УДК 004

О КВАНТОВЫХ АЛГОРИТМАХ

К.В. Кошелев
АО «Навигатор»
Россия, 199106, Санкт-Петербург, Шкиперский проток ул., д. 14, к. 19, лит. З
E-mail: kkoshelev@navigat.ru

Ключевые слова: квантовый компьютер, алгоритм, программное обеспечение, киберфизические системы, квантовая логика.

Аннотация: Квантовые вычисления представляют собой бурно развивающееся направление науки и техники. Весьма нетривиальной в этой связи является задача написания программного обеспечения для квантового компьютера. Авторы доклада доказывают теорему, утверждающую эквивалентность квантового алгоритма и унитарного оператора. Затем, основываясь на свойствах этого оператора, авторы делают вывод о методах оценки эффективности квантового алгоритма.

1. Введение

С самого начала появления вычислительных систем не прекращается борьба за увеличение их эффективности. Не смотря на многогранность понятия эффективность часто на практике этим термином обозначают скорость обработки информации. Более эффективной считается вычислительная система производящая расчет в соответствии с поставленной задачей при прочих равных условиях за меньшее время.

В процессе борьбы за производительность лучшие умы человечества добрались до идеи использовать квантово-механические системы для обработки информации. Изначально мысль о том, что квантовые компьютеры могут более эффективно обрабатывать информацию по сравнению с обыкновенными компьютерами, пришла в голову физикам, которые занимались моделированием процессов, протекающих в микромире. Было замечено, что конвенциональные компьютеры, используемые для расчетов, не достаточно эффективны для моделирования квантово-механических объектов и процессов. Поэтому Р. Фейнманом [1] было высказано предположение, что вычислительные системы, управляющиеся законами квантовой механики, будут обладать большей производительностью. Наконец, значимой вехой в развитии теории квантовых вычислений явилось открытие П. Шором [2] квантового алгоритма факторизации целых чисел и демонстрации его квантового превосходства. В настоящее время существуют фирмы, сферой деятельности которых является написание программного обеспечения для квантовых компьютеров. Серьезным стимулирующим фактором для производителей программного обеспечения является наличие компаний, производящих сами квантовые компьютеры на коммерческой основе.

Упомянутый выше термин квантовое превосходство имеет совершенно конкретный смысл. Он означает, что количество операций, которое является функцией числа квантовых битов, используемых в расчете, растет медленнее аналогичного числа операций для лучшего конвенционального алгоритма при стремлении числа классических битов к бесконечности. Таким образом задача изобретения квантового алгоритма сводится к написанию последовательности элементарных операций или программы для квантовой вычислительной системы для начальных условий произвольного размера и последующее доказательство квантового превосходства.

2. Генератор алгоритма

Квантовый алгоритм или программа для квантового компьютера, это последовательность элементарных операций, выполняемых компьютером для получения результата. Квантовый компьютер вне зависимости от его физической реализации это квантово-механическая система. Исходные данные для расчета кодируются в коэффициентах волновой функции, представляемой в виде суперпозиции конечного набора базисных функций. Сам расчет представляет собой действие унитарной матрицы на волновую функцию входных данных. Таким образом эта унитарная матрица и представляет собой квантовый алгоритм для исходных данных подходящего конечного размера.

Важно отметить, что существование квантового алгоритма означает существование унитарной матрицы произвольного конечного размера. Можно сказать, что квантовый алгоритм, это то общее, что есть у бесконечного множества унитарных матриц. В квантовой механике такой генератор матриц называется оператором, а каждая конечная матрица называется представлением оператора в конечном базисе векторов.

Таким образом можно сформулировать утверждение, что для существования квантового алгоритма необходимо и достаточно существование унитарного оператора. Достаточность очевидна. Если задан оператор, то найти его матричное представление в любом базисе не представляет труда. Необходимость также доказывается тривиально. Матрица большего порядка строится из матрицы меньшего порядка просто путем добавления новых матричных элементов к ее матричным элементам (как показано на рис. 1).

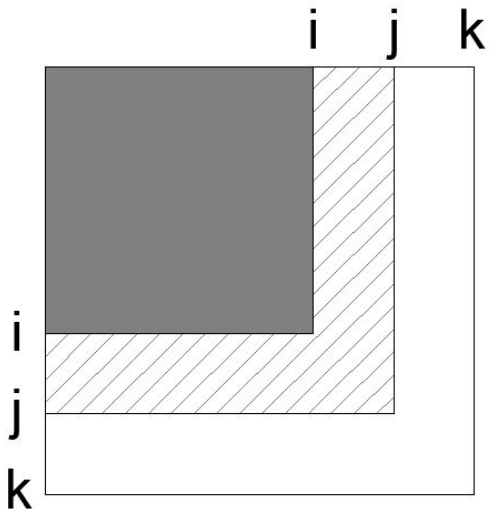

Рис. 1. На рисунке изображены три матрицы. Первая образована матричными элементами с индексами от 1 до i. Вторая матрица является расширением первой путем добавления матричных элементов с индексами от i до j (заштриховано). Третья матрица является расширением второй путем добавления матричных элементов с индексами от j до k.

В целом вся конструкция является матричными представлением оператора, который однозначно существует, так как существует его матричное представление. Иными словами, доказательство существования искомого оператора осуществляется его явным построением. Эквивалентность квантового алгоритма оператору может сыграть важную роль в развитии методов автоматического построения алгоритмов.

3. Эффективность алгоритма

Как показано выше квантовый алгоритм эквивалентен унитарному оператору. Собственные значения λ_i унитарного оператора $\widehat{U}$, в общем случае комплексные, по модулю всегда равны единице. Если задан оператор $\widehat{U}$, то можно построить другой оператор, имеющий те же собственные функции, но обладающий другим набором собственных значений, как показано в формуле (1)

(1) $$\widehat{U} - (\lambda_i - w_i)|i\rangle\langle i|,$$

где λ_i это старое собственное число, w_i – новое, а $|i\rangle$ это соответствующий собственный вектор. Таким образом имея один оператор, можно получить бесконечное множество операторов, обладающих одинаковыми наборами собственных векторов, но при этом имеющих различные наборы собственных значений.

Частный случай унитарного оператора-ортогональный оператор, который в матричном представлении дается ортогональной матрицей. Собственные значения ортогонального оператора равны плюс или минус единице. Представим, что некий квантовый алгоритм дается ортогональным оператором и зададимся вопросом об эффективности этого алгоритма. Выберем в качестве базиса представления набор собственных функций нашего ортогонального оператора. Тогда в этом представлении работа квантового компьютера представляется формулой (2)

(2) $$|out\rangle = \widehat{U}|in\rangle,$$

где $|in\rangle$ это входные данные задачи, $|out\rangle$ – результат обработки данных алгоритмом, а $\widehat{U}$ это матрица алгоритма, имеющая диагональную форму, причем на главной диагонали находятся собственные значения.

Так как собственные значения ортогональной матрицы равны плюс или минус единице, то действие оператора алгоритма в формуле (2) сводится к изменению знака у коэффициентов вектора входных данных в том случае если эти коэффициенты умножается на собственное значение равное минус единице. Иными словами, действие алгоритма-оператора естественным образом представляется в виде набора элементарных операций, каждая из которых представляет собой изменения знака соответствующего коэффициента в разложении на противоположный. Легко видеть, что при таком подходе эффективность алгоритма определяется поведением количества отрицательных собственных значений оператора при стремлении размерности задачи к бесконечности.

4. Заключение

Установленный факт об эквивалентности квантового алгоритма и унитарного оператора открывает перспективы развития методов построения квантовых алгоритмов автоматическим путем, то есть при минимальном участии человека-программиста. Для этого можно выбрать оператор в виде некоторого приближенного оператора с набором коэффициентов, подлежащих определению. Нахождение параметров приближенного оператора решает проблему написания программы для любого объема входных данных, так как этот оператор позволит сгенерировать матрицу произвольного порядка. Выражения подобные, даваемым формулой (1) предоставляет дополнительные возможности для гибкой модификации алгоритмов.

Свойства оператора, реализующего квантовый алгоритм, позволяют ввести понятие элементарной операции для квантового компьютера естественным способом. Это предоставляет возможность оценить эффективность или скорость выполнения программы для квантового компьютера.

Список литературы

1. Feynman R.P. Simulating Physics with Computers // International Journal of Theoretical Physics. 1982. Vol. 21, No. 6/7. P. 467.
2. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computers // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124.