации параллельно благодаря суперпозиции состояний.

14. В квантовых вычислениях кубиты могут применять квантовые алгоритмы, такие как алгоритм Шора или алгоритм Гровера [4], для решения сложных задач быстрее классических компьютеров.

15. Состояние кубита определяется с помощью вектора состояния, который указывает вероятности нахождения кубита в каждом из состояний.

16. Квантовые состояния играют ключевую роль в развитии квантовых технологий и научных исследований в области квантовой физики.

17. Понимание кубитов и квантовых состояний является важным элементом для развития квантовых компьютеров и приложений в будущем.

Принципы суперпозиции и квантового параллелизма являются ключевыми концепциями в квантовой механике и основой для работы квантовых компьютеров.

Принцип суперпозиции гласит, что квантовая система может существовать одновременно во всех возможных состояниях, предусмотренных ее квантовой описательной функцией, до тех пор, пока не производится измерение. Это означает, что кубит может находиться в линейной комбинации базовых состояний, например, состояния 0 и состояния 1, с определенными амплитудами. В результате суперпозиции кубит может одновременно представлять несколько возможных состояний. Принцип квантового параллелизма заключается в возможности выполнения параллельных вычислений над всеми возможными комбинациями состояний кубитов. В отличие от классических компьютеров, которые могут обрабатывать только одну комбинацию состояний за раз, квантовые компьютеры могут одновременно обрабатывать все возможные комбинации состояний благодаря принципу суперпозиции. Это позволяет квантовым компьютерам выполнять определенные задачи значительно быстрее, чем классические компьютеры.

Принцип суперпозиции и принцип квантового параллелизма вместе дают квантовым компьютерам вычислительное преимущество при решении определенных задач. Например, при факторизации больших чисел алгоритм Шора использует суперпозицию и квантовый параллелизм для эффективного поиска периода функции, что приводит к разложению числа на простые множители за экспоненциально меньшее время, чем классические алгоритмы.

Однако, важно отметить, что выходные данные квантового компьютера после измерения ограничиваются одним конкретным состоянием, выбранным с определенной вероятностью. Анализ и интерпретация результатов квантовых вычислений требует использования статистических методов и алгоритмов для получения полезной информации из вероятностных результатов измерений.

Основными квантовыми компьютерами, разработанными в лабораториях, являются:

1. IBM Q System One: IBM создал квантовый компьютер под названием IBM Q System One. Этот квантовый компьютер имеет кубиты, использующие квантовые эффекты для выполнения операций (20 кубитов, 2019).

2. Google Quantum AI: Команда Google квантовых инженеров также работает над разработкой квантовых компьютеров. Они представили Bristlecone – 72-кубитный квантовый процессор.

3. IonQ: Компания IonQ развивает квантовые компьютеры, используя ионы для хранения информации. Они создали 11-кубитный квантовый процессор и работают над увеличением числа кубитов.

Выделяют следующие преимущества и недостатки существующих моделей квантовых компьютеров:

– преимущества:

1. Высокая вычислительная мощность. Квантовые компьютеры могут обрабатывать большие объемы данных параллельно благодаря принципу суперпозиции и квантовому параллелизму, что значительно увеличивает скорость выполнения вычислений.

2. Решение сложных задач. Квантовые компьютеры имеют потенциал для решения задач, которые непосильны для классических компьютеров, таких как факторизация больших чисел или оптимизация сложных систем.

3. Эффективность алгоритмов. Для некоторых задач квантовые алгоритмы могут быть значительно более эффективными, чем классические алгоритмы, что позволяет сократить время обработки данных.

4. Потенциал для развития. Использование квантовых вычислений может привести к созданию новых технологий и научных открытий, которые недоступны с использованием классических компьютеров.

– недостатки:

1. Технические сложности. Реализация квантовых компьютеров требует высокоточных квантовых систем и технологий, что может быть технически сложным и дорогостоящим процессом.

2. Возможность ошибок. Из-за чувствительности квантовых систем к внешним воздействиям существует риск возникновения ошибок в процессе вычислений, что требует использования корректирующих кодов.

3. Ограничения на размер квантовых систем. В настоящее время размер квантовых систем ограничен, что ограничивает масштабируемость и возможности квантовых компьютеров.

4. Сложность программирования. Написание эффективных квантовых алгоритмов требует специальных знаний и навыков, и по сравнению с классическим программированием может быть более сложным и трудоемким процессом.

Квантовые компьютеры в научных исследованиях имеют широкие применения, в том числе и технологические, среди которых одними из основными являются следующие:

1. Использование для моделирования сложных квантовых систем, молекул и материалов, что позволяет исследователям понять их свойства и взаимодействия на более глубоком уровне. Это может привести к разработке новых материалов с уникальными свойствами, которые могут найти применение в различных отраслях, от электроники до медицины.

2. Химические расчеты. Квантовые компьютеры могут использоваться для моделирования химических структур и реакций, биохимических процессов и взаимодействий между молекулами с высокой точностью и скоростью, что позволяет исследователям разрабатывать новые материалы и лекарства. Это позволит исследователям и фармацевтам быстрее и точнее прогнозировать эффективность потенциальных лекарственных препаратов и сокращать время и стоимость их разработки.

3. Оптимизация сложных систем. Квантовые компьютеры могут применяться для решения задач оптимизации в различных областях, таких как логистика, финансы и транспорт, что может привести к улучшению эффективности и экономии ресурсов.

4. Разработка новых материалов. С помощью квантовых компьютеров можно проводить моделирование и анализ свойств различных материалов, что может привести к созданию новых материалов с уникальными свойствами и приложениями.

5. Квантовая криптография [1]. Квантовые компьютеры могут использоваться для разработки квантово-стойких криптографических методов, которые обеспечивают более высокий уровень безопасности передачи информации, а также оказать существенную помощь в разработке квантовых шифров и протоколов, которые обеспечивают более высокий уровень безопасности, чем существующие классические методы криптографии. Эти методы могут использовать принципы квантовой механики, такие как непрерывное изменение квантовых состояний, для обеспечения защиты данных.

6. Исследование квантовой физики. Квантовые компьютеры могут помочь исследователям в изучении основных принципов квантовой физики и проведении экспериментов для проверки квантовых теорий.

7. Квантовые компьютеры могут быть использованы для разработки новых методов хранения и передачи энергии, таких как квантовые сети и квантовые аккумуляторы, которые обеспечивают более эффективное и экологически чистое использование энергии.

Развитие квантовых компьютеров имеют огромные перспективы: увеличение числа кубитов и улучшение качества квантовых состояний, что позволяет увеличить количество кубитов на квантовых чипах, приводящее к увеличению мощности и скорости квантовых компьютеров; развитие алгоритмов и программного обеспечения для квантовых компьютеров позволит создавать более эффективные и оптимизированные вычислительные задачи для квантовых компьютеров; разработка новых методов программирования для квантовых компьютеров значительно упростит процесс создания программ и повысит производительность вычислений; создание специализированных инструментов разработки и отладки программ для квантовых компьютеров улучшит качество и надежность программного обеспечения; развитие квантовых библиотек и фреймворков сделает доступ к квантовым вычислениям более удобным и эффективным.

Разработка квантовых компьютеров связана с техническими проблемами, из которых одними из основных является создание стабильных квантовых состояний. Квантовые состояния крайне чувствительны к внешним воздействиям, таким как температурные флуктуации, радиационное излучение и электромагнитные поля. Это может привести к декогеренции [5] – потере квантовой когерентности. В результате кубиты перестают быть в состоянии суперпозиции и вместо этого принимают классические значения, что делает невозможным проведение квантовых вычислений. Решение этой проблемы включает создание окружений с низким уровнем шума и разработку методов коррекции ошибок. Кроме того, квантовые системы подвержены ошибкам из-за взаимодействия с окружающей средой. Эти ошибки могут быть вызваны множеством факторов, таких как флуктуации температуры и электромагнитного поля. Сами квантовые операции также могут быть источником ошибок. Разработка методов исправления ошибок становится критической для обеспечения надежности квантовых вычислений. Создание и поддержание стабильных квантовых состояний требует высокоточных и сложных технологий. Например, для квантовых точек, которые могут быть использованы в качестве кубитов, необходимо обеспечить точное управление над их положением и энергией. Это может включать в себя использование специальных материалов и техник нанотехнологий.

Проблемы управления и поддержки квантовых систем также являются ключевыми вызовами в разработке квантовых компьютеров. Квантовая контрольная инженерия – управление квантовыми системами требует разработки сложных алгоритмов и методов, которые обеспечивают точное управление и манипулирование кубитами. Это включает в себя инициализацию квантовых состояний, выполнение квантовых операций и считывание результатов вычислений. Отсутствие эффективных методов управления может привести к ошибкам и потере квантовой информации. Оптимизация квантовых алгоритмов – эффективное управление квантовыми системами также требует разработки оптимизированных квантовых алгоритмов. Это включает в себя поиск эффективных способов реализации квантовых операций и улучшение производительности квантовых алгоритмов для решения конкретных задач.

Интеграция с классическими системами – квантовые компьютеры будут работать в среде, где присутствуют и классические вычислительные системы. Это требует разработки методов интеграции и совместной работы квантовых и классических систем, чтобы обеспечить эффективную и надежную обработку данных.

Обеспечение стабильности и надежности работы, что включает в себя разработку методов диагностики и обнаружения ошибок, а также создание систем автоматического восстановления и резервирования для обеспечения непрерывной работы.

Вопросы безопасности и конфиденциальности данных, обрабатываемых квантовыми компьютерами являются одними из ключевых при работе компьютеров. Это угрозы криптографии – квантовые компьютеры обладают потенциалом для взлома многих существующих криптографических методов, основанных на сложности математических задач. Например, алгоритм Шора позволяет эффективно факторизовать большие целые числа, что

приводит к угрозе для алгоритмов шифрования, таких как RSA. Алгоритм Гровера может значительно ускорить поиск по базе данных или нахождение дискретного логарифма, что может подорвать безопасность многих симметричных криптографических алгоритмов.

В контексте квантовых компьютеров также возникают новые вопросы о защите от атак. Например, существует угроза криптографической атаки на квантовые протоколы связи, если злоумышленник может перехватить или подделать квантовые состояния в канале связи. Необходимо разработать новые методы квантовой криптографии, которые будут устойчивы к таким видам атак.

Вместе с угрозами появляются и новые возможности для обеспечения безопасности. Квантовые системы могут быть использованы для разработки новых криптографических методов, например, квантовых ключей и квантовых протоколов распределения ключей, которые обеспечивают более высокий уровень безопасности и защиты от квантовых атак.

Решение этих вопросов требует широкого междисциплинарного подхода, который включает в себя работу специалистов по криптографии, физики, инженеров и информационных технологий.

Влияние квантовых компьютеров на развитие сферы искусственного интеллекта (ИИ) и машинного обучения (МО) может быть значительным и привести к новым возможностям и улучшению эффективности существующих методов. Вот несколько способов, как квантовые компьютеры могут повлиять на эту область. Разработка новых алгоритмов машинного обучения, которые могут использовать квантовые принципы для решения задач – алгоритмы кластеризации, классификации и регрессии могут быть оптимизированы с использованием квантовых алгоритмов, что может привести к улучшению точности и скорости обучения моделей. Оптимизация функций потерь или поиск оптимальных параметров модели могут обрабатывать большие объемы данных и выполнять сложные операции параллельно, что может значительно ускорить процесс обучения. Кроме того, для решения задач оптимизации, которые часто возникают в контексте машинного обучения, например, в обучении моделей машинного обучения или в настройке гиперпараметров, квантовые компьютеры могут эффективно искать оптимальные решения в больших пространствах параметров и улучшать производительность моделей.

Квантовые компьютеры могут улучшить обработку естественного языка (Natural Language Processing, NLP), позволяя алгоритмам более эффективно анализировать и понимать текстовые данные. Это может привести к разработке более точных и эффективных моделей для задач обработки текста, таких как анализ тональности, машинный перевод и автоматическое распознавание речи.

Квантовые компьютеры могут быть использованы для разработки и обучения квантовых нейронных сетей, которые могут быть более мощными и эффективными, чем классические нейронные сети. Квантовые нейронные сети могут обрабатывать большие объемы данных и решать более сложные задачи с высокой точностью. Однако, необходимо отметить, что многие из перспективных применений квантовых компьютеров в этой области все еще находятся на стадии исследований и разработок, и требуют дальнейших исследований и экспериментов для их полной реализации.

Список использованных источников:

1. Ручкин, В.Н. Естественный параллелизм квантовых компьютеров и нейровычислителей / В.Н. Ручкин, В.А. Романчук, В.А. Фулин – Рязань: Вестник Рязанского государственного университета им. С.А. Есенина, 2013 – С. 6-9.
2. Википедия. Свободная энциклопедия. Квантовый компьютер [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Квантовый_компьютер
3. Торгаев, С.Н. Основы квантовых вычислений: учебное пособие / С.Н. Торгаев, И.Д. Шульга, Е.А. Юрченко, М.Л. Громов. – Томск: STT, 2020. – С. 23-37.
4. Сысоев, С.С. Введение в квантовые вычисления. Квантовые алгоритмы: учеб. пособие / С.С. Сысоев – СПб.: Изд-во С.-Петербур. ун-та, 2019. – С. 53-64.
5. Квантовые вычисления: учеб. пособие / С.Н. Торгаев, И.Д. Шульга, Е.А. Юрченко, М.Л. Громов, 2010. – С.86-93.