имеют узкую направленность на определенные программы или круг пользователей.

К сожалению, большинство компьютерных тренажеров разработаны для людей, которые уже имеют определенный опыт работе на компьютере и в сфере компьютерной безопасности. Часто для людей, которые не имеют опыта или имеют малый опыт общения с компьютерами использование такого тренажера является невозможным.

Таким образом, для решения этой проблемы мы предлагаем создавать интуитивно понятные тренажеры с подробным алгоритмом действий, имеющих широкую направленность на всевозможные проблемы компьютерной безопасности, с которыми может столкнуться начинающий пользователь. Основные плюсы такого тренажера это понятный интерфейс программы, подробная имитация операционной системы и игровая форма выполнения заданий, которая поможет обучающимся быстрее понять способы решения проблемы.

Дерягин П.А., РГППУ
КТ-304

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ В КВАНТОВЫХ КОМПЬЮТЕРАХ

Каждый день на свет появляются все новые компьютеры. Люди привыкли видеть везде их применение, даже не задумываясь о том, какими мощностями должны обладать эти машины. А тем временем требования к компьютерам возрастают в геометрической прогрессии, но наука не стоит на месте, разрабатываются принципиально новые виды компьютеров. Одним из таких видов можно считать квантовые компьютеры. В нашей статье мы рассмотрим и сравним наиболее распространенные алгоритмы вычисления в квантовых компьютерах, а также постараемся определить сферу применения этого мощнейшего вычислительного устройства.

Квантовый компьютер — вычислительное устройство, которое путем выполнения квантовых алгоритмов существенно использует при работе квантовомеханические эффекты, такие как квантовый параллелизм (данные в процессе вычислений представляют собой квантовую информацию, которая по окончании процесса преобразуется в классическую путём измерения конечного состояния квантового регистра) и квантовая запутанность (она же «квантовая суперпозиция» – некое объединенное состояние «распада — не распада» атома).

Основным элементом квантового компьютера являются квантовые биты, или кубиты. Обычный бит – это классическая система, у которой есть только два состояния. Можно сказать, что пространство состояний бита – это множество из двух элементов, например из нуля и единицы. Кубит же – это квантовая система с двумя возможными состояниями (например, спин электрона может быть равен либо 1/2, либо –1/2). Но, поскольку система квантовая, ее пространство состояний будет несравненно богаче.

На данный момент наиболее широкое распространение, по мнению ведущих научных центров мира (Columbia University, Toshiba Research Europe, IBM Group) при разработке квантового компьютера получили три алгоритма:

1. Алгоритм Гровера – квантовый алгоритм быстрого поиска в неупорядоченной базе данных. Для N записей поиск осуществляется за время T(N1/2) с использованием T(logN) места. Другими словами, имея функцию y=f(x), которая может быть вычислена с использованием квантового компьютера, алгоритм Гровера позволяет вычислить «x», зная «y». Поиск в базе данных соотносится с обращением функции, которая принимает определенное значение, если аргумент «x» соответствует искомой записи в базе данных. Toshiba Research Group доказало, что данный алгоритм является наиболее быстрым для осуществления линейного поиска. Таким образом мы можем утверждать, что он является самым оптимальным для поиска значений в неупорядоченной базе данных при работе с квантовым компьютером.

2. Алгоритм Шора – позволяет разложить натуральное число n на простые множители за полиномиальное от «log(n)» время. Специалисты IBM еще в 2001 году доказали, что алгоритм факторизации Шора дает экспоненциальный выигрыш по сравнению с соответствующими классическими алгоритмами и алгоритмом Гровера. Таким образом мы можем использовать данный алгоритм для взлома криптографических систем с открытым ключом, хотя для этого безусловно понадобится достаточно мощный квантового компьютер. Метод Шора являет собой единственную реальную возможность взлома RSA на сегодняшний день и потому большинство организаций, занимающихся его изучением, представляют собой крупнейшие компании в области компьютерной безопасности и защиты информационных систем.

3. Алгоритм Дойча-Джоза – сущность его в определении, является ли функция двоичной переменной «f(n)» постоянной (принимает либо значение «0», либо «1» при любых аргументах) или сбалансированной (для половины

области определения принимает значение «0», для другой половины «1»). Он стал одним из первых примеров алгоритмов, предназначенных для выполнения на квантовых компьютерах, а благодаря использованию явления квантовой запутанности и принципа суперпозиции обладает значительным приростом скорости выполнения операций прямого поиска значений некоторого множества. Алгоритм Дойча — Джоза всегда дает верный ответ, совершив лишь одно вычисление значения функции f, благодаря чему мы можем эффективно применять его в сложных математических вероятностных расчетах, то есть там, где выполнение подобных операций на обычных компьютерах, пусть даже они объединены в огромную сеть, заняло бы тысячи лет.

Однако на практике дело обстоит не так хорошо, как в теории. Единственный на сегодня реально существующий квантовый компьютер «Orion» – первая практическая реализация технологии, позволяющей осуществлять одновременно до 65 536 вычислительных потоков. Его создатель – компания D-Wave, полностью посвятила себя и бюджет в 20 млн. долларов на разработку «Orion». Потому, для нас это будет единственный реальный источник информации, из которого мы сделаем некоторые выводы стороны по возможностям применения квантовых компьютеров в реальности. В конечном счете, компьютер Orion – аналоговое устройство. Работа программ квантового компьютера – это процесс аналогового физического моделирования, а программы в цифровых вычислительных машинах по существу выполняют математические процедуры. Отсюда мы можем выявить ряд следующих проблем, связанных с созданием и применением квантовых компьютеров:

- необходимость обеспечения высочайшей точности измерений;
- внешние воздействия могут разрушить квантовую систему или внести в неё искажения;
- сама физическая структура квантового компьютера настолько сложна в реализации, что на сегодняшний день невозможно технически воссоздать его (компьютер) в идеальном состоянии;
- скорость передачи данных безумно мала, что делает невозможным передачу даже относительно небольших пакетов данных.

Однако присутствует и ряд бесспорных, недостижимых обычным компьютером, плюсов:

- квантовый канал передачи данных можно использовать для генерации и передачи криптографический ключей, что делает данный метод теоретически недоступным для взлома;

• квантовый компьютер позволяет производить беспрецедентную параллелизацию вычислений за счет своего кубитового строения;

• квантовый компьютер имеет минимальный расход энергии. Ниобий, использующийся при его построении, – сверхпроводник и, таким образом, не излучает тепло. Квантовый чип непосредственно рассеивает мощность всего несколько нановатт. Для современных супер-компьютеров требуются многоваттные дорогие охлаждающие системы.

Один из ведущих специалистов в области квантовых вычислений Джон Прескилл из Калифорнийского технологического института говорит, что поистине уникальные возможности использования квантового компьютера открываются для быстрого поиска в базах данных, моделирования физических процессов на микроуровне, а профессор из Оксфорда сэр Роджер Пенроуз, всерьез говорят о решающем вкладе квантового компьютера в создание искусственного интеллекта.

Таким образом, мы рассмотрели основные алгоритмы квантового компьютера, выделив те реальные стороны, где применение каждого из них будет наиболее продуктивным. Мы также рассмотрели проблемы применения и построения квантовых систем. На сегодня трудно оценить все плюсы, минусы квантовых компьютеров и их будущее, однако нет сомнения в том, что они установили планку производительности машин на новый, доселе никем даже не предвиденный уровень, и их применение уже в скором времени будет не научным, а практически необходимым, ведь потребности в вычислениях растут намного быстрее, чем техническое оснащение обычных компьютеров. Перспективу развития и применения квантовых компьютеров на сегодня видят крупнейшие корпорации мира (Amazon, IBM Group, Google и многие другие), ежегодно инвестирующие многомиллионные состояния в их разработку.

Литература:

1. Портал современных информационных систем. [Электронный ресурс]. Режим доступа: www.inauka.ru.

2. Физическое описание взаимодействия компонентов квантового компьютера. [Электронный ресурс]. Режим доступа: www.elementry.ru.

3. Портал, посвященный квантовым компьютерам и квантовым алгоритмам. [Электронный ресурс]. Режим доступа: www.quantumcomputers.narod.ru.

4. Международный портал квантовых систем. [Электронный ресурс]. Режим доступа: www.sciencedaily.com.