Министерство цифрового развития, связи

и массовых коммуникаций Российской Федерации

Сибирский Государственный Университет Телекоммуникаций и Информатики

СибГУТИ

Кафедра вычислительных систем

Расчетно-графическое задание.

Перевод статьи.

Квантовые вычисления.

Выполнил: студент 3 курса группы ИП-014

Рыльский Григорий Максимович

Преподаватель: Насонова Алина Олеговна

Новосибирск, 2022

ТЕКСТ СТАТЬИ НА АНГЛИЙСКОМ

QUANTUM COMPUTING: WHAT IT IS, WHY WE WANT IT, AND HOW WE'RE TRYING TO GET IT

SARA GAMBLE.

https://www.ncbi.nlm.nih.gov/books/NBK538701/

Quantum mechanics emerged as a branch of physics in the early 1900s to explain nature on the scale of atoms and led to advances such as transistors, lasers, and magnetic resonance imaging. The idea to merge quantum mechanics and information theory arose in the 1970s but garnered little attention until 1982, when physicist Richard Feynman gave a talk in which he reasoned that computing based on classical logic could not tractably process calculations describing quantum phenomena. Computing based on quantum phenomena configured to simulate other quantum phenomena, however, would not be subject to the same bottlenecks. Although this application eventually became the field of quantum simulation, it didn't spark much research activity at the time.

In 1994, however, interest in quantum computing rose dramatically when mathematician Peter Shor developed a quantum algorithm, which could find the prime factors of large numbers efficiently. Here, “efficiently” means in a time of practical relevance, which is beyond the capability of state-of-the-art classical algorithms. Although this may seem simply like an oddity, it is impossible to overstate the importance of Shor's insight. The security of nearly every online transaction today relies on an RSA cryptosystem that hinges on the intractability of the factoring problem to classical algorithms.

WHAT IS QUANTUM COMPUTING?

Quantum and classical computers both try to solve problems, but the way they manipulate data to get answers is fundamentally different. This section provides an explanation of what makes quantum computers unique by introducing two principles of quantum mechanics crucial for their operation, superposition and entanglement.

Superposition is the counterintuitive ability of a quantum object, like an electron, to simultaneously exist in multiple “states.” With an electron, one of these states may be the lowest energy level in an atom while another may be the first excited level. If an electron is prepared in a superposition of these two states it has some probability of being in the lower state and some probability of being in the upper. A measurement will destroy this superposition, and only then can it be said that it is in the lower or upper state.

Understanding superposition makes it possible to understand the basic component of information in quantum computing, the qubit. In classical computing, bits are transistors that can be off or on, corresponding to the states 0

and 1. In qubits such as electrons, 0 and 1 simply correspond to states like the lower and upper energy levels discussed above. Qubits are distinguished from classical bits, which must always be in the 0 or 1 state, by their ability to be in superpositions with varying probabilities that can be manipulated by quantum operations during computations.

Entanglement is a phenomenon in which quantum entities are created and/or manipulated such that none of them can be described without referencing the others. Individual identities are lost. This concept is exceedingly difficult to conceptualize when one considers how entanglement can persist over long distances. A measurement on one member of an entangled pair will immediately determine measurements on its partner, making it appear as if information can travel faster than the speed of light. This apparent action at a distance was so disturbing that even Einstein dubbed it “spooky” (Born 1971, p. 158).

The popular press often writes that quantum computers obtain their speedup by trying every possible answer to a problem in parallel. In reality a quantum computer leverages entanglement between qubits and the probabilities associated with superpositions to carry out a series of operations (a quantum algorithm) such that certain probabilities are enhanced (i.e., those of the right answers) and others depressed, even to zero (i.e., those of the wrong answers). When a measurement is made at the end of a computation, the probability of measuring the correct answer should be maximized. The way quantum computers leverage probabilities and entanglement is what makes them so different from classical computers.

WHY DO WE WANT IT?

The promise of developing a quantum computer sophisticated enough to execute Shor's algorithm for large numbers has been a primary motivator for advancing the field of quantum computation. To develop a broader view of quantum computers, however, it is important to understand that they will likely deliver tremendous speed-ups for only specific types of problems. Researchers are working to both understand which problems are suited for quantum speed-ups and develop algorithms to demonstrate them. In general, it is believed that quantum computers will help immensely with problems related to optimization, which play key roles in everything from defense to financial trading.

Multiple additional applications for qubit systems that are not related to computing or simulation also exist and are active areas of research, but they are beyond the scope of this overview. Two of the most prominent areas are (1) quantum sensing and metrology, which leverage the extreme sensitivity of qubits to the environment to realize sensing beyond the classical shot noise limit, and (2) quantum networks and communications, which may lead to revolutionary ways to share information.

HOW ARE WE TRYING TO GET IT?

Building quantum computers is incredibly difficult. Many candidate qubit systems exist on the scale of single atoms, and the physicists, engineers, and materials scientists who are trying to execute quantum operations on these systems constantly deal with two competing requirements. First, qubits need to be protected from the environment because it can destroy the delicate quantum states needed for computation. The longer a qubit survives in its desired state the longer its "coherence time." From this perspective, isolation is prized. Second, however, for algorithm execution qubits need to be entangled, shuffled around physical architectures, and controllable on demand. The better these operations can be carried out the higher their "fidelity." Balancing the required isolation and interaction is difficult, but after decades of research a few systems are emerging as top candidates for large-scale quantum information processing.

Superconducting systems, trapped atomic ions, and semiconductors are some of the leading platforms for building a quantum computer. Each has advantages and disadvantages related to coherence, fidelity, and ultimate scalability to large systems. It is clear, however, that all of these platforms will need some type of error correction protocols to be robust enough to carry out meaningful calculations, and how to design and implement these protocols is itself a large area of research. For an overview of quantum computing, with more detail regarding experimental implementations, see .

In this article, "quantum computing" has so far been used as a blanket term describing all computations that utilize quantum phenomena. There are actually multiple types of operational frameworks. Logical, gate-based quantum computing is probably the best recognized. In it, qubits are prepared in initial states and then subject to a series of "gate operations," like current or laser pulses depending on qubit type. Through these gates the qubits are put in superpositions, entangled, and subjected to logic operations like the AND, OR, and NOT gates of traditional computation. The qubits are then measured and a result obtained.

Another framework is measurement-based computation, in which highly entangled qubits serve as the starting point. Then, instead of performing manipulation operations on qubits, single qubit measurements are performed, leaving the targeted single qubit in a definitive state. Based on the result, further measurements are carried out on other qubits and eventually an answer is reached.

A third framework is topological computation, in which qubits and operations are based on quasiparticles and their braiding operations. While nascent implementations of the components of topological quantum computers have yet to be demonstrated, the approach is attractive because these systems are theoretically protected against noise, which destroys the coherence of other qubits.

Finally, there are the analog quantum computers or quantum simulators envisioned by Feynman. Quantum simulators can be thought of as special purpose quantum computers that can be programmed to model quantum systems. With this ability they can target questions such as how high-temperature superconductors

work, or how certain chemicals react, or how to design materials with certain properties.

CONCLUSIONS AND OUTLOOK

Quantum computers have the potential to revolutionize computation by making certain types of classically intractable problems solvable. While no quantum computer is yet sophisticated enough to carry out calculations that a classical computer can't, great progress is under way. A few large companies and small start-ups now have functioning non-error-corrected quantum computers composed of several tens of qubits, and some of these are even accessible to the public through the cloud. Additionally, quantum simulators are making strides in fields varying from molecular energetics to many-body physics.

As small systems come online a field focused on near-term applications of quantum computers is starting to burgeon. This progress may make it possible to actualize some of the benefits and insights of quantum computation long before the quest for a large-scale, error-corrected quantum computer is complete.

ПЕРЕВОД СТАТЬИ

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: ЧТО ЭТО ТАКОЕ, ПОЧЕМУ МЫ ЭТО ХОТИМ И КАК МЫ ПЫТАЕМСЯ ЕГО ПОЛУЧИТЬ

ВВЕДЕНИЕ

Квантовая механика возникла как отрасль физики в начале 1900-х годов для объяснения природы в масштабе атомов и привела к таким достижениям, как транзисторы, лазеры и магнитно-резонансная томография. Идея объединить квантовую механику и теорию информации возникла в 1970-х годах, но привлекала мало внимания до 1982 года, когда физик Ричард Фейнман выступил с докладом, в котором обосновал, что вычисления, основанные на классической логике, не могут эффективно обрабатывать вычисления, описывающие квантовые явления. Однако вычисления, основанные на квантовых явлениях и настроенные на моделирование других квантовых явлений, не будут подвержены узким местам (процесс в цепочке процессов, ограниченная мощность которого снижает мощность всей цепочки.). Хотя это применение в конечном итоге стало областью квантового моделирования, в то время оно не вызвало большой исследовательской активности.

Однако в 1994 году интерес к квантовым вычислениям резко возрос, когда математик Питер Шор разработал квантовый алгоритм, который мог эффективно находить простые множители больших чисел. Здесь «эффективно» означает за время практической значимости, которое находится за пределами возможностей современных классических алгоритмов. Хотя это может показаться просто странностью, невозможно переоценить важность открытия Шора. Безопасность почти каждой онлайн-транзакции сегодня зависит от криптосистемы RSA, которая основывается на неразрешимости проблемы факторизации для классических алгоритмов.

ЧТО ТАКОЕ КВАНТОВЫЕ ВЫЧИСЛЕНИЯ?

Квантовые и классические компьютеры пытаются решить проблемы, но способ, которым они манипулируют данными для получения ответов, принципиально отличается. В этом разделе дается объяснение того, что делает квантовые компьютеры уникальными, вводятся два принципа квантовой механики, имеющие решающее значение для их работы, - суперпозиция и запутанность.

Суперпозиция — это способность квантового объекта, например электрона, одновременно существовать в нескольких «состояниях». У электрона одно из этих состояний может быть нижним энергетическим уровнем в атоме, а

другое - верхнем возбужденным уровнем. Если электрон подготовлен в суперпозиции этих двух состояний, он имеет некоторую вероятность оказаться в нижнем состоянии и некоторую вероятность оказаться в верхнем. В результате измерения эта суперпозиция будет разрушена, и только тогда можно будет сказать, что он находится в нижнем или верхнем состоянии.

Понимание суперпозиции позволяет понять основной компонент информации в квантовых вычислениях - кубиты. В классических вычислениях биты — это транзисторы, которые могут быть выключены или включены, что соответствует состояниям 0 и 1. В кубитах, таких как электроны, 0 и 1 просто соответствуют состояниям, подобным нижнему и верхнему энергетическим уровням, о которых говорилось выше. Кубиты отличаются от классических битов, которые всегда должны находиться в состоянии 0 или 1, своей способностью находиться в суперпозиции с различной вероятностью, которой можно манипулировать с помощью квантовых операций во время вычислений.

Квантовая запутанность— это явление, при котором квантовые сущности создаются и/или манипулируются таким образом, что ни одна из них не может быть описана без привязки к другим. Индивидуальность теряется. Это понятие чрезвычайно трудно осмыслить, если учесть, как запутанность может сохраняться на большие расстояния. Измерение одного компонента запутанной пары немедленно определит измерения его соседа, что создает впечатление, будто информация может перемещаться быстрее скорости света. Это очевидное явление было настолько тревожным, что даже Эйнштейн назвал(окрестил) его "жутким" (Born 1971 , стр. 158).

В желтой прессе часто пишут, что квантовые компьютеры получают свое ускорение за счет параллельного перебора всех возможных вариантов решения проблемы. В действительности квантовый компьютер использует запутанность между кубитами и вероятности, связанные с суперпозициями, для выполнения серий квантовых алгоритмов таким образом, что определенные вероятности увеличиваются (т.е. вероятности правильных ответов), а другие уменьшаются, вплоть до нуля (т.е. вероятности неправильных ответов). Когда измерение производится в конце вычисления, вероятность правильного ответа должна быть максимальной. То, как квантовые компьютеры используют вероятности и запутанность, отличает их от классических компьютеров.

ПОЧЕМУ МЫ ЭТО ХОТИМ?

Обещание разработать квантовый компьютер, достаточно совершенный для выполнения алгоритма Шора на больших наборах чисел, стало основным стимулом для развития области квантовых вычислений. Однако для более широкого взгляда на квантовые компьютеры важно понимать, что они, скорее всего, обеспечат огромное ускорение только для

определенных типов задач. Исследователи работают над тем, чтобы понять, какие задачи подходят для квантовых ускорений, и разработать алгоритмы для их демонстрации. В целом, считается, что квантовые компьютеры окажут огромную помощь в решении проблем, связанных с оптимизацией, которые играют ключевую роль во всех областях - от обороны до финансовой торговли.

Также существуют и являются активными областями исследований многочисленные дополнительные применения для систем кубитов, не относящихся к вычислениям или моделированию, но они выходят за рамки данного обзора. Две наиболее выдающиеся области: (1) квантовое сканирование и метрология, которые основываются на чрезвычайной чувствительности кубитов к окружающей среде для реализации сканирования за пределом дробового (пуассоновсого) шума, и (2) квантовые сети и коммуникации, которые могут привести к революционным способам обмена информацией.

КАК МЫ ПЫТАЕМСЯ ПОЛУЧИТЬ ЭТО?

Создание квантовых компьютеров невероятно сложно. Многие потенциальные системы кубитов существуют в масштабах отдельных атомов, и физики, инженеры и исследователи материалов, которые пытаются выполнить квантовые операции на этих системах, постоянно имеют дело с двумя противоречащими друг другу требованиями. Во-первых, кубиты должны быть защищены от воздействия окружающей среды, поскольку она может разрушить тонкие квантовые состояния, необходимые для вычислений. Чем дольше кубиты находятся в этом состоянии, тем больше их "время когерентности". С этой точки зрения, изоляция очень важна. Во-вторых, для выполнения алгоритмов кубиты необходимо запутывать, перемещать по физической архитектуре и контролировать их. Чем лучше эти операции могут быть выполнены, тем выше их "точность". Балансировать между требуемой изоляцией и взаимодействием сложно, но после десятилетий исследований несколько систем становятся главными кандидатами на крупномасштабную обработку квантовой информации.

Сверхпроводящие системы, захваченные атомные ионы и полупроводники являются одними из ведущих платформ для создания квантового компьютера. Каждый из них имеет преимущества и недостатки, связанные с когерентностью, точностью и предельной масштабируемостью для больших систем. Однако ясно, что все эти платформы нуждаются в определенном типе протоколов коррекции ошибок, чтобы быть достаточно надежными для проведения важных вычислений, а разработка и реализация этих протоколов сама по себе является большой областью исследований.

В этой статье "квантовые вычисления" до сих пор использовался как общий термин, описывающий все вычисления, использующие квантовые явления. На самом деле существует несколько типов операционных структур.

Логические квантовые вычисления на основе квантовых затворов, вероятно, являются наиболее известными. В нем кубиты находятся в исходном состоянии, а затем подвергаются серии "операций с вентилями", например, с током или лазерными импульсами, в зависимости от типа кубита. Через эти вентили кубиты помещаются в суперпозиции, запутываются и подвергаются логическим операциям, подобным операторам И, ИЛИ и НЕ в традиционных вычислениях. Затем кубиты измеряются, и получается результат.

Другая структура - вычисления на основе измерений, в которых начальной точкой служат сильно запутанные кубиты. Затем, вместо выполнения манипуляционных операций над кубитами, производятся измерения отдельных кубитов, оставляя измеряемый кубит в определенном состоянии. На основе полученного результата проводятся дальнейшие измерения на других кубитах, и в конце концов достигается ответ.

Третья структура - топологические вычисления, в которых кубиты и операции основаны на квазичастицах и их операциях плетения. Несмотря на то, что зарождающиеся реализации компонентов топологических квантовых компьютеров еще не продемонстрированы, подход привлекателен потому, что эти системы теоретически защищены от помех, которые разрушают когерентность других кубитов.

Наконец, существуют аналоговые квантовые компьютеры или квантовые симуляторы, о которых задумывался Фейнман. Квантовые симуляторы можно рассматривать как квантовые компьютеры специального назначения, которые могут быть запрограммированы для моделирования квантовых систем. Благодаря этой способности они могут решать такие вопросы, как работа высокотемпературных сверхпроводников, реакция определенных химических веществ или разработка материалов с определенными свойствами.

ВЫВОДЫ И ПЕРСПЕКТИВЫ

Квантовые компьютеры способны произвести революцию в вычислениях, сделав некоторые типы классически неразрешимых задач решаемыми. Несмотря на то, что ни один квантовый компьютер еще не совершенен, чтобы выполнять вычисления, которые не может выполнить классический компьютер, в настоящее время в этой области наблюдается большой прогресс. Несколько крупных компаний и небольших стартапов уже имеют функционирующие квантовые компьютеры без контроля ошибок (**обнаружения и исправления ошибок в данных при их записи и воспроизведении или передаче по линиям связи.**), состоящие из нескольких десятков кубитов, и некоторые из них даже доступны для общественности через облачный сервер. Кроме того, квантовые симуляторы

добиваются успехов в различных областях - от молекулярной энергетики до физики многих тел.

По мере появления небольших систем в интернете начинает развиваться область, ориентированная на применение квантовых компьютеров в ближайшем будущем. Этот прогресс может позволить реализовать некоторые преимущества и идеи квантовых вычислений задолго до завершения поисков крупномасштабного квантового компьютера с контролем ошибок.