Введение в квантовые вычисления
23 ноября 2005

Ю. Лифшиц*

7 декабря 2005 г.

План лекции

1. Роль квантовых вычислений
2. Квантовые биты и квантовые схемы
3. Телепортация и суперплотное кодирование

1 Роль квантовых вычислений

1.1 Мотивация для квантовых вычислений

Всем нужны быстрые алгоритмы. Но разве можно, например, полный перебор сделать быстрее, чем за n? Оказывается, можно. Для этого надо сменить модель вычислений на квантовую. Квантовая модель вычислений позволяет:

- Разложение чисел на множители за n^2.
- Дискретный алгоритм нахождения логарифма за полиномиальное время.
- Полный перебор за $\sqrt{n}$.
- Стойкая криптосистема — если подслушать квантовый бит, то он изменится.

1.2 Модели вычислений

Каждый алгоритм работает в какой-нибудь модели вычислений. Есть стандартные модели вычислений:

*Законспектировал Т. Магомедов.

- Машина Тьюринга.
- Логическая схема.
- RAM-машина.

Эти модели полиномиально эквивалентны, то есть задачи, которые эффективно решаются в одной модели, эффективно решаются и в другой.

Есть много альтернативных моделей вычислений, например:

- Real-RAM и Real-Тьюринг.
- Оптический компьютер.
- Квантовые вычисления.
- Аналоговые вычисления.
- Бильярдный компьютер.

Real-RAM и Real-Тьюринг — это аналоги RAM-машины и машины Тьюринга, работающие не с дискретными, а с вещественными данными. В оптическом компьютере вычисления проводятся лучами света, проходящими через линзы и отражающимися от зеркал. В модели аналоговых вычислений мы проводим опыты над физической системой, а потом меряем ее параметры, такие, как давление, масса, объем и так далее. В этой модели входные данные — начальное состояние физической системы, алгоритм — набор опытов над ней, а выходные данные — параметры системы после опытов. Бильярдный компьютер — это бильярдный стол с расставленными на нем перегородками, киями и шарами. Алгоритм задается положением перегородок и киев. Входные данные задаются положением шаров. При запуске каждый кий ударяет шарик, находящийся перед ним (если такой есть). Выходные данные в этой системе — попадание или непопадание шариков в лузы.

Подробнее остановимся на модели квантовых вычислений.

1.3 Идея квантовых вычислений

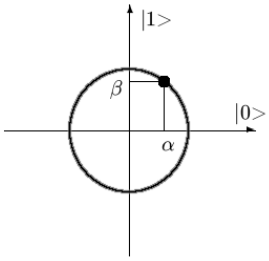
Как решить задачу в квантовой модели? Кодируем начальные данные в системе из нескольких квантов. Потом применяем алгоритм — систему физических преобразований. Проводим измерения и интерпретируем их как выходные данные.

2 Квантовые биты и квантовые схемы

2.1 Квантовый бит

В квантовой модели вычислений носителями информации служат квантовые биты. Квантовый бит имеет 2 базисных состояния, которые обозначаются $|0>$ и $|1>$. Он может быть и в смешанном состоянии $\alpha|0>+\beta|1>$, где

$\alpha, \beta \in \mathbf{C}$ и $|\alpha|^2+|\beta|^2 = 1$. Считается, что домножение α и β на $e^{i\varphi}$ состояния не меняет. Наш квантовый бит трудно представить. Пусть есть двухмерное комплексное пространство. Уравнение $|\alpha|^2 + |\beta|^2 = 1$ задает в нем сферу. Итак, все значения квантовых битов должны лежать на этой сфере. Так как домножение на $e^{i\varphi}$ не меняет состояние квантового бита, то каждое состояние – колечко на сфере. Стоит заметить, что сфера в двухмерном комплексном пространстве – это четырехмерная сфера. Если Вам трудно представить колечко на четырехмерной сфере, представьте себе случай, когда α и β – вещественные числа. Тогда состояние квантового бита – это одна точка на окружности единичного радиуса.



Как ни странно, законам модели квантового бита подчиняются некоторые физические эффекты, такие как:

- Электрон возбужден / не возбужден.
- Фотон поляризован / не поляризован.
- Спин атомного ядра.
- Фотон в ловушке / нет фотона.

Используя эти физические эффекты, конструируют квантовые компьютеры. Физики уже умеют передавать квантовый бит на 100 километров и создавать системы из семи квантовых битов. Почему всего семь? Проблема в том, что квантовые биты должны быть изолированы, а этого очень трудно добиться.

Состояние системы из двух квантовых битов описывается относительно четырех базисных: |00>, |01>, |10>, |11>.

$$\alpha_{00}|00> +\alpha_{01}|01> +\alpha_{10}|10> +\alpha_{11}|11>$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2$$

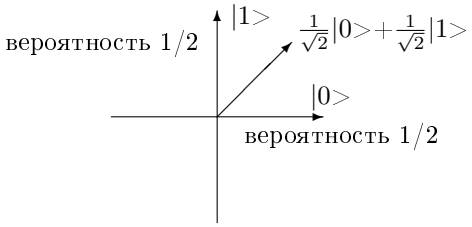
Домножение на $e^{i\varphi}$ всех коэффициентов не меняет состояния системы из двух квантовых битов.

2.2 Измерение квантовых битов

Пусть есть квантовый бит $|\psi>=\alpha|0>+\beta|1>$. В нем хранится вещественная информация, но по техническим причинам мы не можем получить ее. При измерении в стандартном базисе с вероятностью $|\alpha|^2$ получим 0, с вероятностью $|\beta|^2$ получим 1. При этом квантовый бит перейдет в состояние $|0>$ или $|1>$ соответственно.

Да, квантовые биты изменяются при измерении. И этого не обойти. Как, например, измерить плоскость поляризации фотона? Пропустить его через поляризатор. Фотон при этом либо не пройдет через поляризатор, либо его плоскость поляризации станет такой же, как у поляризатора.

При измерении в базисе $\phi, \phi^\perp$ с вероятностью $<\psi|\phi>$ [1] получим $|\phi>$ и квантовый бит перейдет в состояние $|\phi>$, вероятностью $<\psi|\phi^\perp>$ получим $|\phi^\perp>$ и квантовый бит перейдет в состояние $|\phi^\perp>$.



Один раз измерив квантовый бит, мы получим всего один бит информации, несмотря на их емкость. Положение усугубляется тем, что квантовые биты нельзя копировать. С измерением системы квантовых битов все еще хуже. Но мы можем померять только некоторые биты.

2.3 Частичные измерения

Разобраться в том, как измерить только некоторые квантовые биты в системе, проще всего на простом примере. Рассмотрим состояние системы φ из двух квантовых бит:

$$\varphi = \frac{3}{5}|00> + \frac{2}{5}|01> + \frac{2}{5}|10> + \frac{2\sqrt{2}}{5}|11>$$

Сумма квадратов коэффициентов, как и должно быть, равна единице. Давайте измерим второй квантовый бит. С какой вероятностью мы получим в результате замеров единицу?

Второй квантовый бит не ноль во втором и четвертом слагаемом. Вероятность того, что мы замерим единицу, равна сумме квадратов коэффициентов при этих слагаемых:

$$p_1 = \left(\frac{2}{5}\right)^2 + \left(\frac{2\sqrt{2}}{5}\right)^2 = \frac{12}{25}$$

[1] Под этим обозначением понимается проекция ψ на ϕ, возведенная в квадрат.

В какое состояние придет система, если мы замерим во втором бите единицу? Понятно, что первое и третье слагаемые исчезнут, так как в них второй бит ноль. Но просто так убирать их нельзя, хотя бы потому, что сумма квадратов коэффициентов перестанет быть равной единице. Надо вычислить такие новые коэффициенты при оставшихся втором и четвертом слагаемых, которые соотносились бы как старые и сумма их квадратов была равной единице. В нашем случае это будут коэффициенты $\frac{1}{\sqrt{3}}$ и $\frac{\sqrt{2}}{\sqrt{3}}$. Таким образом, состояние системы после измерения единицы во втором квантовом бите будет такое:

$$\varphi = \frac{1}{\sqrt{3}}|01> + \frac{\sqrt{2}}{\sqrt{3}}|11>$$

2.4 Квантовые схемы

Квантовая схема – это последовательность физических преобразований из конечного набора базисных элементарных преобразований – гейтов. На вход квантовая схема получает квантовые биты. Результат ее работы вероятностный. Но не всегда нас устроит вероятное решение задачи. Так как физики умеют стирать значения квантовых битов и выставлять 0 или 1, в этом случае мы можем прогнать квантовую схему много раз на одинаковых входных данных.

Физически мы можем реализовать только линейные, сохраняющие постоянной сумму квадратов коэффициентов (унитарные) преобразования над малым количеством квантовых битов. Из этого следует, что любое преобразование однозначно задается значениями на базисных состояниях и преобразование над k квантовыми битами можно записать в виде матрицы $2^k \times 2^k$.

2.5 Гейт Адамара

Гейт Адамара задается матрицей:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Как получить значение квантового бита после действия на него гейта Адамара? Записать его как вектор в базисе $|0>$, $|1>$ и умножить на него H. Вычислим то, во что преобразуется базисное состояние $|0>$ под действием гейта Адамара:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Гейт Адамара можно однозначно задать и значениями на базисных состояниях, одно из которых мы только что вычислили:

$$|0> \rightarrow \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$$

$$|1> \rightarrow \frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>$$

Если гейт Адамара применить два раза, то получится исходное состояние. Если представлять состояние квантового бита как точку на окружности, то преобразование Адамара – это симметричное относительно луча под углом $\pi/8$ отражение точки.

2.6 Гейт CNOT

Гейт CNOT (Controlled NOT) действует на систему из двух квантовых битов следующим образом:

$$|00> \rightarrow |00>$$
$$|01> \rightarrow |01>$$
$$|10> \rightarrow |11>$$
$$|11> \rightarrow |10>$$

Если первый квантовый бит единица, то меняется второй квантовый бит. Существует также гейт Toffoli, или двойной CNOT. Он действует на систему из трех квантовых битов следующим образом: если хотя бы один из первых двух квантовых битов не единица, то третий бит не изменяют; в противном случае – изменяют.

С помощью схем из гейтов Адамара, CNOT и Toffoli можно сколь угодно точно приблизить любое унитарное преобразование.

3 Телепортация и суперплотное кодирование

3.1 Суперплотное кодирование

Алиса хочет передать Бобу два классических бита в одном квантовом. У них есть по квантовому биту из пары $\frac{1}{\sqrt{2}}|00>+\frac{1}{\sqrt{2}}|11>$. Алиса применяет одно из четырех преобразований к своему квантовому биту и посылает его Бобу. Боб, проведя ряд действий над парой битов, узнает, какое из четырех преобразований применила Алиса. Исходное состояние системы такое:

$$\frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$$

Алиса может применить такие преобразования к своему квантовому биту:

1. Ничего не делать
2. Поменять знак коэффициента у $|1>$
3. Переставить $|0>$ и $|1>$
4. Поменять знак коэффициента у $|1>$ и переставить $|0>$ и $|1>$

Этим преобразованиям соответствуют такие пары квантовых битов:

1. $\frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$
2. $\frac{1}{\sqrt{2}}|00> - \frac{1}{\sqrt{2}}|11>$
3. $\frac{1}{\sqrt{2}}|10> + \frac{1}{\sqrt{2}}|01>$
4. $\frac{1}{\sqrt{2}}|10> - \frac{1}{\sqrt{2}}|01>$

3.2 Квантовая телепортация

Алиса хочет передать Бобу неизвестное состояние $|\varphi>$=a$|0>$+b$|1>$. У них есть по квантовому биту из пары $\frac{1}{\sqrt{2}}|00>+\frac{1}{\sqrt{2}}|11>$. Идея состоит в том, что Алиса перемешивает неизвестный квантовый бит со своим представителем пары, проведет измерения, пошлет результаты Бобу. Боб проделает вспомогательное преобразование и получит $|\varphi>$.

Перемешиваем неизвестный квантовый бит с нашими двумя – ставим его на первое место:

$$\frac{a}{\sqrt{2}}|000> + \frac{a}{\sqrt{2}}|011> + \frac{b}{\sqrt{2}}|100> + \frac{b}{\sqrt{2}}|111>$$

Применяем CNOT к первому и второму квантовым битам:

$$\frac{a}{\sqrt{2}}|000> + \frac{a}{\sqrt{2}}|011> + \frac{b}{\sqrt{2}}|110> + \frac{b}{\sqrt{2}}|101>$$

После измерения среднего бита получаем либо $a|00> + b|11>$, либо $a|01> + b|10>$. Средний бит находится у Алисы. Результат его измерения она пошлет Бобу. Если средний квантовый бит равен $|1>$, Боб инвертирует свой бит. Таким образом, всегда получим:

$$a|00> + b|11>$$

Алиса применяет гейт Адамара к первому биту (это тот самый неизвестный бит).

$$\frac{a}{\sqrt{2}}|00> + \frac{a}{\sqrt{2}}|10> - \frac{b}{\sqrt{2}}|11> + \frac{b}{\sqrt{2}}|01>$$

Теперь Алиса измеряет средний бит. Получается либо $a|0> + b|1>$, либо $a|0> - b|1>$. Если результат измерений был $|1>$, то Боб меняет знак при $|1>$ и таким образом всегда получает $a|0> + b|1>$. Квантовый бит от Алисы "телепортировался"к Бобу. Но для того, чтобы воссоздать у себя неизвестный квантовый бит, ему нужно было получить два обычных бита с результатами измерений от Алисы.