Введение в квантовые вычисления

Лекция N 9 курса “Современные задачи теоретической информатики” — СПбГУ ИТМО

Юрий Лифшиц
yura@logic.pdmi.ras.ru

Лаборатория мат. логики ПОМИ РАН

Осень’2005

... Мы не можем применить здесь здравый смысл, мы можем только стремиться понять внутреннюю логику этого безумия, которая наверняка есть...

Александр Шень

План лекции

1. **Роль квантовых вычислений**
2. **Квантовые биты и квантовые схемы**
   - Квантовый бит
   - Квантовые схемы
3. **Телепортация и суперплотное кодирование**
   - Суперплотное кодирование
   - Телепортация
4. **Задача**

План лекции

Мотивация для квантовых вычислений

Эффективные алгоритмы

- Разложение чисел на множители за n^2
- Алгоритм для дискретного логарифма
- Полный перебор за $\sqrt{n}$

Мотивация для квантовых вычислений

Эффективные алгоритмы

Разложение чисел на множители за n^2

Алгоритм для дискретного логарифма

Полный перебор за $\sqrt{n}$

Криптография

Стойкая криптосистема без предположений
о вычислительной сложности каких-либо задач

Мотивация для квантовых вычислений

Эффективные алгоритмы

- Разложение чисел на множители за n^2
- Алгоритм для дискретного логарифма
- Полный перебор за $\sqrt{n}$

Криптография

- Стойкая криптосистема без предположений о вычислительной сложности каких-либо задач

Кванты как модель вычисления

- Сравнить с другими моделями
- Переоценить пределы вычислимых задач

Модели вычислений

Стандартные модели

Модели вычислений

Стандартные модели

- Машина Тьюринга
- Логическая схема
- RAM-машина

Модели вычислений

Стандартные модели

- Машина Тьюринга
- Логическая схема
- RAM-машина

Альтернативные модели

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

Идея квантовых вычислений

1. Есть задача: вычислить функцию $f(x)$

Идея квантовых вычислений

1. Есть задача: вычислить функцию $f(x)$
2. Создаем систему из нескольких квантов “кодирующих” x

Идея квантовых вычислений

1. Есть задача: вычислить функцию $f(x)$
2. Создаем систему из нескольких квантов “кодирующих” x
3. Строим систему физических преобразований (аналог алгоритма)

Идея квантовых вычислений

1. Есть задача: вычислить функцию $f(x)$
2. Создаем систему из нескольких квантов “кодирующих” x
3. Строим систему физических преобразований (аналог алгоритма)
4. Проводим измерения (получаем классическую информацию)

Идея квантовых вычислений

1. Есть задача: вычислить функцию $f(x)$
2. Создаем систему из нескольких квантов “кодирующих” x
3. Строим систему физических преобразований (аналог алгоритма)
4. Проводим измерения (получаем классическую информацию)
5. Интерпретируем результат

План лекции

Квантовый бит

Два базисных состояния:

Обозначение $|0\rangle$ и $|1\rangle$

Квантовый бит

Два базисных состояния:

Обозначение $|0\rangle$ и $|1\rangle$

Смешанные состояния:

$\alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$ и $|\alpha|^2 + |\beta|^2 = 1$

Домножение всех коэффициентов на $e^{i\varphi}$

не меняет состояние

Квантовый бит

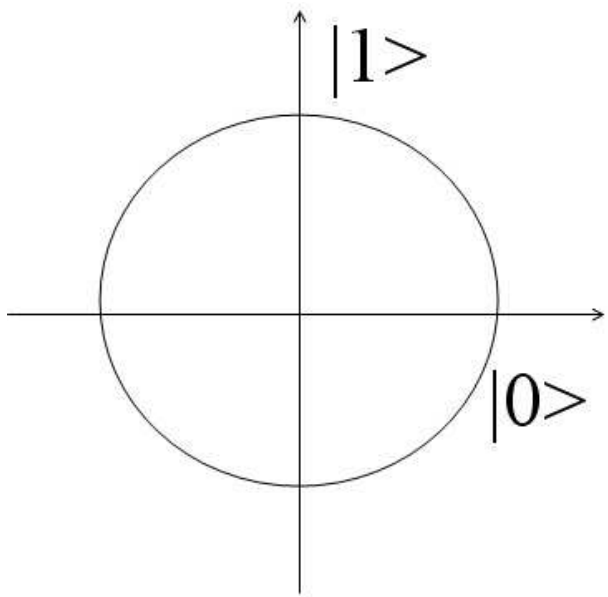
Два базисных состояния:

Обозначение $|0\rangle$ и $|1\rangle$

Смешанные состояния:

$\alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$ и $|\alpha|^2 + |\beta|^2 = 1$

Домножение всех коэффициентов на $e^{i\varphi}$ не меняет состояние



Физические реализации

Законам модели квантового бита подчиняются разные физические эффекты:

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

Физические реализации

Законам модели квантового бита подчиняются разные физические эффекты:

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

Успехи физиков:

- Передача квантового бита на 100 км.
- Квантовый компьютер на 7 q-битах

Два q-бита

Состояние системы из двух q-битов

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

Два q-бита

Состояние системы из двух q-битов

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

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Два q-бита

Состояние системы из двух q-битов

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

$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

Домножение на $e^{i\varphi}$ не меняет состояние

Измерение

Есть q-бит в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Измерение

Есть q-бит в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Измерение в стандартном базисе:

С вероятностью $|\alpha|^2$ получим “0”, с вероятностью $|\beta|^2$ — “1”

Сам q-бит перейдет в соответствующее состояние

Измерение

Есть q-бит в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Измерение в стандартном базисе:

С вероятностью $|\alpha|^2$ получим “0”, с вероятностью $|\beta|^2$ — “1”

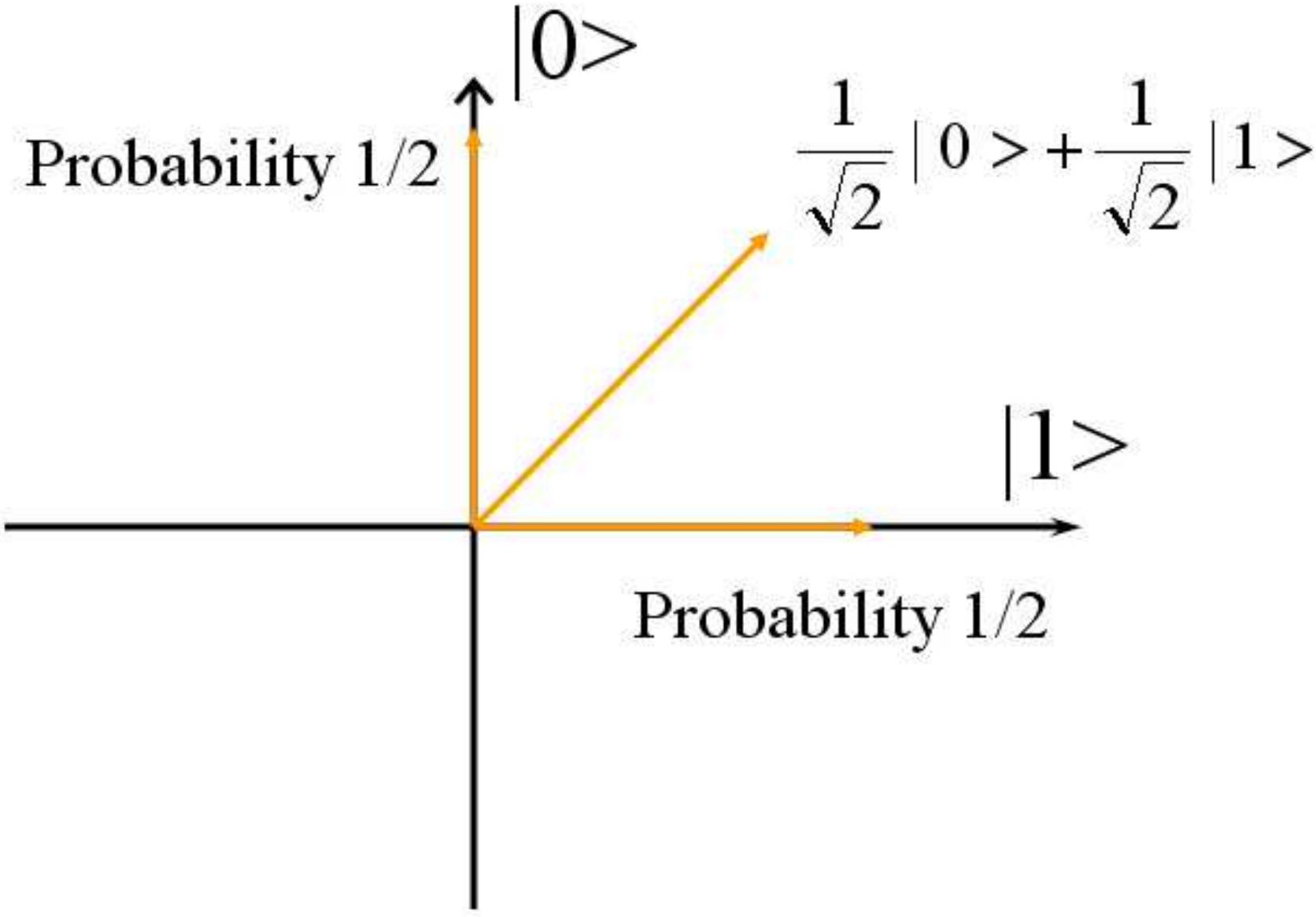
Сам q-бит перейдет в соответствующее состояние

Измерение в базисе $\phi, \phi^\top$:

С вероятностью $\langle\psi|\phi\rangle$ получим $|\phi\rangle$

С вероятностью $\langle\psi|\phi^\top\rangle$ получим $|\phi^\top\rangle$

Сам q-бит перейдет в $|\phi\rangle$ или $|\phi^\top\rangle$


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

Частичные измерения

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

Result 0

Result 1

$$\frac{1}{\sqrt{2}}|\,00> + \frac{1}{\sqrt{2}}|\,01>$$

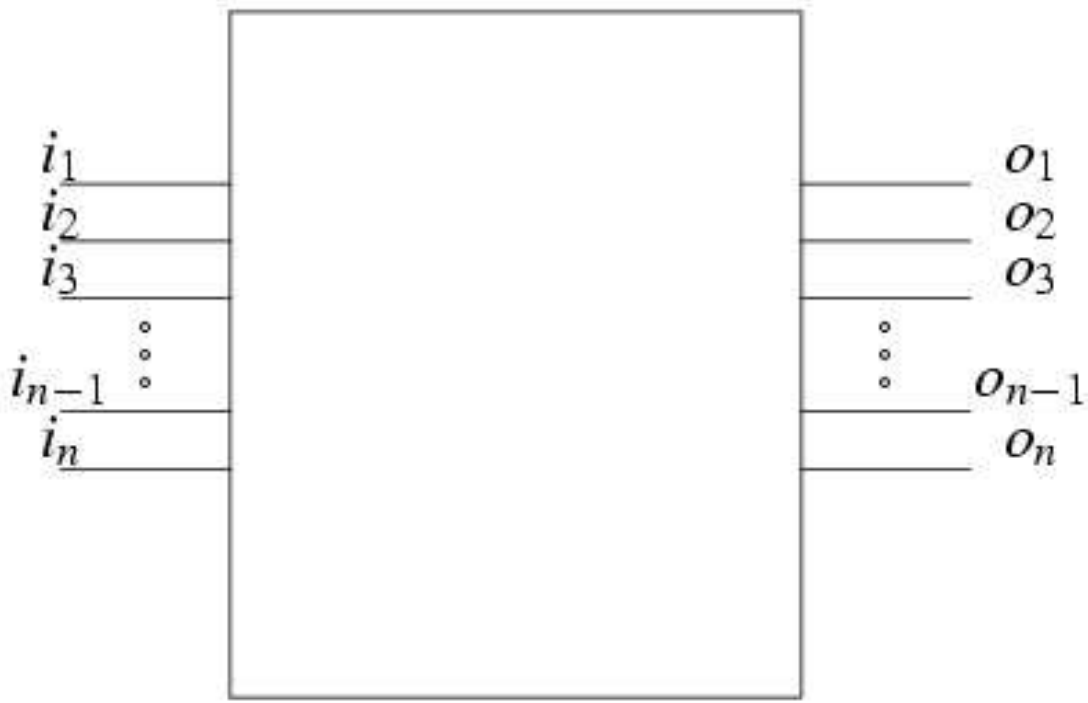
$$|\,10>$$

Квантовая схема

Квантовая схема: последовательность физических преобразований из конечного набора (базисных) гейтов.

Квантовая схема

Квантовая схема: последовательность физических преобразований из конечного набора (базисных) гейтов.



Что могут физики?

Физически реализуемые преобразования:

- Над малым количеством q-битов
- Только линейные преобразования
- Только преобразования, сохраняющие длину (унитарные)

Что могут физики?

Физически реализуемые преобразования:

- Над малым количеством q-битов
- Только линейные преобразования
- Только преобразования, сохраняющие длину (унитарные)

Следствие:

Любое преобразование однозначно задается значениями на базисных состояниях

Преобразование над k q-битами можно записать в виде матрицы

Что могут физики?

Физически реализуемые преобразования:

- Над малым количеством q-битов
- Только линейные преобразования
- Только преобразования, сохраняющие длину (унитарные)

Следствие:

Любое преобразование однозначно задается значениями на базисных состояниях

Преобразование над k q-битами можно записать в виде матрицы $2^k \times 2^k$

Гейт Адамара

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

Гейт Адамара

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

Действие на базисных состояниях:

$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Гейт Адамара

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

Действие на базисных состояниях:

$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Геометрическая интерпретация:

Отражение относительно луча под углом $\pi/8$

Гейт CNOT

$$CNOT = \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases}$$

Факт: с помощью схем из гейтов Адамара, CNOT и Toffoli (двойное коннтролированное отрицание) можно сколь угодно точно приблизить любое унитарное преобразование.

План лекции

Суперплотное кодирование

Постановка задачи

Алиса хочет передать Бобу 2 классических бита в одном q-бит

У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Суперплотное кодирование

Постановка задачи

Алиса хочет передать Бобу 2 классических бита в одном q-бит
У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Идея

Алиса применяет одно из четырех преобразований к своему q-биту и посылает его Бобу
Боб проводит ряд действий над парой кубитов и узнает, какое преобразование сделала Алиса

Суперплотное кодирование

Постановка задачи

Алиса хочет передать Бобу 2 классических бита в одном q-бит
У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Идея

Алиса применяет одно из четырех преобразований к своему q-биту и посылает его Бобу
Боб проводит ряд действий над парой кубитов и узнает, какое преобразование сделала Алиса

Исходное состояние системы

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

Алгоритм кодирования

Исходное состояние:

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

Алгоритм кодирования

Исходное состояние:

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

Четыре преобразования Алисы:

Ничего не делать

Поменять знак коэффициента у $|1\rangle$

“$1 \leftrightarrow 2$”

Поменять знак коэффициента у $|1\rangle$ и “$1 \leftrightarrow 2$”

Алгоритм кодирования

Исходное состояние:

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

Четыре преобразования Алисы:

Ничего не делать

Поменять знак коэффициента у $|1\rangle$

“1$\leftrightarrow$2”

Поменять знак коэффициента у $|1\rangle$ и “1$\leftrightarrow$2”

Состояния пары q-битов:

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

$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$

$\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle$

$\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|01\rangle$

Квантовая телепортация

Постановка задачи

Хотим передать неизвестное состояние $|\psi\rangle = a|0\rangle + b|1\rangle$ от Алисы к Бобу

У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Квантовая телепортация

Постановка задачи

Хотим передать неизвестное состояние $|\psi\rangle = a|0\rangle + b|1\rangle$ от Алисы к Бобу

У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Идея

Алиса перемешает неизвестный q-бит со своим представителем пары

Алиса проведет измерения и перешлет результаты Бобу

Боб проделает вспомогательное преобразование и получит $|\psi\rangle$

Квантовая телепортация

Постановка задачи

Хотим передать неизвестное состояние $|\psi\rangle = a|0\rangle + b|1\rangle$ от Алисы к Бобу

У них есть по биту из пары $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Идея

Алиса перемешает неизвестный q-бит со своим представителем пары

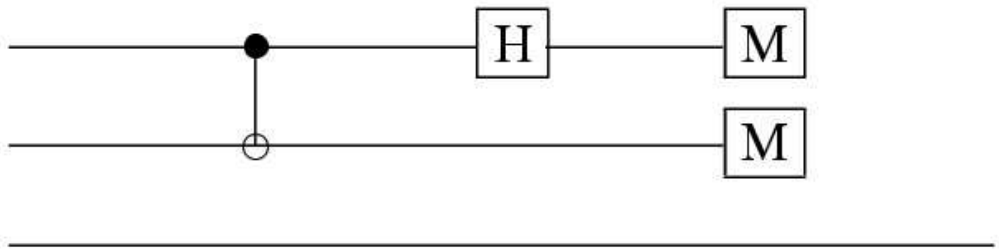
Алиса проведет измерения и перешлет результаты Бобу

Боб проделает вспомогательное преобразование и получит $|\psi\rangle$

Исходное состояние системы

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

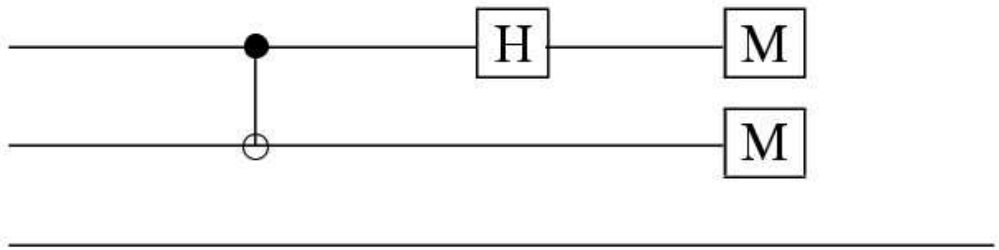
Алгоритм телепортации



Исходное состояние:

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

Алгоритм телепортации



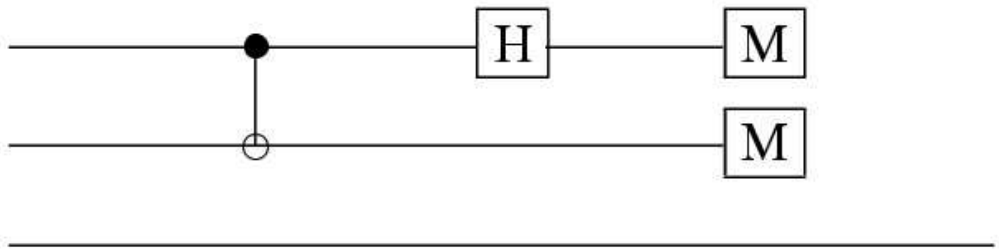
Исходное состояние:

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

После CNOT:

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

Алгоритм телепортации



Исходное состояние:

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

После CNOT:

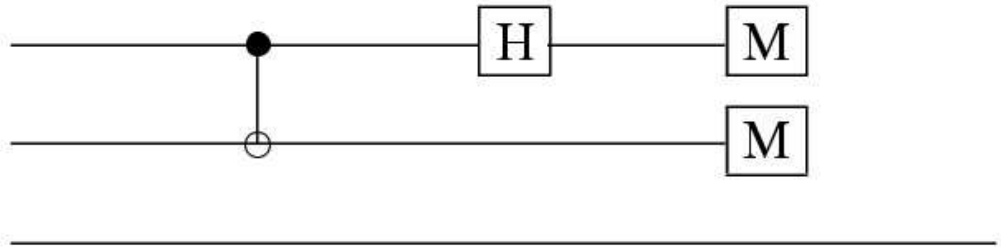
$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle$

После измерения среднего бита:

Или $a|00\rangle + b|11\rangle$

Или $a|01\rangle + b|10\rangle$

Алгоритм телепортации



Исходное состояние:

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

После CNOT:

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

После измерения среднего бита:

Или $a|00\rangle + b|11\rangle$

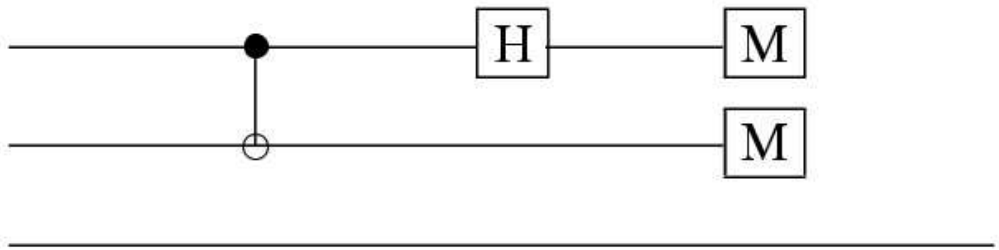
Или $a|01\rangle + b|10\rangle$

Если средний бит равен 1, Боб применяет “0↔1”:

Или $a|00\rangle + b|11\rangle$

Или $a|00\rangle + b|11\rangle$

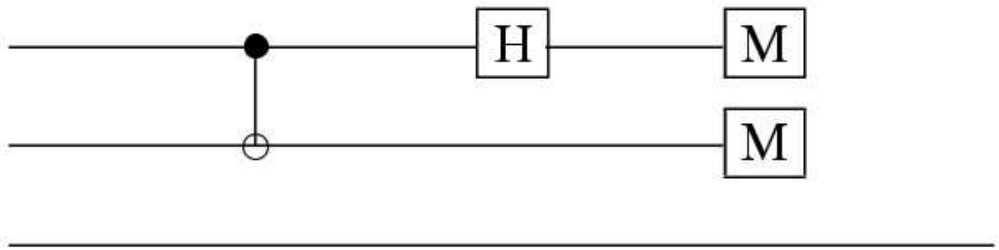
Алгоритм телепортации II



Продолжаем:

$a|00\rangle + b|11\rangle$

Алгоритм телепортации II



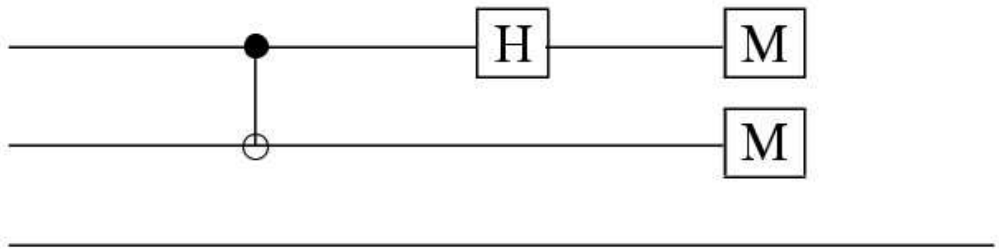
Продолжаем:

$a|00\rangle + b|11\rangle$

Алиса применила H к первому биту:

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

Алгоритм телепортации II



Продолжаем:

$a|00\rangle + b|11\rangle$

Алиса применила H к первому биту:

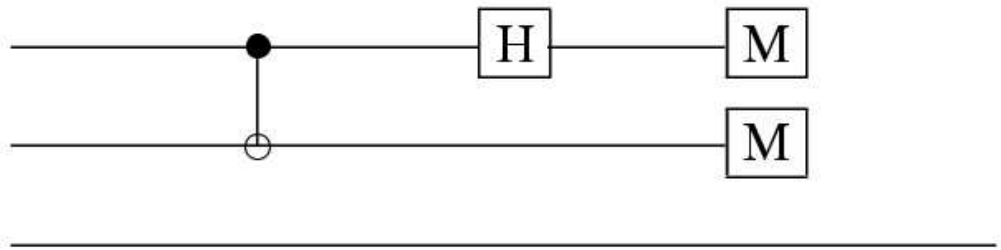
$\frac{a}{\sqrt{2}}|00\rangle + \frac{a}{\sqrt{2}}|10\rangle - \frac{b}{\sqrt{2}}|11\rangle + \frac{b}{\sqrt{2}}|01\rangle$

После измерения верхнего бита:

Или $a|0\rangle + b|1\rangle$

Или $a|0\rangle - b|1\rangle$

Алгоритм телепортации II



Продолжаем:

$a|00\rangle + b|11\rangle$

Алиса применила H к первому биту:

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

После измерения верхнего бита:

Или $a|0\rangle + b|1\rangle$

Или $a|0\rangle - b|1\rangle$

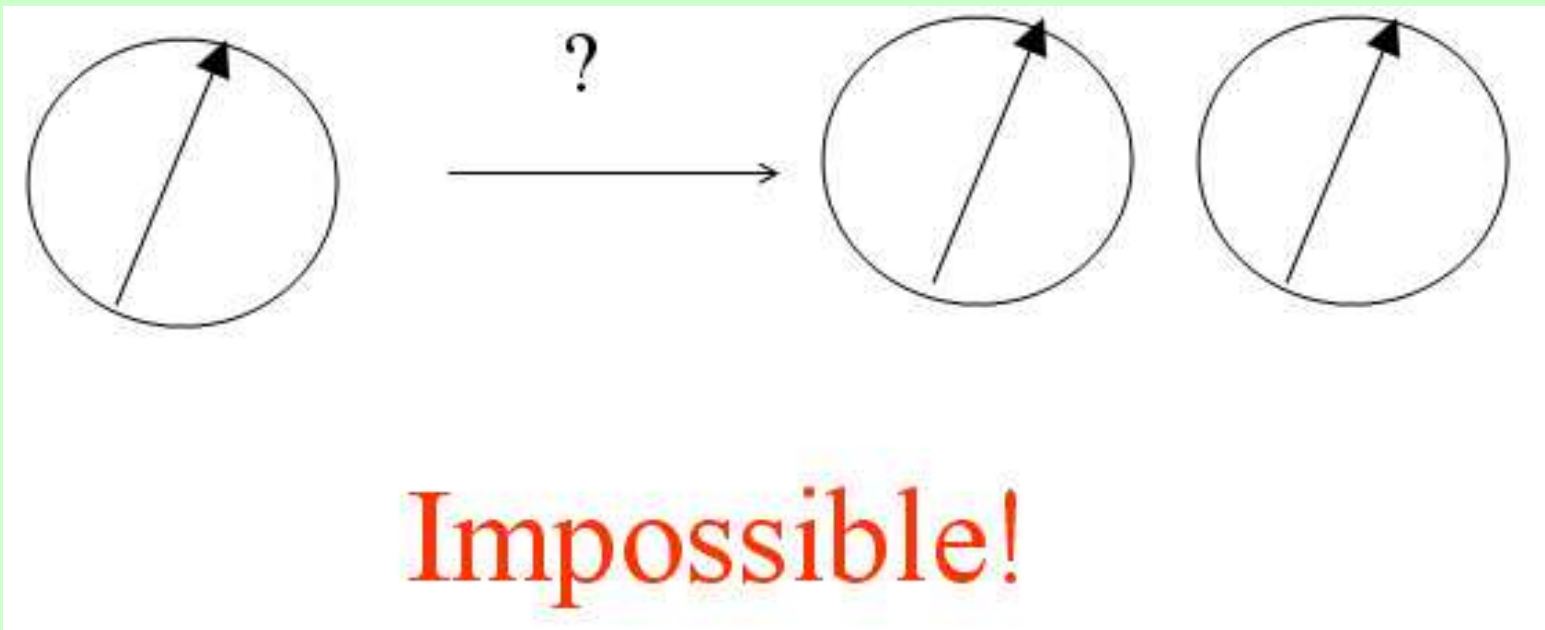
Если нужно, Боб меняет знак у $|1\rangle$:

$a|0\rangle + b|1\rangle$

План лекции

Задача

Опираясь на слайд “Что могут физики?” докажите, что невозможно реализовать преобразование, получающее на вход пару битов в состояниях $|\phi\rangle$ и $|0\rangle$ и выдающее $|\phi\rangle$ и $|\phi\rangle$. Этот факт известен как No-Cloning Theorem



Последний слайд

Если не запомните ничего другого:

- Квантовые вычисления основаны на проведении преобразований над системой из нескольких q-битов и последующих измерениях

Последний слайд

Если не запомните ничего другого:

- Квантовые вычисления основаны на проведении преобразований над системой из нескольких q-битов и последующих измерениях
- Передав один квантовый бит можно передать два классических

Последний слайд

Если не запомните ничего другого:

- Квантовые вычисления основаны на проведении преобразований над системой из нескольких q-битов и последующих измерениях
- Передав один квантовый бит можно передать два классических
- Передав два классических бита можно передать квантовое состояние

Последний слайд

Если не запомните ничего другого:

- Квантовые вычисления основаны на проведении преобразований над системой из нескольких q-битов и последующих измерениях
- Передав один квантовый бит можно передать два классических
- Передав два классических бита можно передать квантовое состояние

Последний слайд

Если не запомните ничего другого:

- Квантовые вычисления основаны на проведении преобразований над системой из нескольких q-битов и последующих измерениях
- Передав один квантовый бит можно передать два классических
- Передав два классических бита можно передать квантовое состояние

Вопросы?