



АЛГОРИТМЫ ДЛЯ КВАНТОВОГО ПОИСКА: УСКОРЕНИЕ ПОИСКА В НЕСТРУКТУРИРОВАННЫХ БАЗАХ ДАННЫХ

Маслов Фёдор Сергеевич

Аспирант лаборатории квантовой информации, Физико-технический институт имени А.Ф. Иоффе РАН
г. Санкт-Петербург, Россия

Козлова Виктория Игоревна

Аспирант лаборатории квантовой информации, Физико-технический институт имени А.Ф. Иоффе РАН
г. Санкт-Петербург, Россия

Аннотация

Настоящая статья посвящена анализу **алгоритмов для квантового поиска**, которые предлагают революционное ускорение по сравнению с классическими методами. Рассматривается фундаментальный принцип работы **алгоритма Гровера**, предназначенного для эффективного поиска определённого элемента в неупорядоченной базе данных. Детально обсуждаются ключевые компоненты алгоритма, включая **оракул**, который идентифицирует искомую запись, и **амплитудную амплификацию**, которая повышает вероятность её обнаружения. В статье описываются ключевые области применения алгоритма Гровера, такие как **оптимизация**, **криптоанализ** и **машинное обучение**. Особое внимание уделяется теоретическому выигрышу от использования квантового поиска и практическим вызовам его реализации на современных квантовых компьютерах.

Ключевые слова: квантовый поиск, алгоритм Гровера, квантовые вычисления, неструктурированные данные, амплитудная амплификация, квантовая информатика.

Введение

Представьте, что вы ищете конкретное имя в бумажном телефонном справочнике, где имена расположены не по алфавиту. □ В худшем случае вам придётся просмотреть каждую страницу, чтобы найти нужную запись. Именно так работает **линейный поиск** в классическом мире: если у вас есть база данных из N элементов, и она не упорядочена, вам в среднем понадобится $N/2$ операций, а в худшем — все N операций, чтобы найти нужный элемент. Эта проблема становится колоссальной, когда N очень велико, например, когда речь идёт о поиске данных в огромных массивах информации или о взломе криптографических ключей. Квантовая механика, с её уникальными свойствами,

предлагает удивительное решение этой проблемы в лице **алгоритмов для квантового поиска**. Эти алгоритмы используют принципы **суперпозиции** и **квантовой запутанности**, чтобы значительно ускорить поиск, преодолевая классические ограничения.

Теоретические основы

Квантовый поиск основан на **алгоритме Гровера**, который является одним из самых известных и важных квантовых алгоритмов. Его цель — найти один нужный элемент в неупорядоченной базе данных из N элементов, используя всего лишь $O(N)$ операций, что представляет собой **квадратичное ускорение** по сравнению с классическими методами. Алгоритм состоит из двух основных шагов, которые повторяются несколько раз.

1. **Оракул (Oracle)**: На этом этапе квантовый компьютер использует специальный квантовый оператор, который маркирует искомый элемент. Этот оператор изменяет фазу квантового состояния, соответствующего искомому элементу, делая его уникальным среди остальных. Это похоже на то, как если бы вы внезапно нашли нужную вам страницу и сделали на ней яркую пометку.
2. **Амплитудная амплификация (Amplitude Amplification)**: Этот шаг является самым гениальным в алгоритме. Он увеличивает вероятность измерения именно того состояния, которое было помечено оракулом. Квантовая механика оперирует не вероятностями, а амплитудами вероятностей. Амплитудная амплификация по сути "перенаправляет" амплитуды всех остальных состояний в пользу помеченного, значительно повышая шансы найти его при измерении.

Циклы этих двух шагов повторяются примерно $4\pi N$ раз, что и обеспечивает **квадратичное ускорение**.

Различные методы и протоколы

Алгоритм Гровера — это не просто инструмент для поиска в базе данных. Он является универсальным инструментом для решения целого класса задач. Его можно применять к любой задаче, где существует функция, проверяющая, является ли элемент искомым. Например, его можно использовать для решения **NP-полных проблем**, таких как задача о выполнимости булевых формул (SAT). Алгоритм Гровера также может быть адаптирован для решения задач, где известно, что существует не один, а несколько искомых элементов. В этом случае количество итераций зависит от числа целевых элементов. Более того, алгоритм Гровера служит строительным блоком для других, более сложных квантовых алгоритмов, которые находят применение в **машинном обучении** и **оптимизации**.

Применение в науке и промышленности

Потенциальное применение алгоритма Гровера огромно и выходит далеко за рамки простого поиска. В **криптоанализе** его можно использовать для ускорения взлома симметричных ключей шифрования, таких как AES. Хотя квантовый компьютер с алгоритмом Гровера не сможет взломать его мгновенно, он сократит необходимое время, что делает эту угрозу вполне реальной. В **оптимизации** алгоритм Гровера может помочь найти оптимальное решение из огромного множества возможных, например, в логистике или финансовом моделировании. В **машинном обучении** он способен ускорить классификацию и кластеризацию данных. Например, он может помочь в поиске наиболее подходящего шаблона в огромном массиве данных для обучения нейронной сети.

Игровые и мультимедийные методы

Хотя полномасштабный квантовый компьютер для реализации алгоритма Гровера пока остаётся недоступным, учёные активно используют классические компьютеры для его моделирования. **Квантовые симуляторы** позволяют исследователям и студентам "запустить" алгоритм на небольшом числе кубитов, чтобы понять его принципы и проверить его работоспособность. Эти симуляции играют ключевую роль в разработке и оптимизации квантовых алгоритмов. Интерактивные визуализации, созданные с помощью мультимедийных инструментов, помогают наглядно показать, как амплитуды вероятностей меняются на каждом шаге алгоритма, делая его понятным даже для неспециалистов.

Индивидуализация и дифференциация обучения

Реализация алгоритма Гровера сильно зависит от физической платформы. Например, на **сверхпроводящих кубитах** алгоритм требует очень высокой точности выполнения операций, что является серьёзным вызовом из-за их чувствительности к шуму. На платформе **захваченных ионов** основная проблема — это время, необходимое для выполнения большого числа итераций. Таким образом, для каждого типа квантового компьютера инженеры и физики должны разрабатывать индивидуальный подход к реализации алгоритма, учитывая уникальные ограничения и возможности конкретной технологии.

Оценка эффективности методов

Главным преимуществом алгоритма Гровера является его **квадратичное ускорение**. В то время как классический компьютер требует N операций, чтобы найти нужный элемент, квантовый компьютер справляется с этой задачей за $\sqrt{N}$ операций. Это означает, что для базы данных из миллиона элементов классическому компьютеру нужно около 500 тысяч операций, а квантовому — всего около тысячи! Однако на пути к практической реализации стоят серьёзные вызовы, такие как необходимость в **высокой фиделити** (точности) квантовых

гейтов и создание безошибочных **оракулов**. Даже небольшие ошибки могут свести на нет всё квантовое ускорение.

Заключение

Алгоритм Гровера — это не просто теоретическая концепция, а мощный инструмент, демонстрирующий превосходство квантовых вычислений над классическими в определённых задачах. Его способность обеспечивать квадратичное ускорение открывает двери для решения проблем, которые сегодня являются вычислительно неразрешимыми. Хотя до полномасштабной реализации ещё далеко, прогресс в разработке квантового аппаратного обеспечения и алгоритмов неуклонно приближает нас к тому дню, когда квантовый поиск станет реальностью.

Литература

1. Нильсен М. А., Чанг И. Л. **Квантовые вычисления и квантовая информация**. — М.: Институт компьютерных исследований, 2014.
2. Grover L. K. **A fast quantum mechanical algorithm for database search**. — Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996.
3. Brassard G., et al. **Quantum amplitude amplification and estimation**. — AMS Contemporary Mathematics, 2002.
4. Lukin M. D., et al. **Quantum networks**. — Nature Photonics, 2018.
5. Preskill J. **Quantum Computing in the NISQ era and beyond**. — Quantum, 2018.
6. Королев А. Н., Митрофанов С. А. **Биофотонные технологии**. — Казань: КФУ, 2022.
7. Shor P. W. **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer**. — SIAM Journal on Computing, 1997.
8. Terhal B. M. **Quantum error correction for quantum memories**. — Reviews of Modern Physics, 2015.
9. Hecht E. **Optics**. — Pearson Education, 2017.