Д.О. ПРОКОФЬЕВ, В.Н. ЯКОВЛЕВ

ИСПОЛЬЗОВАНИЕ КВАНТОВЫХ ЭФФЕКТОВ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ

Рассматриваются основные принципы квантовых вычислений, математические и технические основы построения квантового компьютера, его отличия от классических вычислительных машин, сложности в реализации и перспективы его использования. Статья адресована студентам и сотрудникам, работающих в сфере информационных технологий.

Квантовые вычисления – это новейшее направление в современной науке. С момента рождения этой идеи прошло чуть больше двух десятилетий. Предпосылки, начальные предположения и гипотезы были высказаны в 1980х годах в работах Фейнмана, Дойча и Брауна [1].

Переломный момент в развитии теории квантовых вычислений произошел в 1994 году. Американский математик Питер Шор [2, 4] показал, что с помощью таких вычислений можно разложить любое, даже очень большое целое число N на простые множители с потрясающей эффективностью, недостижимой при работе на обыкновенных электронных вычислительных машинах. Это имело крайне важное прикладное значение – столь эффективный алгоритм и мощный квантовый компьютер делают возможным взлом криптографических систем с открытым ключом. Однако «криптографическую катастрофу» предотвращает отсутствие сколько-нибудь мощных квантовых компьютеров. В процессе их технической реализации исследователи столкнулись с рядом серьезных сложностей.

Сила квантовых компьютеров заключается в использовании квантовых феноменов: суперпозиции, обратимости и параллелизма. Согласно принципу суперпозиции состояние квантовой системы описывается линейной комбинацией волновых функций (ψ-функций)

$$\psi = \sum_i C_i \psi_i \ , \qquad (1)$$

каждая, из которых, соответствует какому-то определенном состоянию системы. А квадрат модуля коэффициента $|C_i|^2$ характеризует вероятность данного состояния. Получается, что система находится в нескольких состояниях (параллелизм) и только измерение может дать нам конкретный результат, но с определенной (равной $|C_i|^2$) вероятностью. При этом надо учитывать, что сумма вероятностей всех состояний должна быть равна единице:

$$\sum_i |C_i|^2 = 1 \ . \qquad (2)$$

Из одного состояния в другое систему можно переводить с помощью линейного унитарного оператора, то есть такого, который сохранит выполнение условия (1). Обратимость состоит в том, что линейные унитарные операторы позволяют вернуть систему в первоначальное состояние. Чтобы использовать возможности, которые дают нам эти эффекты, нам необходимо разработать совершенно новые подходы к машинным вычислениям [2].

В классическом компьютере носителями информации являются биты, с которыми можно выполнять арифметические операции. В квантовой модели вычислений носителями информации служат квантовые биты – кубиты (от Quantum Bit). Обычный бит – это классическая система, у которой есть только два возможных состояния. Можно сказать, что пространство состояний бита – это множество из двух элементов: из нуля и единицы. Кубит же – это квантовая система с двумя базовыми состояниями. Обозначаются эти состояния так: $|0\rangle$ и $|1\rangle$. Но на самом деле, у квантовой системы гораздо большее пространство состояний, чем у обычного классического триггера. Кубит может находиться и в смешанном состоянии $\alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in C$, и согласно (2)

$$|\alpha|^2 + |\beta|^2 = 1. \quad (3)$$

Имеется ряд примеров квантовых систем, состояния которых можно представить в подобном виде. Это электрон, у которого спин может быть равен либо +1/2 либо –1/2, атомы в кристаллической решетке при некоторых условиях.

Это электрон, у которого спин может быть равен либо +1/2 либо –1/2, атомы в кристаллической решетке при некоторых условиях.

В таком пространстве состояний можно выполнять унитарные преобразования, то есть такие, при которых сохраняется условие (3). С точки зрения геометрии эти преобразования – прямой аналог вращении и симметрий обычного трехмерного пространства. Согласно принципу суперпозиции, можно складывать состояния, вычитать их, умножать на комплексные числа.

Таким образом, по отношению к компьютеру классическому, в квантовом компьютере имеет место аналогичная ситуация. Он тоже работает с нулями и единицами. Но его функциональные элементы реализуют действия прямо в фазовом пространстве некоторой квантовой системы – при помощи унитарных преобразований этого пространства на входе логического устройства обычного компьютера мы имеем последовательность состояний битов, которая называется словом. В дальнейшем над этим словом будет выполнен некий алгоритм, состоящий из базовых операций. На выходе логического устройства мы имеем измененное алгоритмом слово. В квантовом компьютере происходит то же самое.

Если в каждом кубите фиксирован базис (он будет состоять из двух векторов), то фазовое пространство – это комплексное линейное пространство, базис которого индексирован словами из нулей и единиц. Таким способом двоичное слово на входе определяет базисный вектор.

Итак, вход – двоичное слово, определяющее один из базисных векторов. Сам же алгоритм – предписанная последовательность элементарных операторов. Применяем эту последовательность к вектору на входе, в результате получаем некоторый вектор на выходе.

Согласно квантовой механике, пока система меняется под воздействием приложенных унитарных операторов (то есть операторов, сохраняющих длину вектора), мы не можем сказать, в каком именно классическом состоянии она находится. Когда мы пытаемся это выяснить, мы все равно измеряем какие-то классические значения. Если мы имеем дело с системой, состояние которой – либо спин влево, либо спин вправо, и если мы все-таки выясним, какой именно спин, то мы получим одно из двух в любом случае. А вот вероятности того, что мы получим тот или другой результат, – это квадраты модуля коэффициентов разложения. Квантовая механика утверждает, что точно предсказать результат измерения нельзя, но вероятности возможных результатов вычислить можно. Вероятность возникает в процессе измерения. А пока система живет, для нас существенно, что там есть сам этот вектор.

Другими словами, существенно, что система «находится одновременно во всех возможных состояниях». Возникает эффект параллелизма в вычислениях: в случае нашей системы из двух кубитов мы проводим действия со всеми возможными ее состояниями: 00, 01, 11, 10.

Чтобы интерпретировать ответ, надо заранее условиться, что какой-то бит – предположим, первый – это бит ответа. Пусть алгоритм завершил работу. В итоге получился какой-то вектор, не обязательно базисный. Тогда мы можем сказать, что первый бит с некоторой вероятностью равен 1. И требование к алгоритму такое: если ответ «да», то вероятность того, что первый бит, равен 1, должна быть, допустим, больше двух третей.

Одно из фундаментальных отличий квантового компьютера от классических – это обратимость операций. Допустим, на обычной вычислительной машине мы провели простую операцию сложения a и b и получили результат $c = a + b$. Но после этого по данному числу c мы никак не сможем восстановить исходные операнды a и b. С другой стороны, почти все операции на квантовых компьютерах обратимы, поскольку они представляются унитарными линейными операторами квантовой механики.

Вероятностный характер результата, обратимость и параллелизм – эти эффекты используются во многих квантовых алгоритмах, и именно они позволяют выполнять нестандартные, сверхпроизводительные ходы в квантовых алгоритмах.

Для примера рассмотрим уже упоминавшийся квантовый алгоритм Шора – алгоритм вычисления дискретного логарифма.

Пусть p – простое число. Множество $F_p = \{0,..., p-1\}$ называется полем вычетов по модулю p. Элементы этого поля перемножаются по следующему правилу: вычисляется их произведение как обычных целых чисел, и берется остаток от его деления на p. Элемент x поля F_p называется первообразным корнем, если путем возведения в степень из него можно получить все ненулевые элементы поля. Теперь пусть у нас есть поле вычетов по модулю простого числа. Если задан первообразный корень и задана степень, то возвести в степень можно быстро. Дискретный логарифм – это обратная задача. Дан первообразный корень и какой-то элемент поля; нужно найти, в какую степень нужно возвести этот корень, чтобы получить данный элемент. Эта задача очень сложна. Современные криптографические системы исходят из того, что вычислить дискретный логарифм за приемлемое время невозможно, если модуль p – достаточно большое простое число [3, 4].

Шор использовал существенно квантовую идею. Пусть имеется базис в фазовом пространстве квантовой системы. Он состоит из классических состояний. Но в линейном пространстве много базисов. Можно найти некий оператор, который эффективно строит другой базис, затем можно к нему перейти, сделать там вычисления, вернуться обратно в исходный базис и получить результат, совершенно отличный от того, что мы имели бы в классическом базисе. Это и есть прямое использование всех квантовых преимуществ. Интересно, что преобразование, строящее необходимый базис, – это дискретное преобразование Фурье, которое имеет принципиальное значение и для физики, и для математики.

Рассмотрим алгоритм Шора подробнее [4]. На вход алгоритма подается составное число N, на выходе – простое число p и нетривиальный делитель q, такие что $N = p \cdot q$.

Основные шаги:

1. Выбрать случайный остаток a по модулю N.
2. Проверить НОД (a, N) == 1 (числа должны быть взаимно простыми).
3. Найти порядок r остатка a по модулю N (минимальное число r, при котором $\frac{a^r - 1}{N}$ – целое). Порядок r является периодом функции $f(x) = a^x \bmod N$.
4. Если r – четен, вычислить НОД($a^{\frac{r}{2}} - 1, N$).

Полученное на четвертом шаге число с большой вероятностью окажется нетривиальным делителем $N – q$.

Таким образом, задача разложения числа N на множители сводится к быстрому нахождению периода r для случайно подобранного числа a.

Техническая реализация этого алгоритма – это нахождение периода волновой функции текущего состояния системы кубитов, к которой применено дискретное преобразование Фурье. Доказано, что с большой вероятностью период этой функции равен $\frac{M}{r}$, где M – число использованных в вычислении входных векторов ($M \geq N^2$). Повторяя алгоритм, можно увеличивать точность значения $\frac{M}{r}$. В классической вычислительной математике говорят, что алгоритм сходится к $\frac{M}{r}$.

Есть еще одна область применения КК, где заведомо возможен радикальный выигрыш у существующих технологий. Это моделирование самих квантовых систем. Есть очень серьезные препятствия для моделирования квантовых систем на классических компьютерах – за счет экспоненциального роста размерности, для моделирования, например, десяти спинов взаимодействующих электронов обычный компьютер должен

оперировать с тысячемерным пространством. В таком случае, моделирование системы хотя бы из ста электронов не представляется возможным. А если создать вычислительное устройство, которое ведет себя квантовым образом, то, по крайней мере, один важный класс задач на нем есть смысл решать – можно моделировать реальные квантовые системы, возникающие в физике, химии, биологии.

Хоть квантовые компьютеры и представляют богатые возможности для обработки информации, создать стабильно работающий вычислитель такого типа пока не представляется возможным. Основная проблема реализации квантового компьютера состоит в следующем: любая физическая реализация будет приближенной. Во-первых, мы не сможем сделать прибор, который будет давать нам абсолютно произвольный вектор фазового пространства. Во-вторых, работа любого устройства подвержена разнообразным случайным ошибкам. А в квантовой системе такие минимальные ошибки запрещены. Если в систему попадет, к примеру, хотя бы один «лишний» фотон, он может провзаимодействовать с ней и полностью разрушить текущее состояние системы, а значит, прервать процесс вычислений.

В целом, физической системе, претендующей на реализацию квантового компьютера, можно предъявить пять требований:

1. Система должна состоять из точно известного числа частиц.
2. Должна быть возможность привести систему в точно известное начальное состояние.
3. Степень изоляции от внешней среды должна быть очень высока.
4. Надо уметь менять состояние системы согласно заданной последовательности унитарных преобразований ее фазового пространства.
5. Необходимо иметь возможность выполнять такие измерения состояния системы, которые переводят ее в одно из чистых состояний.

Из этих пяти задач наиболее трудными считаются третья и четвертая. От того, насколько точно они решаются, зависит точность выполнения операций. Пятая задача тоже весьма неудобна для решения, так как измерить состояние отдельной частицы нелегко.

Впрочем, несмотря на серьезные технические ограничения, появляются сообщения, что создаются реальные квантовые системы с небольшим числом кубит. В ноябре 2009 года физикам из Национального института стандартов и технологий в США впервые удалось собрать настоящий программируемый квантовый компьютер, состоящий из двух кубит.

Таким образом, эксперименты есть, но это даже не прототипы. Два бита – это и для классического, и для квантового компьютера слишком мало. Для вычисления дискретного логарифма нужно порядка тысячи кубит, для моделирования квантовых процессов – уже более ста тысяч кубит.

Задача эта возникла слишком недавно, и не исключено, что она потребует каких-либо фундаментальных исследований в самой физике. Поэтому в обозримом будущем ожидать появления квантовых компьютеров не приходится.

Однако решения задач, поставленных сейчас, в дальнейшем могут привести к еще более интересным открытиям в прикладных областях, таких, как быстрая передача и обработка данных, распознавание образов, алгоритмизация нелинейных процессов, криптография, моделирование сложных систем. А если в обозримом будущем все-таки удастся построить полноценный работающий квантовый компьютер, то информационное общество получит в свое распоряжение наиболее совершенный инструмент обработки больших потоков информации.

ЛИТЕРАТУРА

1. Ekert A., Hayden P., Inamori H. Basic Concepts in quantum computation. – UK : University of Oxford, 2000. – 90 с.
2. Elemer E., Rosinger F. Basics of Quantum Computation (part 1). – University of Pretoria, South Africa, 2004. – 87 с.
3. Ожигов Ю.И. Квантовые вычисления, учебно-методическое пособие. – М.: МГУ, 2003. – 104 с.