INFORMATICA CUANTICĂ

Acad. AȘM, Profesor univ. Sidorenko Anatolie

Institutul de Inginerie Electronica
și Nanotehnologii al UTM

E-mail: sidorenko.anatoli@gmail.com
anatolie.sidorenko@mib.utm.md
Tel./viber *+37369513294*

Тема 3. Принципы построения и работы идеального квантового компьютера

3.1. Идеальный квантовый компьютер

Схема квантового компьютера представлена на рис. 5. По существу квантовый компьютер представляет собой регистр из n кубитов, управляемых внешними (классическими) сигналами. Квантовый компьютер встроен в классическое окружение, состоящее из управляющего классического компьютера и генераторов импульсов, управляющих эволюцией кубитов, а также средствами измерений состояния кубитов. В ходе вычислений к регистру n можно добавить другие регистры, играющие вспомогательную роль.

Назовем идеальным квантовый компьютер, состояния которого всегда когерентны. Это означает, во-первых, отсутствие взаимодействия компьютера с окружением, создающим шумы и нарушающим когерентность вектора состояния компьютера (декогерентизация); во-вторых, в идеальном квантовом компьютере внешние сигналы осуществляют точное управление.

Вектор состояния $|\psi\rangle$ квантового регистра из n кубитов представляет собой разложение по 2^n базисным состояниям регистра $|i_1 \dots i_n\rangle, \dots, i_n = \{0, 1\}$:

$$|\psi\rangle = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} |i_1 \dots i_n\rangle \qquad (17)$$

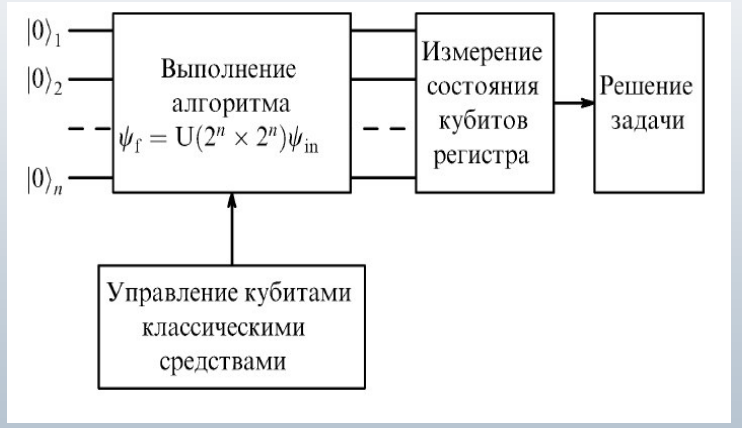

Рис. 5. Схема квантового компьютера.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.1. Идеальный квантовый компьютер

Здесь суперпозиция $|\psi\rangle$ является вектором в 2^n-мерном векторном пространстве, $|i_1 \dots i_n\rangle$ — 2^n базисных векторов (ортов) этого пространства, $a_{i_1,\dots,i_n}$ — проекции вектора $|\psi\rangle$ на направления ортов $|i_1 \dots i_n\rangle$. Все, что можно знать о физической системе, содержится в ее векторе состояния $|\psi\rangle$. Все, что можно сделать с системой, — это преобразовать ее начальный вектор состояния $|\psi_{\text{in}}\rangle$ в другой вектор: $|\psi_{\text{f}}\rangle$. Поэтому процесс вычислений на квантовом компьютере рассматривается как преобразование начального вектора состояния компьютера $|\psi_{\text{in}}\rangle$ в конечный вектор состояния $|\psi_{\text{f}}\rangle$ путем умножения вектора $|\psi_{\text{in}}\rangle$ на унитарную матрицу U и размерности $2^n \times 2^n$:

$$|\psi_{\text{f}}\rangle = \text{U}(2^n \times 2^n)|\psi_{\text{in}}\rangle \qquad (18)$$

Удобно полагать, что в начальном состоянии компьютера все его кубиты находятся в состоянии $|0\rangle$:

$$|\psi_{in}\rangle = |0_1 \dots 0_n\rangle.$$

Эту операцию называют инициализацией. Состояние $|0_1 \dots 0_n\rangle$. можно получить охлаждением кубитов до сверхнизких температур (милликельвин).

Алгоритм решения задачи заключен в матрице преобразования $\text{U}(2^n \times 2^n)$. Классическая информация о решении задачи содержится в конечном векторе состояния $|\psi_{\text{f}}\rangle$; она должна быть получена измерением кубитов.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.1. Идеальный квантовый компьютер

Для решения задачи на квантовом компьютере надо изготовить необходимое количество кубитов, инициализировать их, управлять их квантовой эволюцией, выполнить преобразование $\mathrm{U}|\psi_{\mathrm{in}}\rangle$ и измерить состояния кубитов, описываемых вектором $|\psi_{\mathrm{f}}\rangle = \mathrm{U}|\psi_{\mathrm{in}}\rangle$.

Сейчас рассмотрим вопрос о ресурсах квантового компьютера, дающих ему преимущество по сравнению с классическим компьютером.

Анализ ресурса квантового компьютера проведем исходя из уравнения (18) работы компьютера. Введем сначала более экономные обозначения вектора состояния $|\psi\rangle$. Базисное состояние $|i_1 \dots i_n\rangle$ представляет собой n-разрядное двоичное число $|x\rangle$ разряды которого совпадают с числами $i_1, \dots, i_n = \{0,1\}$. В этих обозначениях

$$|\psi\rangle = \sum_{x=0}^{2^n-1} a_x |x\rangle.$$

Суперпозиция $|\psi\rangle$ содержит 2^n слагаемых, представляющих собой разложение вектора $|\psi\rangle$ по базисным функциям $|x\rangle$, $0 \le x \le 2^n - 1$. Ограниченный физический ресурс, т.е. небольшое количество $n \simeq 10^3$ частиц (кубитов), создает экспоненциально большой $2^n = 2^{1000} \simeq 10^{300}$ математический информационный ресурс квантового компьютера!

Именно из этого обстоятельства вытекают основные преимущества квантового компьютера.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.1. Идеальный квантовый компьютер

Следствием принципа суперпозиции является 2^n - кратный квантовый параллелизм вычислений. Действительно, изменение состояния только одного кубита перестраивает всю суперпозицию. Поскольку набор базисных функций $|x\rangle$ постоянен, перестраиваются все 2^n проекций a_x вектора $|\psi\rangle$.

Сравним эти факты с возможностями регистра классического компьютера. Классический регистр из n битов может находиться только в одном из 2^n состояний, поскольку он не подчиняется принципу суперпозиции. Состояние классического регистра одномерно. Изменение состояния одного бита переводит регистр в другое одномерное (близкое по значению) состояние. **Ресурсы классического компьютера экспоненциально малы по сравнению с ресурсами квантового компьютера.**

Тема 3. Принципы построения и работы идеального квантового компьютера

3.2. Квантовый компьютер —цифровой компьютер с аналоговым управлением

Анализ уравнения $|\psi_f\rangle = \mathrm{U}|\psi_{\mathrm{in}}\rangle$ для квантового компьютера позволяет установить принципы работы и управления квантовым компьютером. Состояние $|\psi_{in}\rangle = |0_1 \dots 0_n\rangle$ не содержит никакой информации ни о задаче, ни о способах ее решения. Всю информацию о решаемой задаче и алгоритме ее решения содержит матрица преобразования U. Наконец, конечный вектор состояния

$$|\psi_f\rangle = \sum_{x=0}^{2^n-1} a_x^{(\mathrm{f})} |x\rangle$$

содержит информацию о решении задачи.

Получить эту информацию можно, измерив в базисе $|0\rangle$, $|1\rangle$ состояние каждого из n кубитов компьютера в состоянии $|\psi_f\rangle$. Выполнив измерение, мы получим любое из значений $0 \le x \le 2^n - 1$ с вероятностями $\left|a_x^{(\mathrm{f})}\right|^2$, как это следует из общих принципов квантовой физики.

Как разные числа x могут представлять решение задачи, если решение должно быть единственным? Действительно, это так; только одно значение $|s\rangle$ является правильным решением, остальные значения $|x\rangle \neq |s\rangle$ ошибочные. Чтобы идея квантового компьютера имела реальный смысл, квантовый алгоритм должен приводить к такому состоянию $|\psi_{\mathrm{f}}\rangle$, что вероятность найти правильное решение $p_s = |a_s|^2 \simeq 1$, тогда как сумма вероятностей всех ошибочных решений мала:

$\sum_{x \neq s} |a_s|^2 \ll 1$. Все придуманные к настоящему времени квантовые алгоритмы обладают описанным свойством. Итак, квантовый компьютер дает цифровое решение задачи s с определенной вероятностью, т.е. является цифровым вероятностным компьютером.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.2. Квантовый компьютер —цифровой компьютер с аналоговым управлением

Теперь выявим способ управления квантовым компьютером. В ходе квантовых вычислений происходит преобразование начального вектора состояния $|\psi_{\text{in}}\rangle = \sum_x a_x^{(\text{in})}$ в конечный вектор $|\psi_{\text{f}}\rangle = \sum_x a_x^{(\text{f})}|x\rangle$ через непрерывный ряд состояний. Базисный набор состояний $|x\rangle$ сохраняется неизменным. Динамика состояния компьютера передается изменениями во времени амплитуд $a_x(t)$ которые являются аналоговыми величинами, принимающими непрерывный ряд значений в интервале $0 \leq |a_x| \leq 1$. Управлять компьютером, — значит, управлять процессами $a_x(t)$), т.е. по способу управления квантовый компьютер является аналоговым компьютером.

Такое сочетание свойств — аналоговый способ управления, вероятностный характер представления цифрового решения — не присутствует ни в одном типе классических компьютеров. Квантовый компьютер выглядит минотавром или утконосом в мире компьютеров, сочетая несовместимые в классическом мире свойства аналоговых и цифровых классических компьютеров.

По современным оценкам параметры управляющих кубитами сигналов (импульсов) должны контролироваться с погрешностью 10^{-5} – 10^{-4}. Высокая точность операций необходима, чтобы справиться с проблемой декогерентизации квантовых состояний. Проблему декогерентизации мы рассмотрим в следующей главе.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.3. Классическая и квантовая информация в квантовой системе

Аналоговый характер квантовой информации имеет принципиальное значение для квантовой теории. Этим выражается тот факт, что множество квантовых состояний образует континуум: любые два состояния из этого континуума могут быть преобразованы друг в друга непрерывным образом посредством унитарного преобразования. Харди показал, что, приняв в системе аксиом теории вероятностей возможность непрерывного (continious) преобразования состояний друг в друга (вместо скачкообразного перехода в классической теории вероятностей), можно интерпретировать квантовую механику как квантовую теорию вероятностей.

Процессы квантовых вычислений протекают в пространстве аналоговых переменных, т.е. амплитуд a_x при базисных состояниях $|x\rangle$ системы.

Квантовая теория информации строится во многом по аналогии с теорией классической информации Шеннона: аналогично информационной энтропии Шеннона строится квантовая энтропия фон Неймана. Как энтропия Шеннона характеризует количество информации, содержащейся (в среднем) в одном сигнальном символе x, появляющемся с вероятностью $p(x)$, так и энтропия фон Неймана характеризует информацию в квантовых состояниях ρ_x, выступающих в качестве сигнальных символов и появляющихся с вероятностью $p(\rho_x)$.

Свойства энтропии фон Неймана отличаются от свойств энтропии Шеннона, если рассматривать квантовые состояния ρ_x со свойствами, отличными от свойств классических систем, такими как неполная различимость неортогональных состояний, запутанные (entangled) состояния квантовых систем.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.4. Как реализовать квантовый алгоритм

Управление работой квантового компьютера с n кубитами описывает преобразование $|\psi_{\mathrm{f}}\rangle = \mathrm{U}(2^n \times 2^n)|\psi_{\mathrm{in}}\rangle$, где $|\psi_{\mathrm{in}}\rangle$ и $|\psi_{\mathrm{f}}\rangle$ — векторы с 2^n компонентами. При значениях $n = 10^3$ умножение $\mathrm{U}|\psi_{\mathrm{in}}\rangle$ становится недоступным для самых быстрых (порядка 10^{12} операций в секунду) компьютеров. Еще более трудной представляется физическая реализация преобразования $|\psi_{in}\rangle \rightarrow |\psi_{f}\rangle$.

Путь к реализации квантовых алгоритмов обнаруживается, если рассмотреть возможность разложения матрицы $\mathrm{U}(2^n \times 2^n)$ в упорядоченное произведение матриц второго и четвертого порядков:

$$\mathrm{U}(2^n \times 2^n) = \prod_{i,j} \mathrm{U}_i(2 \times 2) \otimes \mathrm{U}_j(2^2 \times 2^2). \quad (22)$$

Матрица второго порядка $\mathrm{U} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

преобразует вектор $\begin{vmatrix} a \\ b \end{vmatrix}$

состояния одного кубита: $\begin{vmatrix} a' \\ b' \end{vmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{vmatrix} a \\ b \end{vmatrix}$,

т.е. каждая матрица $\mathrm{U}_i(2 \times 2)$ в разложении (22) описывает операцию на том или другом отдельном кубите компьютера.

Тема 3. Принципы построения и работы идеального квантового компьютера

3.4. Как реализовать квантовый алгоритм

Матрицы $U(2^2 \times 2^2)$ преобразуют векторы состояния пар кубитов:

$$|\psi_{in}\rangle = a_{00}|00\rangle + a_{10}|10\rangle + a_{01}|01\rangle + a_{11}|11\rangle \rightarrow |\psi_f\rangle = a'_{00}|00\rangle + a'_{10}|10\rangle + a'_{01}|01\rangle + a'_{11}|11\rangle \ . \quad (23)$$

числа сомножителей второго и четвертого порядков в разложении (22) определяют число однокубитовых и двухкубитовых операций, необходимых для реализации алгоритма. Чтобы **алгоритм был эффективным, необходимо, чтобы полное число операций было полиномиальным** от числа ”задействованных” кубитов в компьютере: $N = P(n)$. **Если число операций возрастает экспоненциально с размером задачи (числом задействованных в решении задачи кубитов компьютера), то алгоритм относится к классу неэффективных.**

QUBIT.jpg

Тема 3. Принципы построения и работы идеального квантового компьютера

Темы для самостоятельного изучения (темы рефератов):

3.5. Универсальные наборы элементарных операций
3.6. Осцилляция Раби между состояниями кубита и однокубитовые операции
3.7. Кубит, управляемый рамановскими переходами А-типа