

## 8. Квантовые вычисления

Идея использовать квантовые элементарные ячейки вместо классических была впервые чётко сформулирована в начале 1980-х годов физиками Фейнманом и Манином. Основная мотивация состояла в том, что классические компьютеры плохо справляются с моделированием квантовых систем, поскольку размерность пространства состояний растёт экспоненциально. Квантовые вычисления, напротив, естественным образом используют суперпозицию и интерференцию состояний, что потенциально обеспечивает высокий параллелизм вычислений.

Квантовая элементарная ячейка называется квантовым битом, или кубитом. Его состояние описывается волновой функцией  $\psi$ , которая представляется вектором. Базисными состояниями кубита являются  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  или  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Физическая реализация кубита может быть различной. Например, электрон имеет 3 характеристики: масса, заряд и спин. Спин можно использовать как значение кубита

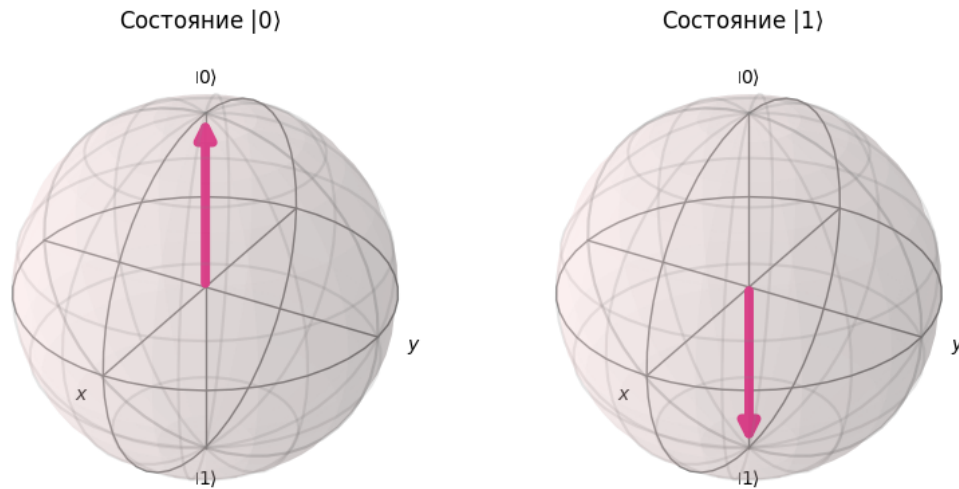
В классических компьютерах используется двоичная логика, основанная на наличии или отсутствии электрического тока. Такое кодирование обеспечивает высокую помехоустойчивость: небольшие флуктуации напряжения не приводят к ошибке логического состояния.

В квантовых системах ситуация иная: состояния чрезвычайно чувствительны к внешним воздействиям, что является одной из ключевых инженерных проблем квантовых вычислений. Состояния 0 обозначаются  $|0\rangle$ , а состояние 1 –  $|1\rangle$

Квантовые ячейки также могут обладать смешанными состояниями  $\alpha|0\rangle + \beta|1\rangle$ . Такие кубиты могут иметь состояние  $|0\rangle$  с вероятностью  $|\alpha|^2$ , а состояние  $|1\rangle$  с вероятностью  $|\beta|^2$ . Из-за этого  $|\alpha|^2 + |\beta|^2 = 1$

Элементы в матричной записи обозначают  $\alpha$  и  $\beta$ . В общем случае  $\alpha$  и  $\beta$  – комплексные числа. Для отображения вектора состояния нужно четырехмерное пространство. Так как  $|\alpha|^2 + |\beta|^2 = 1$ , все физически различимые состояния одного кубита можно представить точками на единичной сфере, так называемой сфере Блоха. При стандартной параметризации  $\alpha = \cos \frac{\theta}{2}$  и  $\beta = e^{i\varphi} \sin \frac{\theta}{2}$  каждому состоянию соответствует точка с углами  $(\theta, \varphi)$

Сфера Блоха позволяет визуализировать только один кубит. Так выглядят  $|0\rangle$  и  $|1\rangle$ :



Квантовый компьютер должен иметь более 1000 хорошо различаемых кубитов и обеспечить условия для приведения входного регистра в исходное основное базисное состояние

Практический квантовый компьютер должен содержать большое число хорошо различимых кубитов (порядка сотен или тысяч), обеспечивать их инициализацию в заданное базисное состояние и позволять выполнять управляемые операции над ними. Ключевым параметром является когерентность кубитов — время, в течение которого сохраняется квантовая суперпозиция. Типичные времена когерентности составляют миллисекунды или меньше, однако при тактовых частотах порядка гигагерц за это время удаётся выполнить миллионы квантовых операций. Результат вычислений при этом носит вероятностный характер и извлекается посредством измерений

Хотя квантовый регистр физически может быть очень малым по размеру, управление им требует чрезвычайно сложной экспериментальной инфраструктуры: сверхнизких температур, вакуума, экранирования от внешних полей и высокоточной электроники

Квантовые компьютеры находят применение в моделировании молекул и материалов, оптимизационных задачах, машинном обучении и, в частности, в криптографии. Например, алгоритм Шора позволяет эффективно факторизовать большие числа, что делает уязвимыми классические криптографические схемы. В то же время реализация масштабируемых квантовых компьютеров сталкивается с серьёзными технологическими трудностями, и на текущий момент такие устройства находятся на экспериментальной стадии

Состояние двух кубитов можно записать так:  $(\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) = \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle$

Некоторые двухкубитные состояния не допускают представления в виде произведения состояний отдельных кубитов — такие состояния называются запутанными

Для работы с кубитами также существуют логические операции – квантовые вентили или гейты. Так как состояние можно представить волновой функцией, то вентиль можно представить оператором (а значит и матрицей)

Однокубитные вентили описываются матрицей  $2 \times 2$ , двухкубитные –  $4 \times 4$ ,  $n$ -кубитные –  $2^n \times 2^n$ .

Из-за этого матрицы вентилей для больших чисел кубитом занимает очень много памяти

Рассмотрим простейшие квантовые гейты:

- Гейт Адамара (Hadamard) – гейт, который состояние  $|0\rangle$  переводит в состояние  $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$  (то есть с равновероятными состояниями) и описывается матрицей  $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

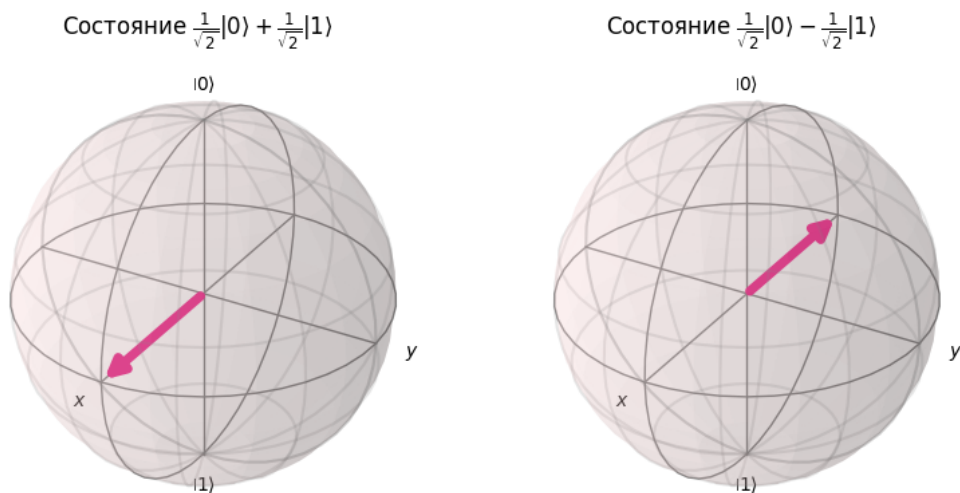
Физически гейт Адамара может быть реализован, например, с помощью переменного магнитного поля, управляющего спином электрона, или короткого лазерного импульса, воздействующего на атом

На схемах он изображается так:

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Здесь одна строка – это кубит и примененные к нему гейты. Использование гейта Адамара в литературе называют «приготовлением кубита», поскольку он переводит кубит из определённого базисного состояния в квантовую суперпозицию

Также гейт Адамара переводит состояние  $|1\rangle$  в  $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$



- Гейт X (или гейт NOT) инвертирует состояние, то есть переводит из  $|0\rangle$  в  $|1\rangle$  и из  $|1\rangle$  в  $|0\rangle$ . По сути гейт переворачивает состояния на сфере Блоха по оси  $OX$ , а его матрица

равна  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Гейт X изображается так:

$$\begin{aligned} |0\rangle &\text{---} \boxed{X} \text{---} \longrightarrow |1\rangle \\ a|0\rangle + b|1\rangle &\text{---} \boxed{X} \text{---} \longrightarrow b|0\rangle + a|1\rangle \end{aligned}$$