УДК 621.3

Квантовый компьютер

Петрулевич А.В.
Научный руководитель – к.т.н., доцент ЕЖОВ В.Д.

Впервые, идея о квантовых вычислениях была заявлена Юрием Маниным в 1980, а теоретическая модель квантового компьютера — Ричардом Фейнманом в 1981. Технологическая реализация такого компьютера была описана Полом Бениоффом в 1982. В 1989 была разработана концепция квантовых логических вентилей Дэвидом Дойчем. Однако, резкий скачок в исследовании и разработке квантовых компьютеров вызвала статья Питера Шора 1997 года. В ней описывается алгоритм, позволяющий разложить натуральное число N на простые множители за полиномиальное от log(N) время, факторизация или нахождения дискретного логарифма. Поскольку алгоритмы обычных компьютеров имеют экспоненциальную зависимость, то, например, временные затраты современного суперкомпьютера, выполняющего более 10^{15} операций в секунду, на разложение числа с 500 знаками на простые множители возрастают до 5 миллиардов лет. Квантовый компьютер, выполняющий 10^{6} операций в секунду, решил бы аналогичную задачу за 18 секунд. Так как алгоритм факторизации используется в криптоанализе, а именно в расшифровке данных, то возможность применения данной технологии в военной, экономической и других сферах предполагает огромные перспективы развития.

Квантовый компьютер — это вычислительное устройство, которое использует квантово-механические явления для передачи и обработки данных. В обычных компьютерах, работающих на основе транзисторов и кремниевых чипов, для обработки информации применяется бинарный код. Бит, как известно, имеет два возможных значения — 0 и 1, и может находиться только в одном из них. Что же затрагивает область квантового компьютера, то его работа организуется с помощью принципа суперпозиции, а вместо битов используются квантовые биты, именуемые q–битами или кубитами. У q–бита также имеется два основных состояния: ноль и единица. Однако, благодаря суперпозиции, q–бит может принимать значения, полученные путем их комбинирования, и находиться во всех этих состояниях одновременно, например, 72% нуля и 28% единицы. В алгоритмах для квантовых компьютеров большую роль играет интерференция, а именно помехи деструктивно интерферируют, а сигналы — конструктивно. Для вычисления состояний q–битов используются обозначения Дирака, а для удобства представления, q–бит изображается с помощью сферы Блоха, в которой любое преобразование волновой функции можно представить, как простое перемещение точки по поверхности сферы.

К квантовому компьютеру предъявляется ряд требований:

- Масштабируемость физической системы: возможность увеличения количества q–битов до необходимой величины, которая будет достаточна для сложных вычислений;
- Инициализация системы: изначально система должна находится в точном, известном и простом состоянии;
- Долговечность: время выполнения операций на всех вентилях должно быть больше времени перехода системы в декогерентное состояние;
- Реализация необходимого набора операций (вентилей): вентиль Адамара, вентиль фазового сдвига, вентиль CNOT и вентиль $\pi/8$;
- Возможность определения конечного состояния отдельного q–бита;
- Корректность передачи q–битов между конечными точками;
- Преобразование данных, хранящихся в виде стационарных q–битов в сетевые.

Крупнейшими компаниями, участвующими в разработке квантовых компьютеров, являются: D–Wave, Google, IBM, Intel и др.

Например, квантовые компьютеры компании D-Wave являются узконаправленными, но самыми мощными. В частности, квантовый компьютер D-Wave 2000Q содержит 2048 q–битов, 5600 сцепок, 128000 Джозефсоновских переходов. Процессор построен из тонких,

расположенных в форме решетки, ниобиевых (Nb) петель, которая составляет 1 q–бит. Температура, при помощи рефрижератора растворения, в верхней части установки достигает 50К и понижается в сторону квантового процессора до 15мК, что холоднее межзвездного пространства в 180 раз. Магнитная индукция достигает области меньше 1 нТл, что меньше магнитного поля Земли в 50000 раз.

Языки программирования, работающие на виртуальной машине: Q#, LIQUi, QCL, Quipper и др.

Платформы, позволяющие использовать и изучать квантовые компьютеры: IBM Quantum Experience, Quantum Computing Playground, Qbsolv и др.

Ведутся разработки по передаче q–битов через оптоволокно, облучая молибден (Mo) в кристаллах карбида кремния (SiC), $\bar{e}$ переходил на более высокий энергетический уровень. Затем происходила релаксация $\bar{e}$, и он возвращался на прежний уровень, испуская фотон. Далее создавалась суперпозиция атомов при воздействии двух резонансных оптических полей. В результате удалось создать q–бит, в котором сохранялась суперпозиция в течение длительного промежутка времени, и он испускал фотон длина волны которого равна 1100 нм.

Применение квантовых компьютеров многогранно:

Машинное обучение: разработка искусственного интеллекта, обнаружение статистических аномалий, запоминание схем и изображений, обучение нейронных сетей, классификация неструктурированных данных и др.

Финансовое моделирование: обнаружение дестабилизации рынка, развитие торговой стратегии, оптимизация ценообразования активов и др.

Безопасность: распределение ресурсов и нахождение оптимальных путей, обнаружение компьютерных вирусов, криптография и криптоанализ, и др.

Медицина: выявление подделок, молекулярное моделирование и др.

Хотя, квантовая революция только начинается, предполагается, что при огромном вкладе в развитие данной отрасли науки, квантовые компьютеры помогут раскрыть тайны микромира и построить фундамент для новых исследований.