Алгоритм Шора

Лекция N 10 курса "Современные задачи теоретической информатики" — СПбГУ ИТМО

Юрий Лифшиц
yura@logic.pdmi.ras.ru

Лаборатория мат. логики ПОМИ РАН

Осень'2005

План лекции

1. **Подготовка**
   - Разложение чисел на множители
   - Квантовые вычисления
   - Эмуляция классических вычислений
2. **Алгоритм Саймона**
   - Квантовый параллелизм
   - Задача Саймона
3. **Алгоритм Шора**
4. Задача

План лекции

Разложение на множители

Вычислительная задача

Вход: Составное число N в двоичной записи

Выход: Числа p, q, такие что $N = pq$

Типичный размер — N порядка 2^{2000}

Разложение на множители

Вычислительная задача

Вход: Составное число N в двоичной записи

Выход: Числа p, q, такие что $N = pq$

Типичный размер — N порядка 2^{2000}

Мотивация

Неизвестен полиномиальный классический алгоритм

Решение этой задачи позволит взломать RSA

Одна из самых знаменитых алгоритмических проблем

Разложение на множители

Вычислительная задача

Вход: Составное число N в двоичной записи

Выход: Числа p, q, такие что $N = pq$

Типичный размер — N порядка 2^{2000}

Мотивация

Неизвестен полиномиальный классический алгоритм

Решение этой задачи позволит взломать RSA

Одна из самых знаменитых алгоритмических проблем

Классические и квантовые алгоритмы

Лучший из известных классических алгоритмов $2^{\sqrt[3]{n}}$

Сегодня: квантовый алгоритм $O(n^2)$ [Питер Шор, 1994]

Квантовый бит

Напомните определение

Квантовый бит

Напомните определение

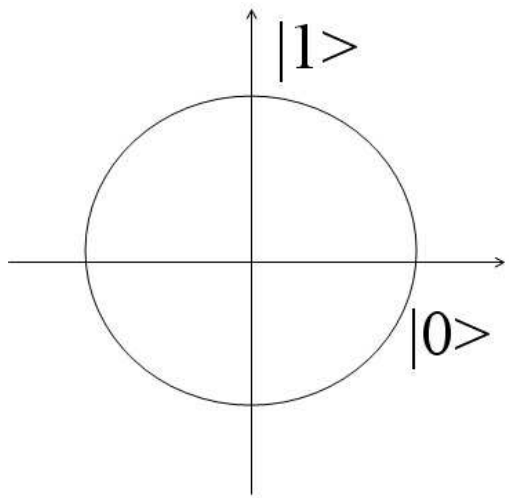
Два базисных состояния:

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



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 $|\phi^\top\rangle$

Частичные измерения

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

Result 0

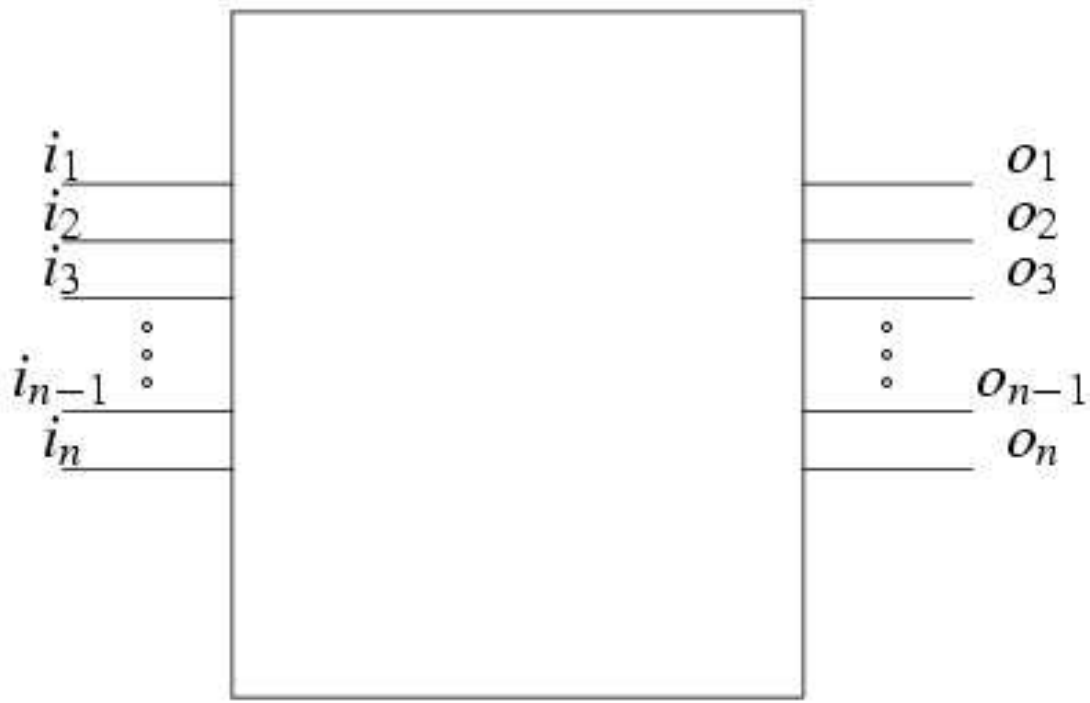
Result 1

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

$$|\,10>$$

Квантовая схема

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



Гейт Адамара

Напомните гейт Адамара

Гейт Адамара

Напомните гейт Адамара

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

Действие на базисных состояниях:

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

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

Эмуляция классических вычислений

Теорема

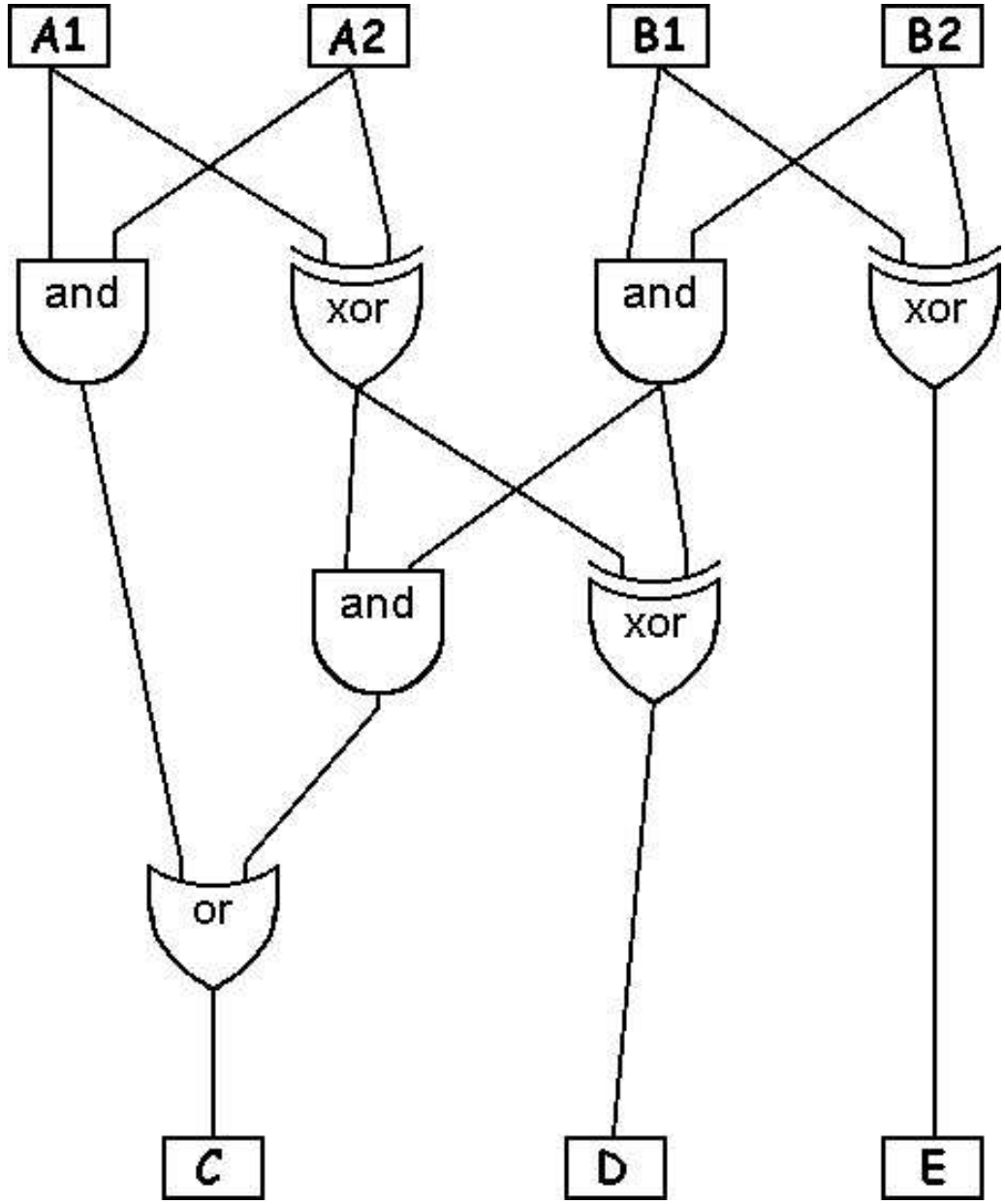
Для каждой классической логической схемы из AND и NOT можно построить квантовую схему, вычисляющую "почти" ту же функцию.

Эмуляция классических вычислений

Теорема

Для каждой классической логической схемы из AND и NOT можно построить квантовую схему, вычисляющую "почти" ту же функцию.

Что такое логическая схема?


A1
A2
B1
B2
and
xor
and
xor
and
xor
or
C
D
E

Обратимость

Факт: Квантовые вычисления обратимы

Другими словами: Нельзя реализовать необратимые преобразования

Обратимость

Факт: Квантовые вычисления обратимы
Другими словами: Нельзя реализовать необратимые преобразования

Следствие: Любое преобразование U инъективно

Обратимость

Факт: Квантовые вычисления обратимы
Другими словами: Нельзя реализовать необратимые преобразования

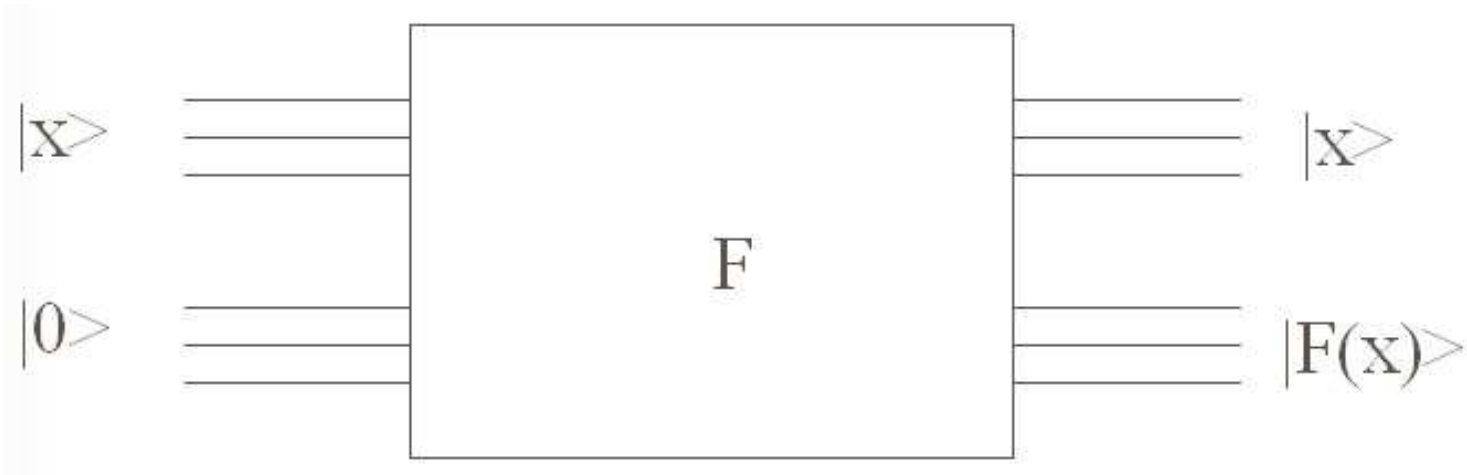
Следствие: Любое преобразование U инъективно

Доказательство.

Пусть $U|x\rangle = |z\rangle = U|y\rangle$, где $x \neq y$
Тогда $U|x - y\rangle = 0$ (по линейности)
Противоречие с унитарностью (сохранением длины)! $\square$

Выход из ситуации

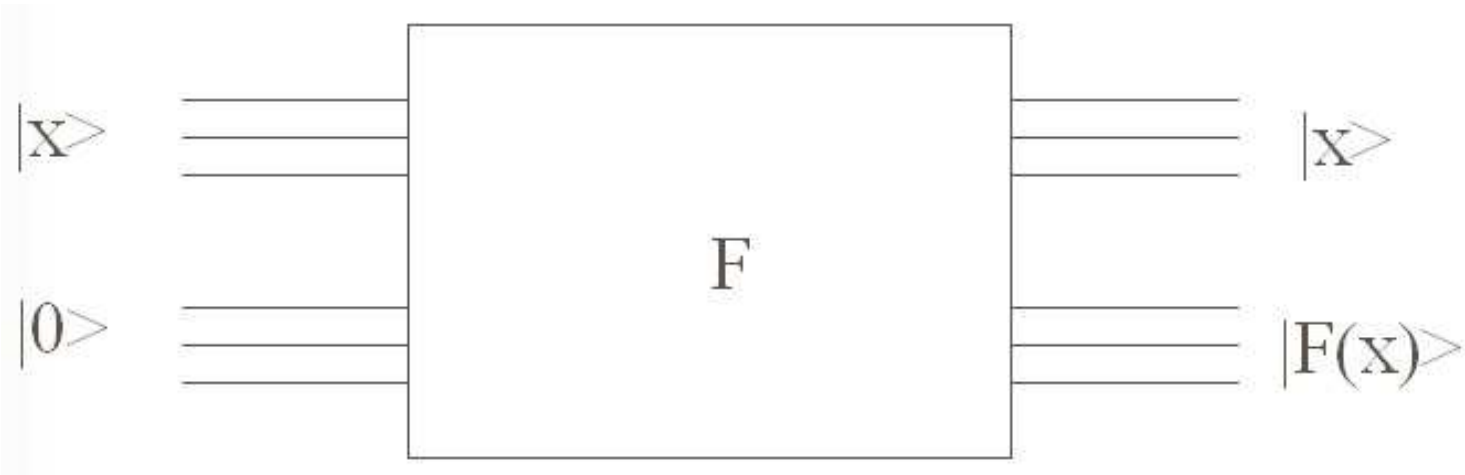
Будем использовать вспомогательные биты:



План лекции

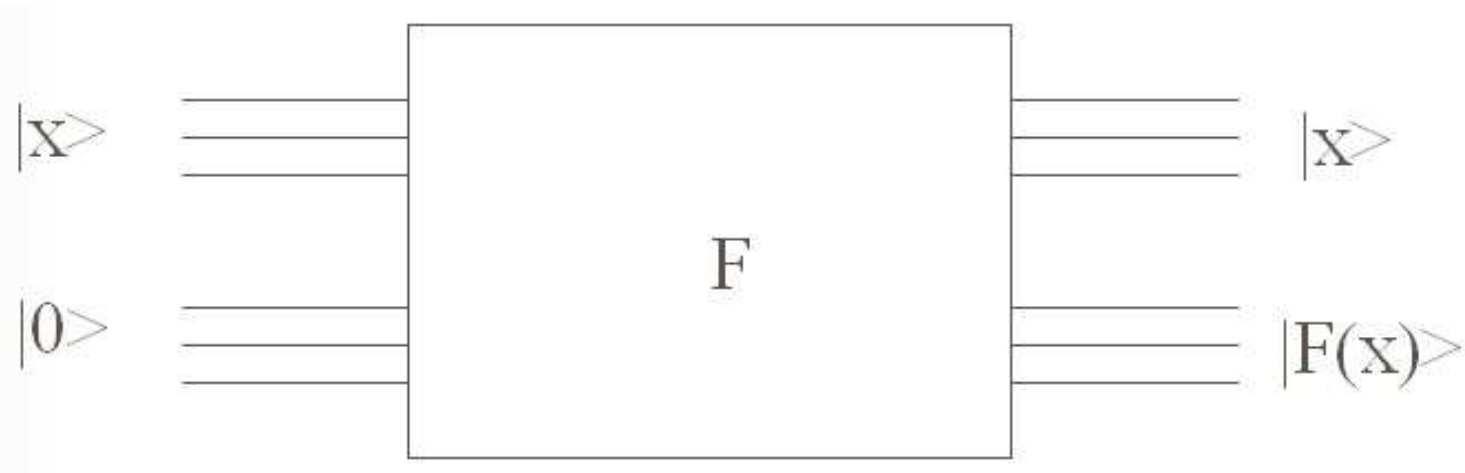
Ключевая идея

Квантовый параллелизм



Ключевая идея

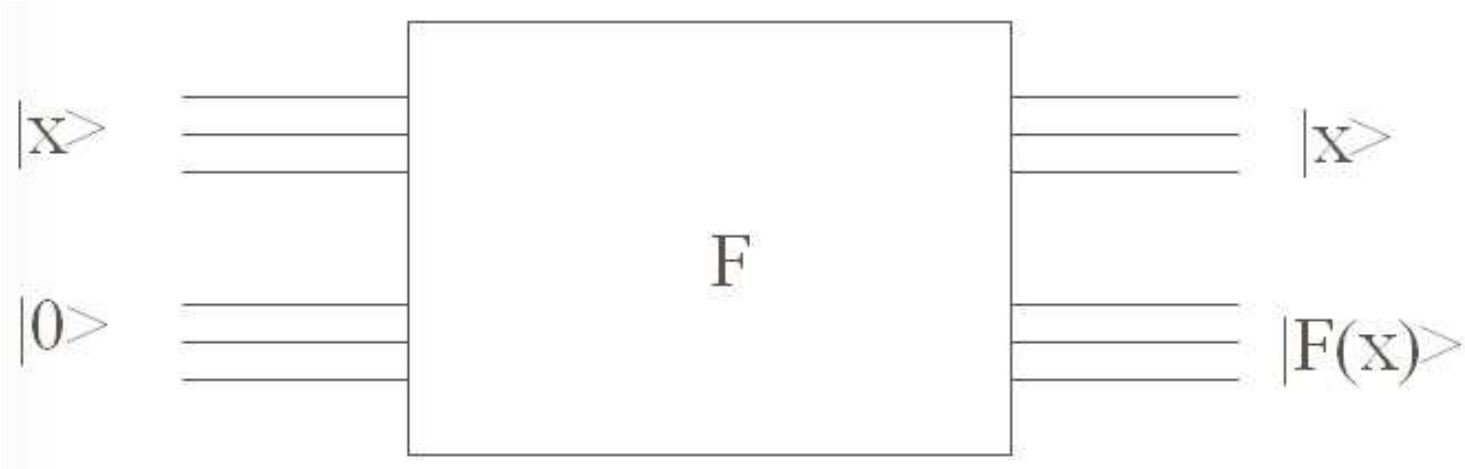
Квантовый параллелизм



$$\sum_x |x\rangle|0\rangle \quad \rightarrow \quad \sum_x |x\rangle|f(x)\rangle$$

Ключевая идея

Квантовый параллелизм



$$\sum_x |x\rangle|0\rangle \quad \rightarrow \quad \sum_x |x\rangle|f(x)\rangle$$

Одновременное вычисление f на многих входах!

Изучаем параллелизм

$$\sum_x |x\rangle|0\rangle \quad \rightarrow \quad \sum_x |x\rangle|f(x)\rangle$$

Что получим при измерении?

Изучаем параллелизм

$$\sum_x |x\rangle|0\rangle \quad \rightarrow \quad \sum_x |x\rangle|f(x)\rangle$$

Что получим при измерении?

Какую-то конкретную пару $x, f(x)$

Изучаем параллелизм

$$\sum_x |x\rangle|0\rangle \quad \rightarrow \quad \sum_x |x\rangle|f(x)\rangle$$

Что получим при измерении?

Какую-то конкретную пару $x, f(x)$

Идеологическая задача: получить результат, характеризующий все множество значений $f(\cdot)$

Задача Саймона

Дана функция F в виде (квантовой) схемы.
Известно, что есть такое y, что $F(x) = F(x + y)$
Здесь “+” — это побитовый XOR
Нужно найти y

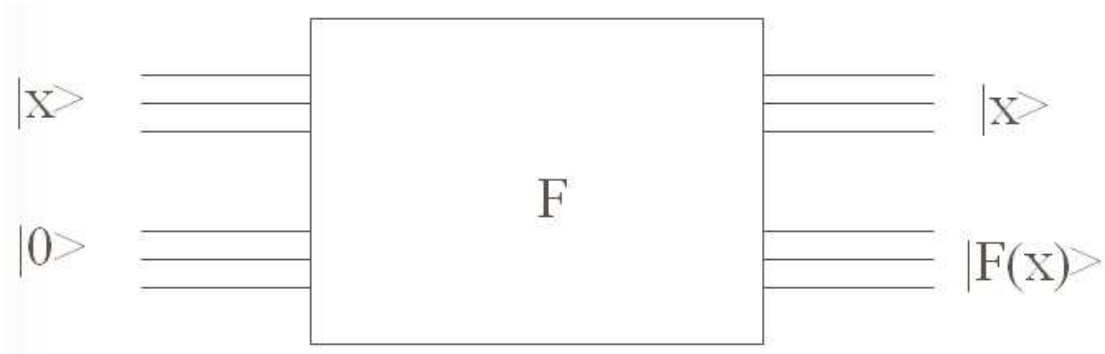
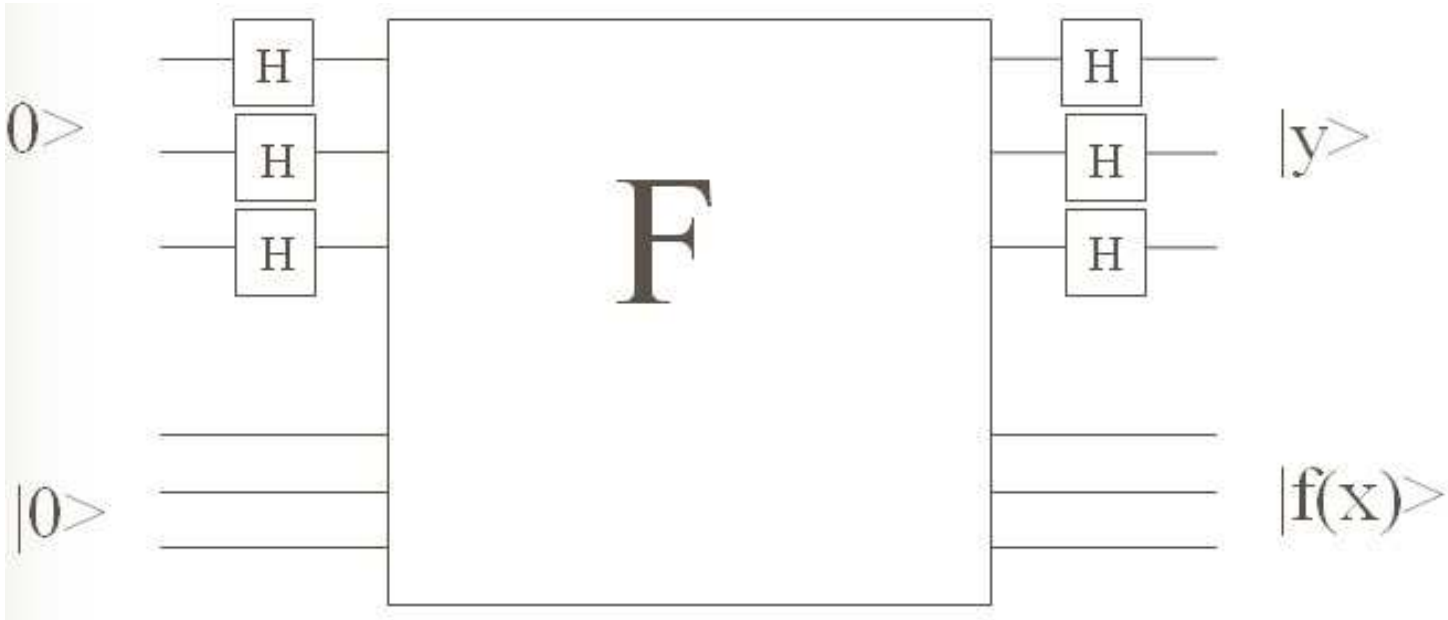


Схема Саймона

Решение, предложенное Саймоном [1994]:



Саймон по шагам I

Преобразование Адамара

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

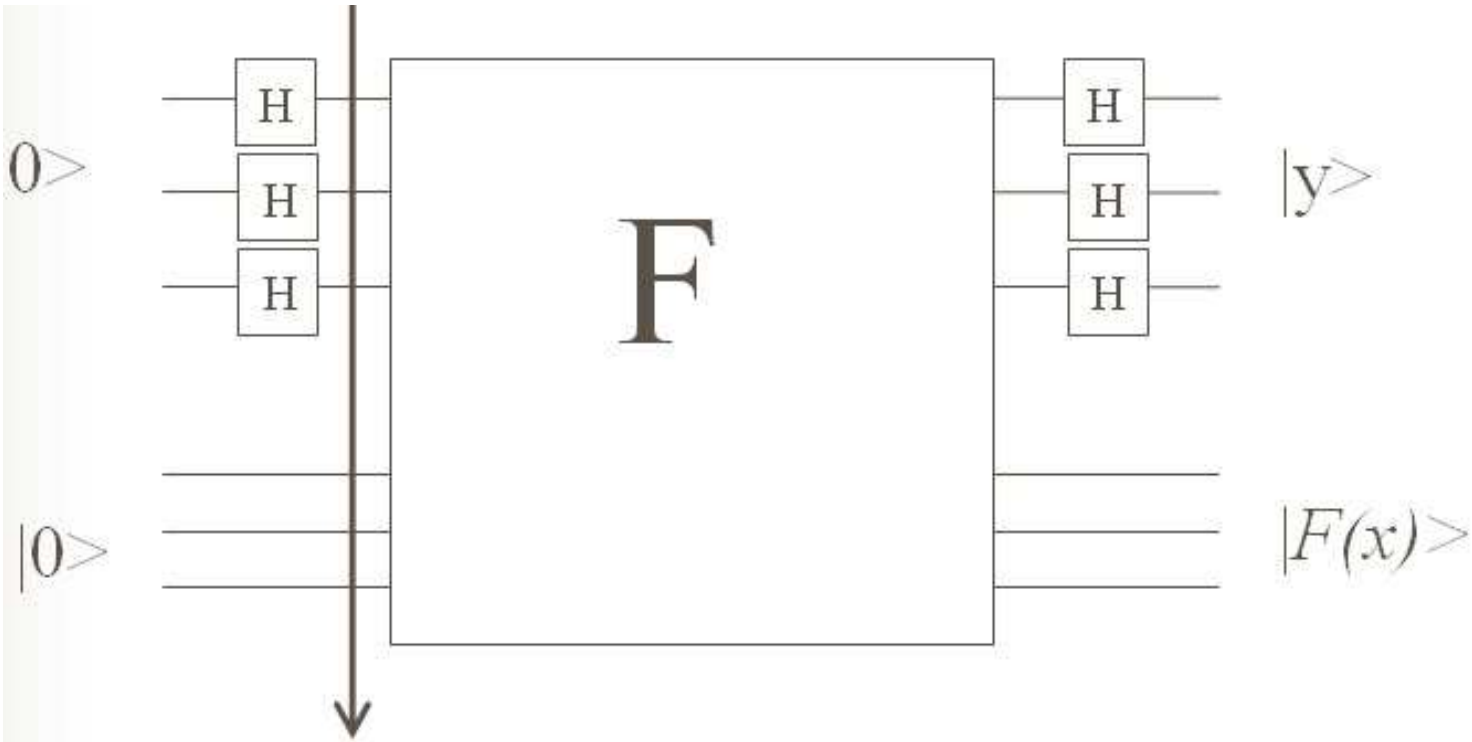
Преобразование Адамара

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

А на n кубитах:

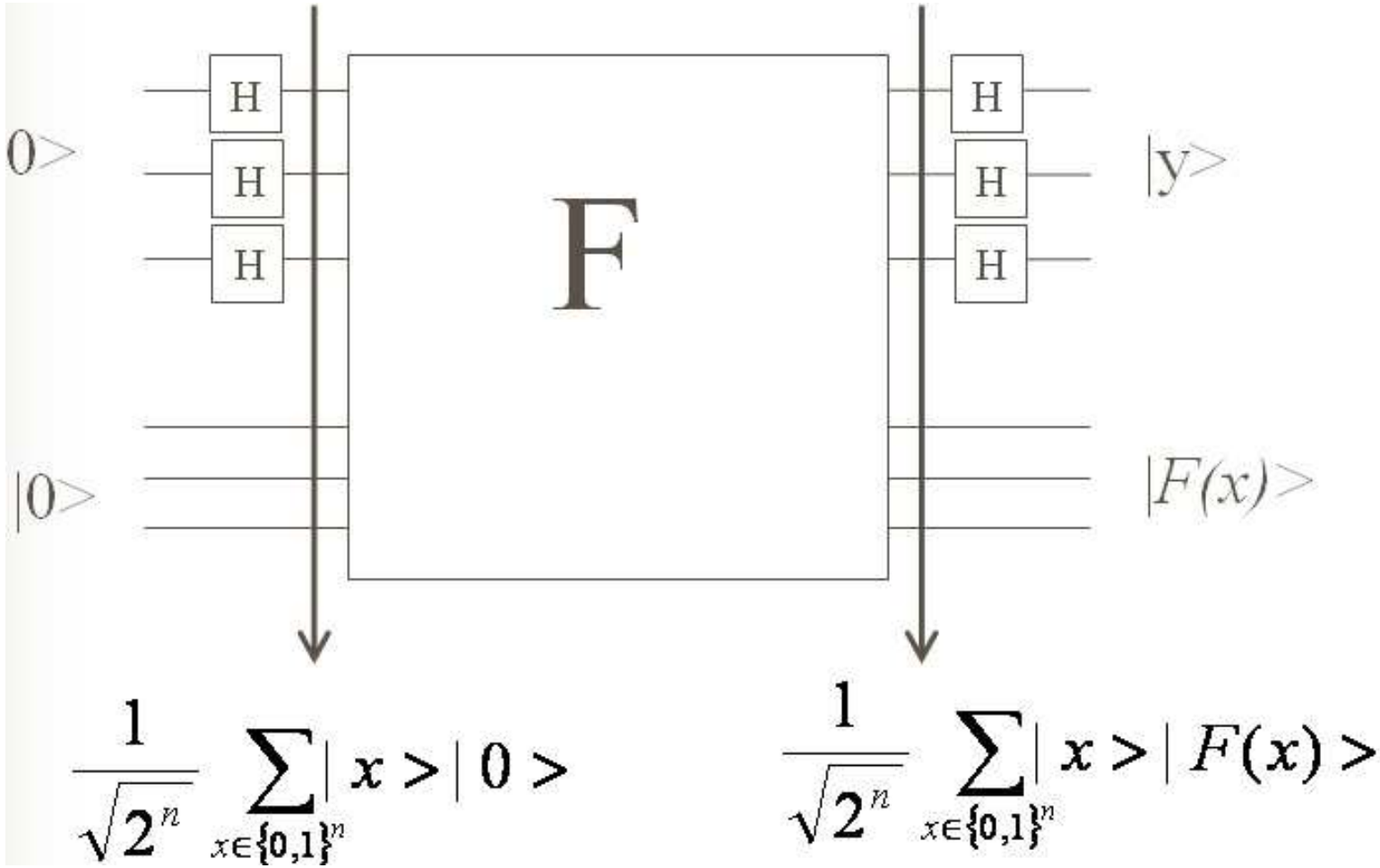
$$|0^n\rangle \to (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)^n = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

Саймон по шагам II



$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$$

Саймон по шагам II



$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle \qquad \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |F(x)\rangle$$

Саймон по шагам III

Измерим биты, содержащие $F(x)$

Получим некоторое значение $|z\rangle$

Состояние верхних битов перейдет в $\sum_{F(x)=z} |x\rangle$

Саймон по шагам III

Измерим биты, содержащие $F(x)$

Получим некоторое значение $|z\rangle$

Состояние верхних битов перейдет в $\sum_{F(x)=z} |x\rangle$

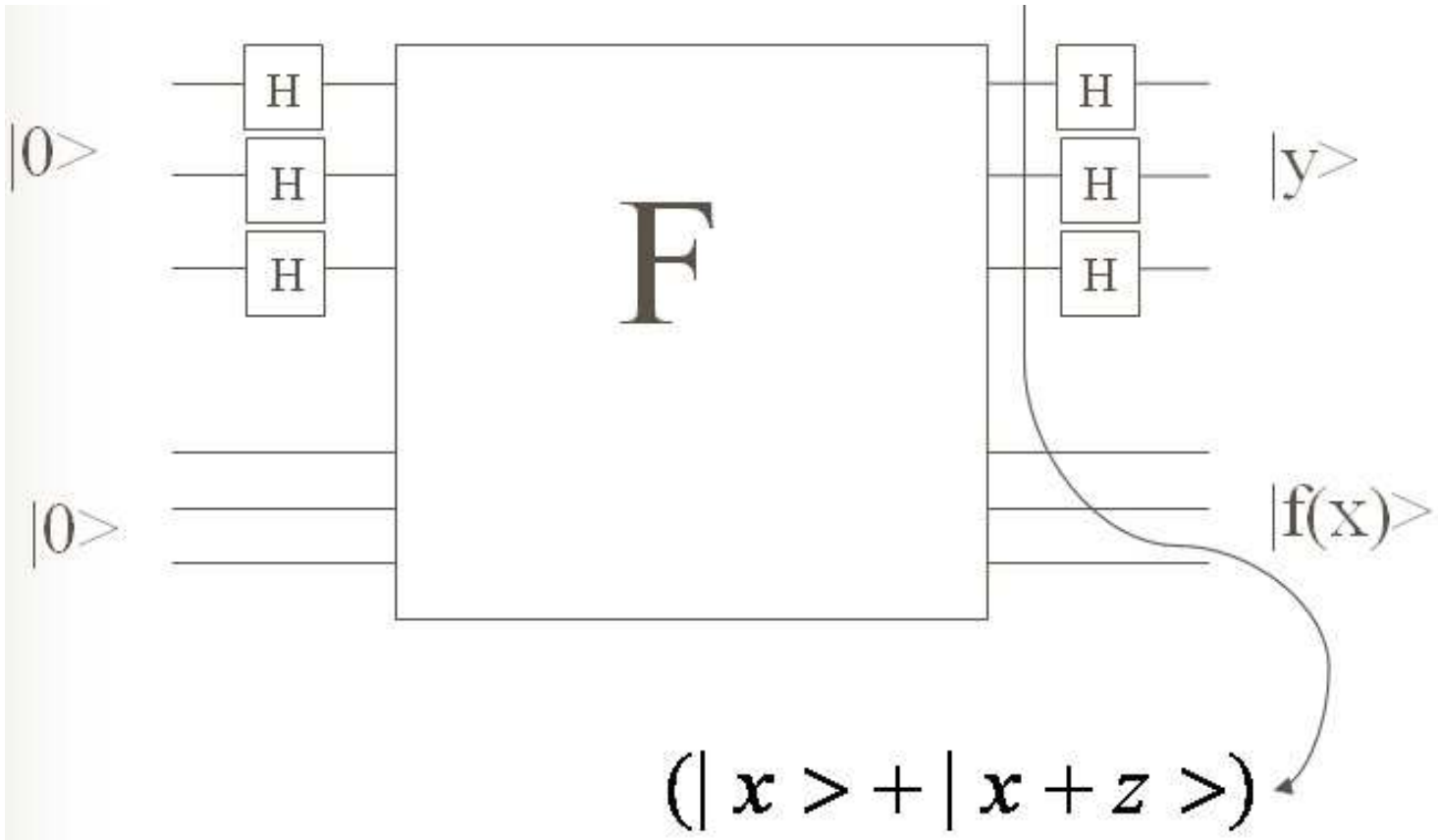
В нашем случае мы получим:

$|x\rangle|z\rangle + |x+y\rangle|z\rangle$

Как “вытащить” y?

Применим к верхним битам гейты Адамара

Саймон по шагам IV



Саймон по шагам V

Преобразование Адамара

$$|x\rangle \to \frac{1}{\sqrt{2}}|0\rangle + (-1)^x \frac{1}{\sqrt{2}}|1\rangle$$

Саймон по шагам V

Преобразование Адамара

$$|x\rangle \to \frac{1}{\sqrt{2}}|0\rangle + (-1)^x \frac{1}{\sqrt{2}}|1\rangle$$

Для n переменных:

$$|x_1 \dots x_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i} |u_1 \dots u_n\rangle$$

Саймон по шагам V

Преобразование Адамара

$$|x\rangle \to \frac{1}{\sqrt{2}}|0\rangle + (-1)^x \frac{1}{\sqrt{2}}|1\rangle$$

Для n переменных:

$$|x_1 \dots x_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i} |u_1 \dots u_n\rangle$$

$$|x_1 \dots x_n + y_1 \dots y_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i + y_i u_i} |u_1 \dots u_n\rangle$$

Саймон по шагам V

Преобразование Адамара

$$|x\rangle \to \frac{1}{\sqrt{2}}|0\rangle + (-1)^x \frac{1}{\sqrt{2}}|1\rangle$$

Для n переменных:

$$|x_1 \dots x_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i} |u_1 \dots u_n\rangle$$

$$|x_1 \dots x_n + y_1 \dots y_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i + y_i u_i} |u_1 \dots u_n\rangle$$

Знаки совпадают в точности для тех $|u\rangle$, для которых $z \cdot u = 0$.

Саймон по шагам V

Преобразование Адамара

$$|x\rangle \to \frac{1}{\sqrt{2}}|0\rangle + (-1)^x \frac{1}{\sqrt{2}}|1\rangle$$

Для n переменных:

$$|x_1 \dots x_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i} |u_1 \dots u_n\rangle$$

$$|x_1 \dots x_n + y_1 \dots y_n\rangle \to \frac{1}{\sqrt{2^n}} \sum_{u_1 \dots u_n} (-1)^{\sum x_i u_i + y_i u_i} |u_1 \dots u_n\rangle$$

Знаки совпадают в точности для тех $|u\rangle$, для которых $z \cdot u = 0$.

Измерив биты получим один такой вектор u

Повторив много раз сможем восстановить y!

План лекции

Алгоритм Шора

Основные шаги

1. Выбрать случайный остаток a по модулю N
2. Проверить $\text{НОД}(a, N) = 1$
3. Найти порядок r остатка a по модулю N
4. Если r четен, вычислить $\text{НОД}(a^{r/2} - 1, N)$

Алгоритм Шора

Основные шаги

1. Выбрать случайный остаток a по модулю N
2. Проверить $\text{НОД}(a, N) = 1$
3. Найти порядок r остатка a по модулю N
4. Если r четен, вычислить $\text{НОД}(a^{r/2} - 1, N)$

Анализ алгоритма: с большой вероятностью полученное на четвертом шаге число будет нетривиальным делителем N
Трудный шаг: найти порядок a по модулю N

Порядок по модулю

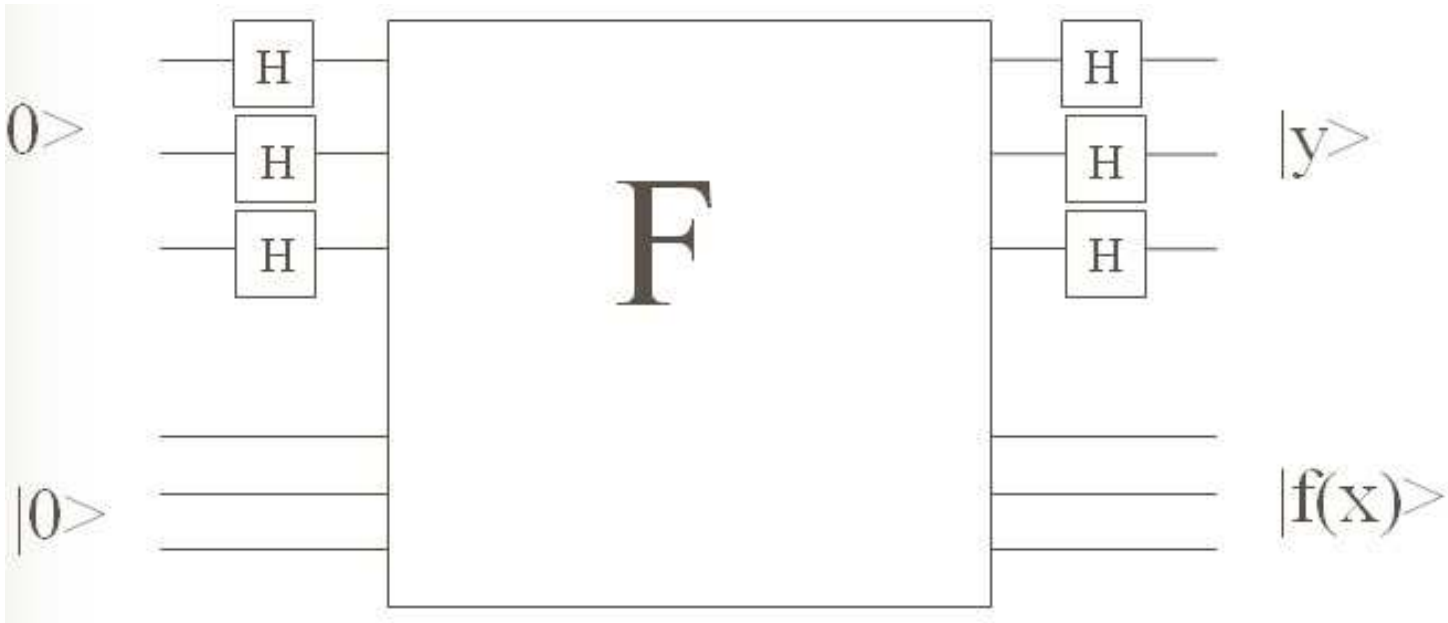
Определение: миниамальное r такое, что $a^r \equiv 1 \mod N$ называется порядком a по модулю N

Порядок по модулю

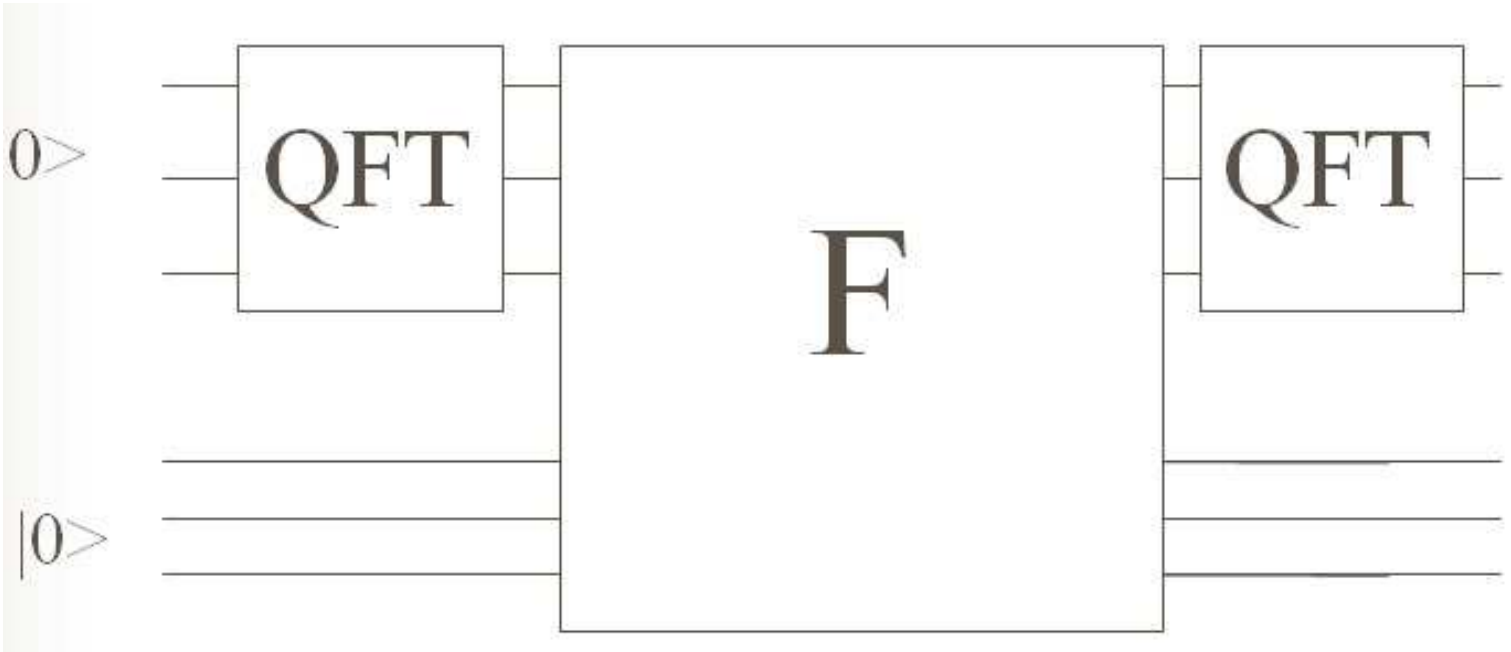
Определение: миниамальное r такое, что $a^r \equiv 1 \mod N$ называется порядком a по модулю N

Порядок r является периодом функции $f(x) = a^x \mod N$.

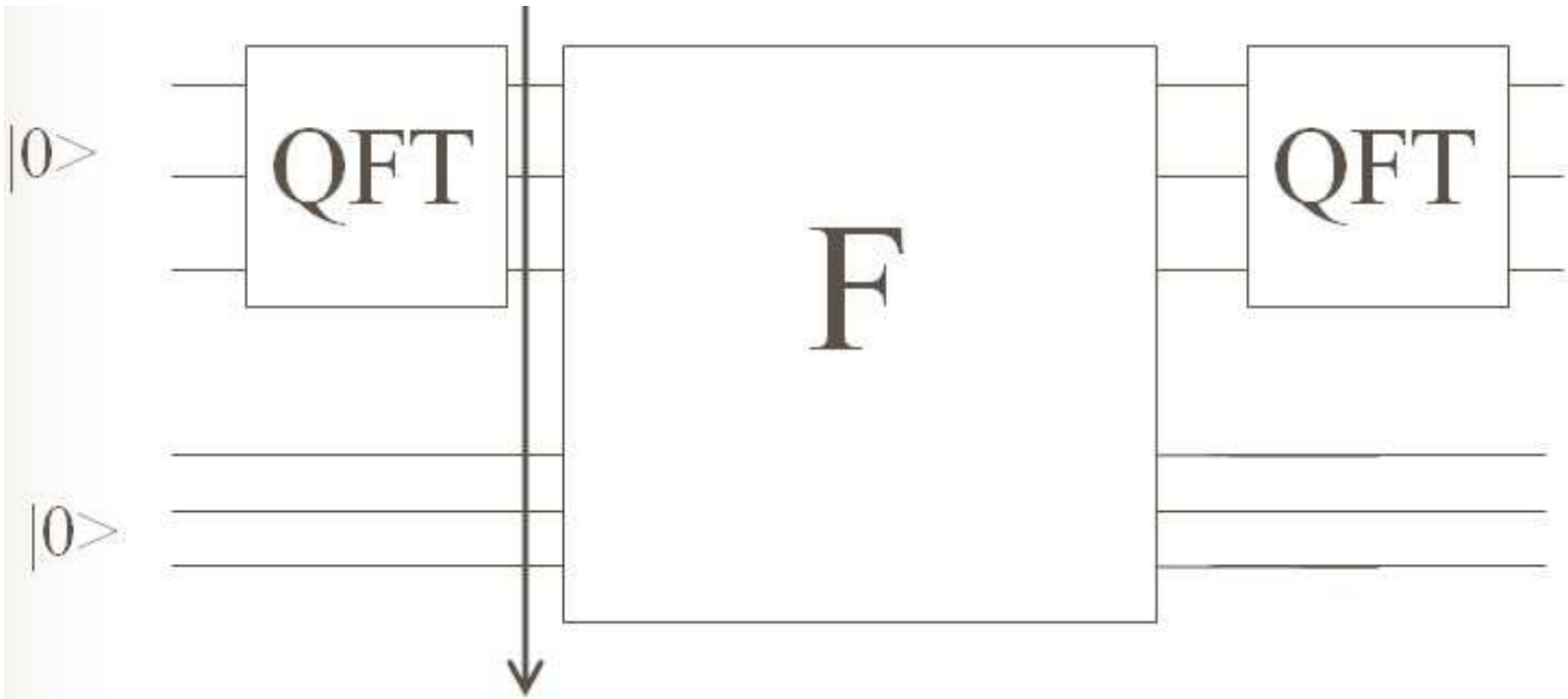
Вычисление порядка



Вычисление порядка

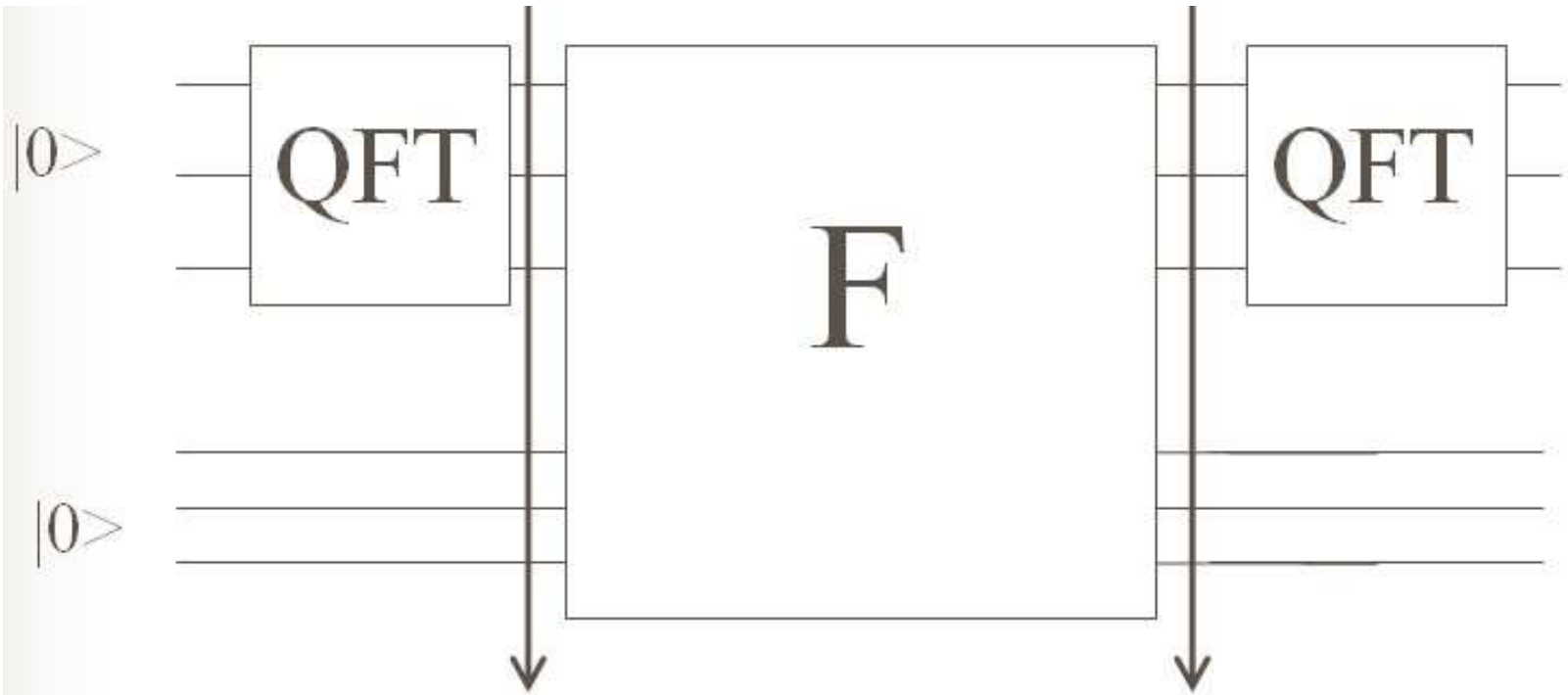


Вычисление порядка II



$$\frac{1}{\sqrt{M}} \sum_{x=1}^{M} |x>|0>$$

Вычисление порядка II



Вычисление порядка III

После измерения нижних битов

$|d\rangle + |d + r\rangle + \ldots$

Вычисление порядка III

После измерения нижних битов

$|d\rangle + |d + r\rangle + \ldots$

Стратегия узнавания M/r:

- Производим преобразование Фурье
- Делаем измерение
- Получаем значение вида jM/r
- Повторяем много раз

План лекции

Задача

Как будет работать алгоритм Саймона, если период у не единственный? Можете ли вы модифицировать алгоритм на этот случай?

Последний слайд

Если не запомните ничего другого:

- Свели разложение на множители к нахождению периода

Последний слайд

Если не запомните ничего другого:

- Свели разложение на множители к нахождению периода
- Построили состояние с периодом r

Последний слайд

Если не запомните ничего другого:

- Свели разложение на множители к нахождению периода
- Построили состояние с периодом r
- Получили смесь состояний “кратных” M/r.

Последний слайд

Если не запомните ничего другого:

- Свели разложение на множители к нахождению периода
- Построили состояние с периодом r
- Получили смесь состояний “кратных” M/r.

Последний слайд

Если не запомните ничего другого:

- Свели разложение на множители к нахождению периода
- Построили состояние с периодом r
- Получили смесь состояний “кратных” M/r.

Вопросы?