

КВАНТОВЫЙ КОМПЬЮТЕР

Авдей А.С.

Кафедра информационных технологий автоматизированных систем

Научный руководитель: Герман О.В., к.т.н., доцент

e-mail: alexcre8or@gmail.com

Аннотация — Квантовый компьютер — вычислительное устройство, работающее на основе квантовой механики. Квантовый компьютер принципиально отличается от классических компьютеров, работающих на основе классической механики.

Ключевые слова: квант, кубит, компьютер

Квантовый компьютер использует для вычисления не обычные (классические) алгоритмы, а процессы квантовой природы, так называемые квантовые алгоритмы, использующие квантовомеханические эффекты, такие как квантовый параллелизм и квантовая запутанность.

Если классический процессор в каждый момент может находиться ровно в одном из состояний $|0\rangle, |1\rangle, \dots, |N-1\rangle$, (обозначения Дирака) то квантовый процессор в каждый момент находится одновременно во всех этих базисных состояниях, при этом в каждом состоянии $|j\rangle$ — со своей комплексной амплитудой λ_j . Это квантовое состояние называется «квантовой суперпозицией» данных классических состояний и обозначается как

$$|\psi\rangle = \sum_{j=0}^{N-1} \lambda_j |j\rangle. \quad (1)$$

Итак, в одной двоичной ячейке квантового компьютера, называемой кубитом, может храниться не только одна из двух цифр двоичного счисления, 0 или 1 (как было бы в случае классического компьютера), но одновременно обе эти цифры. Например, в двух кубитах могут храниться одновременно 4 двоичных числа 00, 01, 10 и 11. А если в некотором регистре квантового компьютера содержится N кубитов, то в таком регистре может храниться одновременно 2^N двоичных чисел длины N . И при действии квантового компьютера одновременно обрабатываются все эти числа. Это и есть квантовый параллелизм. Если бы в нашем распоряжении были только классические компьютеры, каждый из которых работает с двоичными числами длины N , то для одновременной обработки 2^N таких чисел было бы необходимо 2^N компьютеров.

В отличие от классических, квантовые компьютеры не универсальны: не для всяких вычислительных задач существует алгоритм их решения на квантовом компьютере. До сих пор найдено лишь небольшое число квантовых алгоритмов. Наиболее известные квантовые алгоритмы:

- 1) Алгоритм Шора (факторизация)
- 2) Алгоритм Гровера (быстрый поиск в неупорядоченной базе данных)
- 3) Алгоритм Дойча — Джоза (ответ на вопрос,

постоянная или сбалансированная функция)

Квантовые алгоритмы благодаря использованию явления квантовой запутанности и принципа суперпозиции обладают значительным приростом скорости выполнения по сравнению с соответствующими классическими алгоритмами. Решение уравнения Шредингера для этого потенциала.

Физической системе, реализующей квантовый компьютер, 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 «сильные измерения» состояния системы (то есть такие, которые переводят ее в одно из чистых состояний).

Квантовая система эффективно «решает» сложную вычислительную задачу — моделирует саму себя. На квантовом компьютере можно моделировать любую квантовую систему за полиномиальное число шагов. Это позволит (при наличии квантового компьютера) предсказывать свойства молекул и кристаллов, проектировать микроскопические электронные устройства размером в несколько десятков ангстрем. Сейчас такие устройства находятся на пределе технологических возможностей, но в будущем они, вероятно, будут применяться в обычных компьютерах.

Квантовые вычисления дают выигрыш по сравнению с классическими в поиске нужной записи в неупорядоченной базе данных (алгоритм Гровера) и аналогичные задачи (например распознавание изображений — то, что демонстрировала D-Wave на своих первых чипах). В перспективе квантовый компьютер может приблизить нас к решению задачи создания искусственного интеллекта.

Не исключено, что в информационном обществе появление квантового компьютера сыграет ту же роль, что в свое время, в индустриальном, — изобретение атомной бомбы. Действительно, если последняя является средством «уничтожения материи», то первый может стать средством «уничтожения информации»

- [1] Вычислимое и невычислимое. / Манин Ю.И. - М.: Советское радио, 1980 — 15 с.
- [2] Квантовые вычисления: алгоритмы и исправление ошибок. / Китаев А.Ю.
- [3] Человек и квантовый мир. / Менский М.Б. — Москва, «Век2», 2007.