

## Семинар 8. Квантовые алгоритмы.

### 8.1 Алгоритм Дойча (Deutsch).

Алгоритм Дойча сочетает квантовый параллелизм с квантовомеханической интерференцией. Рассмотрим цепь приведенную на рис. 8.1.

Пусть гейт Адамара приводит первый кубит в суперпозицию вида  $(|0\rangle + |1\rangle)/\sqrt{2}$ , а второй кубит в состояние суперпозиции вида  $(|0\rangle - |1\rangle)/\sqrt{2}$ . Это означает, что гейт Адамара действует на первый кубит в состоянии  $|1\rangle$ , а на второй кубит в состоянии  $|1\rangle$ .

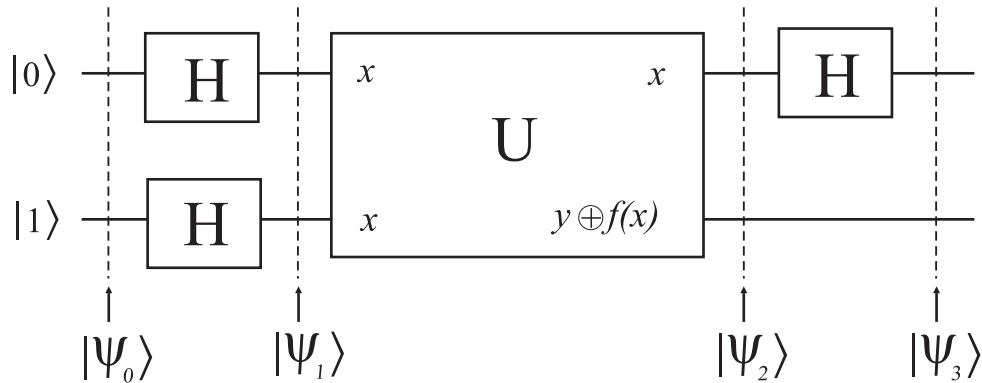


рис. 8.1.

Входное состояние такой цепи, есть двухкубитовое состояние вида:

$$|\psi_0\rangle = |01\rangle. \quad (8.1)$$

После действий оператора Адамара данное двухкубитовое состояние будет иметь вид:

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (8.2)$$

Рассмотрим действие оператора  $\hat{U}$  на  $|x\rangle (|0\rangle - |1\rangle)/\sqrt{2}$ , где  $|x\rangle$  может принимать одно из двух значений:  $|x\rangle = |0\rangle$  или  $|x\rangle = |1\rangle$

$$\hat{U} \left[ |x\rangle (|0\rangle - |1\rangle) \right] = \begin{cases} |0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle, & \text{для } |x\rangle = 0 \\ |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle, & \text{для } |x\rangle = 1. \end{cases} \quad (8.3)$$

Функция  $f(x)$  принимает значения 0 или 1, при  $x = 0, 1$ . Рассмотрим последовательно случай  $|x\rangle = |0\rangle$

$$\hat{U} \left[ |0\rangle (|0\rangle - |1\rangle) \right] = \begin{cases} |0, 0\rangle - |0, 1\rangle, & f(0) = 0 \\ |0, 1\rangle - |0, 0\rangle, & f(0) = 1 \end{cases} = (-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle). \quad (8.4)$$

Аналогично для случая  $|x\rangle = |1\rangle$

$$\hat{U} \left[ |1\rangle (|0\rangle - |1\rangle) \right] = \begin{cases} |1, 0\rangle - |1, 1\rangle, & f(1) = 0 \\ |1, 1\rangle - |1, 0\rangle, & f(1) = 1 \end{cases} = (-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle). \quad (8.5)$$

Объединяя равенства (8.4) и (8.5) получим

$$\hat{U} \left[ |x\rangle (|0\rangle - |1\rangle) \right] = (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) / \sqrt{2}. \quad (8.6)$$

Таким образом после действия цепи  $U$  на двухкубитовое состояние  $|\psi_1\rangle$  получим

$$U : |\psi_1\rangle \rightarrow |\psi_2\rangle = \begin{cases} \pm \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle+|1\rangle}{\sqrt{2}}, & \text{если } f(0) = f(1) \\ \pm \frac{|0\rangle-|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}}, & \text{если } f(0) \neq f(1) \end{cases}. \quad (8.7)$$

Действуя в соответствии с цепью приведенной на рис. 8.1. на первый кубит гейтом Адамара, находим:

$$H_1 : |\psi_2\rangle \Rightarrow |\psi_3\rangle = \begin{cases} \pm |0\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{если } f(0) = f(1) \\ \pm |1\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{если } f(0) \neq f(1) \end{cases}. \quad (8.8)$$

Учитывая, что  $f(0) \oplus f(1) = 0$  если  $f(0) = f(1)$ , и  $f(0) \oplus f(1) = 1$ , если  $f(0) \neq f(1)$  можно переписать выражение (8.8) в виде

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (8.9)$$

Таким образом измеряя состояние первого кубита можно определить значение  $f(0) \oplus f(1)$ , т.е. квантовая цепь дает возможность определить **глобальное свойство** функции  $f(x)$ , используя только одно вычисление  $f(x)$ . Это быстрее, чем с использованием классического вычислительного устройства, которое потребует как минимум двух вычислений.

В простейшем варианте задача Дойча состоит в следующем <sup>1</sup> Пусть имеются четыре бинарные функции  $f_i(x)$  от двоичной переменной  $x = 0, 1$  при этом функции  $f_1$  и  $f_2$  – постоянны и принимают значения  $f_1(x) = 0$ ,  $f_2(x) = 1$ , а функции  $f_3$  и  $f_4$  – принимают следующие значения:  $f_3(x) = x$ ,  $f_4(x) = \neg x$ . При этом говорят, что функции  $f_3$  и  $f_4$  – сбалансированы. В задаче Дойча требуется определить к какой группе (постоянные или сбалансированные) относится функция  $f_i$

Классическое решение такой задачи предполагает проведение как минимум двух операций – вычисление  $f_i(0)$  и  $f_i(1)$ . Квантовый алгоритм позволяет решить задачу за одну операцию. Квантовый компьютер работает как черный ящик (в квантовых вычислениях его принято называть Оракул), выполняя унитарную операцию

$$\hat{U} \left\{ |x\rangle \otimes |y\rangle \right\} \Rightarrow |x\rangle \otimes |y \oplus f(x)\rangle. \quad (8.10)$$

Оператор  $\hat{U}$  представляется четырьмя матрицами размерности  $4 \times 4$ , определяющими четыре

<sup>1</sup> Deutsch D. Quantum Theory the Church-Turing Principle and the Universal Quantum Computer. Proc. Roy. Soc. London, 1985, V A400, № 1818, p. 57. Перевод с английского под ред. В.А. Садовниченко: Сборн "Квантовый компьютер и квантовые вычисления". Ижевск. Ред. журн. "Регулярная и хаотическая динамика", 1999, с. 157.

возможные функции  $f_i(x)$

$$\begin{aligned} \hat{U}_{f_1} &\equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv \hat{I}; & \hat{U}_{f_2} &\equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \equiv \hat{I} \otimes NOT; \\ \hat{U}_{f_3} &\equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \equiv CNOT; & \hat{U}_{f_4} &\equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv CNOT(\hat{I} \otimes NOT). \end{aligned} \quad (8.11)$$

Как следует из изложенного выше алгоритма для решения задачи Дойча достаточно только одной операции (квантовая цепь 8.1). Если состояние первого кубита на выходе цепи (8.9)  $|0\rangle$ , то  $f_{1,2}(x)$ — постоянные функции. Если состояние первого кубита на выходе цепи  $|1\rangle$ , то  $f_{3,4}(x)$ — сбалансированные функции. Существенно, что при этом не вычисляются значения самих функций. Квантовый компьютер выделяет "глобальную" информацию из суперпозиции состояний.

Экспериментально данный алгоритм был реализован на простейших ЯМР— квантовых компьютерах<sup>2</sup>

## 8.2 Алгоритм Дойча — Джозса (Deutsch-Jozsa).

Данный алгоритм был сформулирован для общего случая, когда  $|x\rangle$  и  $|y\rangle$  являются векторами в  $2^n$ -мерном гильбертовом пространстве  $|x\rangle = |x_0, x_1, \dots, x_{n-1}\rangle$ ,  $|y\rangle = |y_0, y_1, \dots, y_{n-1}\rangle$ , а квантовый Оракул  $\hat{U}$  действует на многомерный вектор состояния<sup>3</sup>. Задача, в данном алгоритме формулируется подобно предыдущему алгоритму и имеет целью определить является ли двузначная функция постоянной или сбалансированной, имеющей одно значение для одной половины данных  $x$  и другое — для второй. Квантовый алгоритм позволяет решить эту задачу за  $n$ -операций, тогда как классический алгоритм имеет решение за  $2^n$ -операций.

Алгоритм может быть продемонстрирован на примере следующей игры. Алиса, находясь в Амстердаме, выбирает число  $x$  из  $0 \div 2^n - 1$  и посылает его по почте Бобу в Бостоне. Боб вычисляет некоторую функцию  $f(x)$  и сообщает результат, который может быть или 0, или 1. При этом Боб обещал использовать функцию  $f$ , одну из двух типов: Либо  $f(x)$ — постоянна для всех значений  $x$ , либо  $f(x)$ — сбалансирована, при этом она равна 1 точно для половины всех возможных значений  $x$  и равна 0 для другой половины. Задача Алисы определить достоверно какой тип функции выбран Бобом для вычислений, затратив при этом минимум корреспонденции.

В классическом случае Алиса может послать Бобу только одно значение  $x$  в каждом письме. Поэтому Алиса будет вынуждена запросить Боба по меньшей мере  $2^n/2 + 1$  раз, так как она может получить  $2^n/2$  нулей для окончательного получения 1, объясняющего ей,

<sup>2</sup>К.А. Валиев, А.А. Кокин "Квантовые компьютеры: надежды и реальность", Москва. Ижевск. R&C 2001 г.

<sup>3</sup>Deutsch D., Jozsa R. Rapid Solution of Problems by Quantum Computation. Proc. Roy. Soc., London, 1992, V A439, № 1907, p.553. Перевод с английского под ред. В.А. Садовниченко: Сборн. "Квантовый компьютер и квантовые вычисления". Ижевск: Ред. журн. "Регулярная и хаотическая динамика", 1999, с.191.

что Боб использует сбалансированную функцию, поэтому лучший классический алгоритм она может применять  $2^n/2 + 1$  раз. Подчеркнем, что в каждом письме Алиса посылает Бобу  $n$ -бит информации.

Если Алиса и Боб могут обмениваться кубитами и если Боб согласен вычислить  $f(x)$  используя унитарное преобразование  $U_f$ , тогда Алиса может достичь своей цели одной корреспонденцией используя следующий алгоритм.

Алиса имеет  $n$ -кубитовый регистр для накапливания своего запроса и однокубитовый регистр, который она представляет Бобу для размещения ответа. Алиса готовится как регистр запроса, так и регистр ответа в состоянии суперпозиции. Боб проведет вычисление  $f(x)$  с использованием квантового параллелизма и поместит результат в регистр ответа. Затем Алиса осуществляет интерференцию состояний используя гейт Адамара для регистра запроса и заканчивает исследования путем проведения подходящего измерения с целью определения является ли  $f$  постоянной функцией или сбалансированной.

Пошаговое исполнение алгоритма представлено квантовой цепью на рис. 8.2.

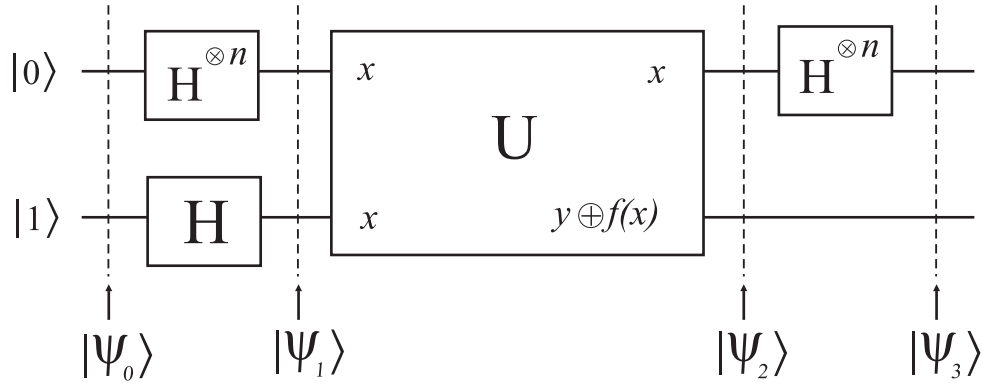


рис. 8.2.

Исходное состояние есть

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle, \quad (8.12)$$

где регистр запроса определяется  $n$ -кубитовым состоянием, каждый из которых находится в состоянии  $|0\rangle$ . После применения Гейта Адамара ко всем кубитам как регистра запроса, так и регистра ответа возникнет состояние  $|\psi_1\rangle$  вида:

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (8.13)$$

Регистр запроса теперь является суперпозицией всех значений  $x$ , а регистр ответа находится в суперпозиции состояний  $|0\rangle$  и  $|1\rangle$ .

Затем Боб вычисляет функцию  $f$ , используя квантовый оракул:

$$\hat{U} : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle. \quad (8.14)$$

В результате образуется состояние  $|\psi_2\rangle$  вида:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (8.15)$$

Теперь Алиса имеет набор кубитов, в которых результат вычисления функции собран в амплитуде суперпозиции кубитового состояния. Алиса далее использует интерференцию слагаемых в суперпозиции путем действия Гейта Адамара на регистр запроса. Чтобы определить результат действия преобразований Адамара полезно, вычислить действие преобразования Адамара на состояние  $|x\rangle$ . Рассматривая случаи  $x = 0$  и  $x = 1$  отдельно, мы видим, что для одиночного кубита

$$H|x\rangle = \sum_z (-1)^{xz} |z\rangle / \sqrt{2}. \quad (8.16)$$

Таким образом

$$H^{\otimes n} |x_1 \dots x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1 \dots z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1 \dots z_n\rangle, \quad (8.17)$$

что может быть записано компактно в форме:

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x \cdot z} |z\rangle, \quad (8.18)$$

где  $x \cdot z$  — побитовое внутреннее произведение  $x$  и  $z$  по модулю 2. Используя (8.18) можно записать результат вычисления состояния  $|\psi_3\rangle$

$$|\psi_3\rangle = \sum_x \sum_z \frac{1}{2^n} (-1)^{x \cdot z + f(x)} |z\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]. \quad (8.19)$$

Теперь Алиса может наблюдать регистр запроса. Отметим, что амплитуда для состояния  $|0\rangle^{\otimes n}$  есть  $\sum_x (-1)^{f(x)} / 2^n$ .

В случае, если  $f$  — константа, амплитуда для  $|0\rangle^{\otimes n}$  равна  $+1$  или  $-1$ , в зависимости от значения константы  $f(x)$ . Так как состояние  $|\psi_3\rangle$  имеет единичную длину отсюда следует, что все другие амплитуды должны быть равны 0 и измерение даст нулевые значения для всех кубитов в регистре запроса. Если  $f$  сбалансирована тогда положительный и отрицательный вклад в амплитуду для  $|0\rangle^{\otimes n}$  сокращается, приводя к нулевому значению амплитуды, а измерение должно дать результат 0 хотя бы одного кубита в регистре запроса. Таким образом, если Алиса измеряет все 0, тогда функция константа, в противном случае функция сбалансирована.

Суммарно алгоритм Дойча-Джозса выглядит следующим образом.

**Входные данные:**

1. Оракул  $U$ , который осуществляет преобразование  $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$  для  $x \in \{0, \dots, 2^{n-1}\}$  и  $f(x) \in \{0, 1\}$ .
2.  $f(x)$  — либо константа для всех  $x$ , либо — сбалансирована, так что  $f(x) = 1$  для половины значений  $x$  и  $f(x) = 0$  для другой половины значений  $x$ .

**Выходные данные:** 0 если  $f$  — константа.

**Время вычислений:** одно вычисление  $U_f$ .

**Алгоритм:**

1.  $|0\rangle^{\otimes n} |1\rangle$  – инициализация состояний.
2.  $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$  – создание суперпозиции с использованием гейта Адамара.
3.  $\rightarrow \sum_x (-1)^{f(x)} |x\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$  – вычисление  $f$  с использованием оракула  $U$ .
4.  $\rightarrow \sum_x \sum_z \frac{1}{2^n} (-1)^{x \cdot z + f(x)} |z\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$  – преобразование Адамара.
5.  $\rightarrow z$  – измерение для получения ответа задачи.

### 8.3 Классы квантовых алгоритмов.

Имеется 3 класса квантовых алгоритмов

- алгоритмы основанные на квантовых версиях Фурье преобразований (Дойча, Дойча-Джозса, алгоритм Шора факторизации целых чисел, дискретный логарифм);
- алгоритмы квантового поиска;
- алгоритмы моделирования квантовых систем.

#### 8.3.1 Квантовые алгоритмы, основанные на квантовых Фурье-преобразованиях.

Дискретное Фурье-преобразование обычно определяется как преобразование набора  $x_0, x_1, \dots, x_{n-1}$   $N$ -комплексных чисел в набор комплексных чисел  $y_0, y_1, \dots, y_{n-1}$ , определенных соотношением

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j. \quad (8.20)$$

Такое преобразование имеет многочисленные приложения в различных отраслях науки. Рассмотренное выше преобразование Адамара, используемое в алгоритме Дойча-Джозса является примером этого класса Фурье-преобразований. Имея в виду, что мы определяем линейное преобразование  $U$  над  $n$ -кубитами путем действия на вычислительный базис состояний  $|j\rangle$ , где  $0 \leq j \leq 2^n - 1$  можно написать

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle. \quad (8.21)$$

Можно проверить, что дискретное Фурье-преобразование унитарно и фактически может быть реализовано как квантовая цепь. Более того, если мы записываем его действие на суперпозицию

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[ \sum_{j=0}^{2^n-1} e^{2\pi i j k / 2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle \quad (8.22)$$

то видно, что преобразование соответствует векторным обозначениям для Фурье-преобразования (8.20) для случая  $N = 2^n$ .

### 8.3.2 Алгоритмы квантового поиска.

Алгоритм квантового поиска решает следующую задачу:

Задано пространство поиска содержащее  $N$  элементов и нет предварительной информации о структуре расположения элементов в пространстве поиска. Необходимо в данном пространстве элементов найти такой, который удовлетворяет заданному свойству.

Классический алгоритм требует порядка  $N$  операций для осуществления решения такой задачи. Алгоритмы квантового поиска используют  $\sqrt{N}$  операций или шагов.

### 8.3.3 Алгоритмы квантового моделирования.

Классические компьютеры имеют большие трудности моделирования общих квантовых систем в силу физической природы квантовых процессов, что выражается в экспоненциальном росте шагов при классическом моделировании квантового объекта.

## 8.4 Квантовое Фурье-преобразование.

Дискретное Фурье-преобразование набора комплексных чисел  $x_0, x_1, \dots, x_{N-1}$  в набор комплексных чисел  $y_0, y_1, \dots, y_{N-1}$  определяется равенством (8.20)

Квантовое Фурье-преобразование есть аналогичное преобразование, хотя общепринятые обозначения для квантовых Фурье-преобразований несколько отличаются. Квантовое Фурье преобразование ортонормированного базиса  $|0\rangle \dots |N-1\rangle$  определено как линейный оператор со следующим действием на базисные состояния:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i j k \cdot \frac{1}{N}\right) |k\rangle. \quad (8.23)$$

Эквивалентное, действие на произвольное состояние может быть записано в виде

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle, \quad (8.24)$$

где амплитуды  $y_k$  являются дискретными Фурье преобразованиями амплитуд  $x_j$ . Это преобразование является унитарным и, поэтому, может определять динамику квантовых вычислений.

В последующем  $N = 2^n$ , где  $n$  — произвольное целое число, а базис  $|0\rangle \dots |2^n - 1\rangle$  — вычислительный базис для  $n$ -кубитового квантового компьютера. Полезно записать состояние  $|j\rangle$ , используя бинарное представление  $j = j_1 j_2 \dots j_n$ :

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0. \quad (8.25)$$

Введем также следующее обозначение  $O.j_\ell j_{\ell+1} \dots j_m$  для представления бинарной функции

$$j_\ell/2 + j_{\ell+1}/4 + \dots + j_m/2^{m-\ell+1}.$$

В результате квантовое Фурье-преобразование может быть задано в следующей полезной форме представления в виде произведения

$$|j_1 \dots j_n\rangle \rightarrow \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i O \cdot j_m} |1\rangle) (|0\rangle + e^{2\pi i O \cdot j_{n-1} j_n} |1\rangle) \dots \dots (|0\rangle + e^{2\pi i O \cdot j_1 j_2 \dots j_n} |1\rangle). \quad (8.26)$$

Это представление в виде произведения настолько полезно, что можно его рассматривать как определение квантового Фурье преобразования. Эквивалентность представления в форме произведения (8.26) и определения (8.23) следует из следующих элементарных алгебраических выражений

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(2\pi i j k / 2^n) |k\rangle = \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \exp(2\pi i j (\sum_{\ell=1}^n k_\ell \cdot 2^{-\ell})) |k_1 \dots k_n\rangle = \\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \prod_{\ell=1}^n \exp(2\pi i j k_\ell \cdot 2^{-\ell}) |k_\ell\rangle = \\ &= \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^n \left[ \sum_{k_\ell=0}^1 \exp(2\pi i j k_\ell \cdot 2^{-\ell}) |k_\ell\rangle \right] = \\ &= \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^n [|0\rangle + \exp(2\pi i j 2^{-\ell}) |1\rangle] = \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + \exp(2\pi i O \cdot j_m) |1\rangle) (|0\rangle + \exp(2\pi i O \cdot j_{n-1} j_n) |1\rangle) \dots \\ &\dots (|0\rangle + \exp(2\pi i O \cdot j_1 j_2 \dots j_n) |1\rangle). \end{aligned} \quad (8.27)$$

Представление Фурье-преобразования в форме произведения (8.26) позволяет легко вывести эффективные квантовые цепи для квантовых Фурье-преобразований. Такие квантовые цепи изображены на рис. (8.5), на которой гейт  $R_k$  обозначает унитарное преобразование вида

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}. \quad (8.28)$$

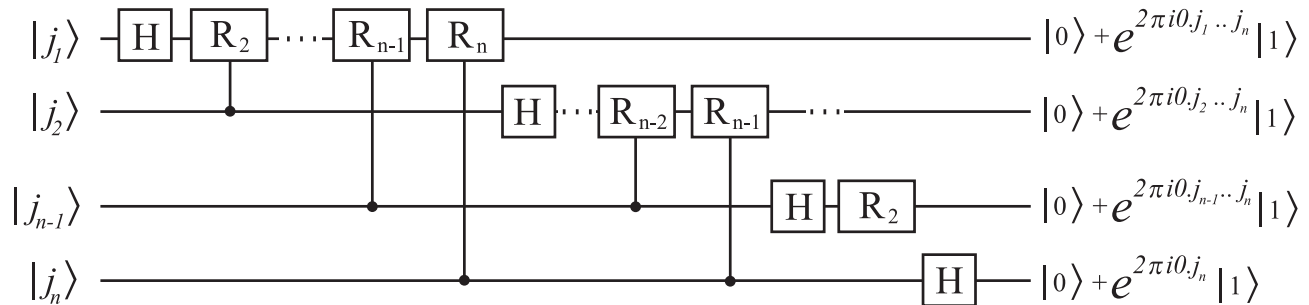


рис. 8.3.



Чтобы показать, что нарисованные цепи действительно вычисляют квантовые Фурье-преобразования, рассмотрим изменения состояний, если начальное состояние имеет вид  $|j_1, \dots, j_n\rangle$ . Применяя гейт Адамара к первому биту получим

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i O \cdot j_1} |1\rangle) |j_2 \dots j_n\rangle \quad (8.29)$$

так как  $\exp(2\pi i O \cdot j_1) = -1$  когда  $j_1 = 1$  и равна  $+1$  в противном случае.

Используя контролируемый  $R_2$ -гейт производим состояние:

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i O \cdot j_1 j_2} |1\rangle) |j_2 \dots j_n\rangle. \quad (8.30)$$

Продолжая вычисление действий контролируемых  $R_3, R_4$  до  $R_n$ -гейтов, каждый из которых добавляет экстра-бит к фазе коэффициента при  $|1\rangle$  первого кубита. В конце этой процедуры получим состояние:

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i O \cdot j_1 j_2 \dots j_n} |1\rangle) |j_2 j_3 \dots j_n\rangle. \quad (8.31)$$

Преобразуем аналогичной процедурой следующий кубит. В результате получим:

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i O \cdot j_1 j_2 \dots j_n} |1\rangle) (|0\rangle + e^{2\pi i O \cdot j_2 \dots j_n} |1\rangle) |j_3 j_4 \dots j_n\rangle. \quad (8.32)$$

Продолжая последовательно для каждого кубита, находим конечное состояние

$$\frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i O \cdot j_1 j_2 \dots j_n} |1\rangle) (|0\rangle + e^{2\pi i O \cdot j_2 \dots j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i O \cdot j_n} |1\rangle) \quad (8.33)$$

Используя далее  $SWAP$  – операторы, состояние кубитов приводится к формуле (8.26), т. е. выполненное Фурье преобразование.