Семинар 9.

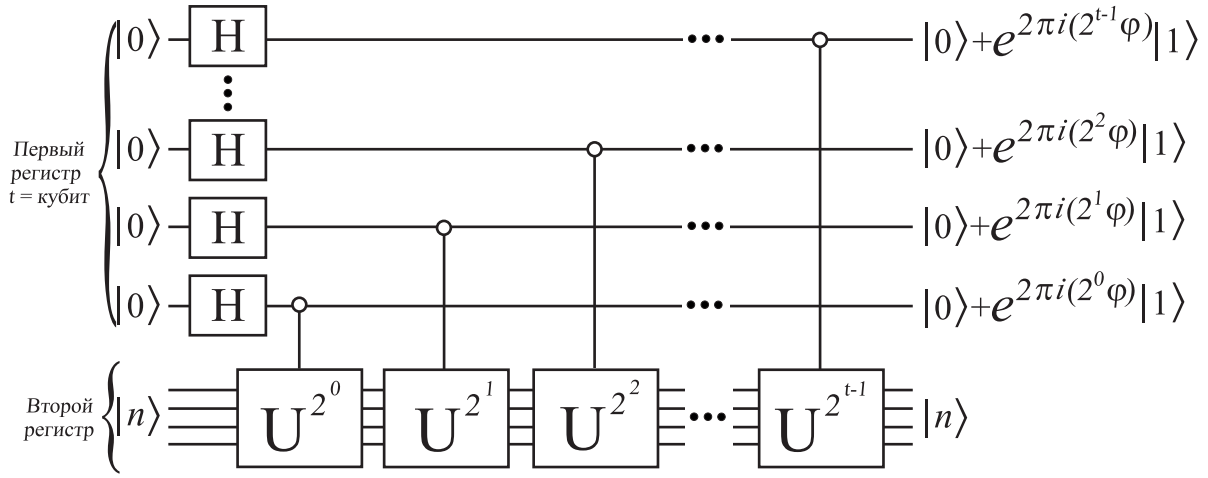
9.1 Оценка фазы.

Фурье- преобразование является основой для общей процедуры, известной как оценка фазы (phase estimation), которая является ключевой для многих квантовых алгоритмов.

Пусть есть унитарный оператор U, имеющий собственный вектор $|U\rangle$ и собственное число $\exp(2\pi i\varphi)$, где φ- неизвестно. Задача алгоритма оценки фазы состоит в вычислении φ.

Квантовая процедура оценки фазы использует два регистра. Первый регистр содержит t кубит первоначально находящихся в состоянии $|0\rangle$. Второй регистр начинается с состояния $|U\rangle$ и содержит столько кубит, сколько необходимо чтобы собрать $|U\rangle$.

Первый шаг процедуры вычисления фазы определяется квантовой цепью вида

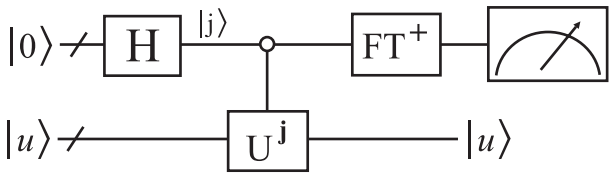


Данная цепь состоит в использовании гейта Адамара с последующим применением controlled-U- операций на второй регистр, с U увеличенным до степени 2. Конечное состояние первого регистра будет иметь вид:

$$\frac{1}{2^{t/2}}\left(|0\rangle+\exp(2\pi i 2^{t-1}\varphi)\,|1\rangle\right)\left(|0\rangle+\exp(2\pi i 2^{t-2}\varphi)\,|1\rangle\right)\ldots$$

$$\ldots\left(|0\rangle+\exp(2\pi i 2^{0}\varphi)\right)=\frac{1}{2^{t/2}}\sum_{k=0}^{2^{t-1}}\exp(2\pi i\varphi k)\,|k\rangle \quad (9.1)$$

Состояние второго регистра не меняется. Второй шаг вычисления фазы состоит в применении обратного квантового Фурье-преобразования для первого регистра. Оно образуется путем обращения цепи квантового Фурье-преобразования. Третий и окончательный шаг есть чтение состояния первого регистра. Схематично весь алгоритм определяется квантовой цепью



Пусть φ - выражается точно t-битами $\varphi = 0.\varphi_1 \dots \varphi_t$, тогда состояние (**??**), после первого шага оценки может быть записано в виде:

$$\frac{1}{2^{t/2}}(|0\rangle + \exp(2\pi i 0.\varphi_t)\,|1\rangle)(|0\rangle + \exp(2\pi i 0.\varphi_{t-1}\varphi_t)\,|1\rangle)\dots$$
$$\dots(|0\rangle + \exp(2\pi i 0.\varphi_1\varphi_2\dots\varphi_t)\,|1\rangle) \quad (9.2)$$

Используя выражение для Фурье-преобразования в виде произведения, ясно, что выходное состояние первого регистра после второго шага есть состояние вида $|\varphi_1 \dots \varphi_t\rangle$. Измерение таким образом дает точно φ.

Алгоритм квантовой оценки фазы.

Входные данные:

1. Черный ящик,который производит controlled - U^j операцию, для целого j.
2. Собственное состояние $|U\rangle$ унитарного преобразования и с собственным числом $e^{2\pi i\varphi}$.
3. $t = n + [\log(2 + \frac{1}{2\varepsilon})]$ кубит находящихся в состоянии $|0\rangle$.

Выходные данные: n- битовое приближение $\widetilde{\varphi_n}$ и φ_n.

Процедура

1. $|0\rangle\,|U\rangle$ - начальное состояние.
2. $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^{t-1}}|j\rangle\,|U\rangle$- создание суперпозиции.
3. $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^{t-1}}|j\rangle\,U^j\,|U\rangle$ - применение "черного ящика".

$= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^{t-1}} e^{2\pi i j\varphi_n}\,|j\rangle\,|U\rangle$ - результат работы "черного ящика".

4. $|\widetilde{\varphi n}\rangle\,|U\rangle$ - применение обратного Фурье-преобразования.
5. $\widetilde{\varphi_n}$ -измерение первого регистра.

Процедура оценки фазы может быть использована для решения ряда интересных задач, таких как проблема нахождения периода и проблема факторизации.

9.2 Алгоритм Шора.

Алгоритм факторизации Шора состоит в определении простых множителей p и q для заданного целого числа $M = p \cdot q$ с использованием квантовой схемы определения периода r некоторой периодической функции вида:

$$y_M(x) = a^x \, mod M$$

где $x = 0, 1, 2 \dots N-1, N = 2^L$, $a -$ любое число, не имеющее общих делителей с M.

Пусть, например, $M = 15$* Выберем $a = 2$. В этом случае последовательность чисел a^x по модулю 15 представляются в следующем виде:

x	0	1	2	3	4	5	6	7	8	...
a^x	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	...
Число	1	2	4	8	16	32	64	128	256	...
$a^x \, mod\, 15$	1	2	4	8	1	2	4	8	1	

*К.А. Валиев, А.А. Копин Квантовые компьютеры: надежды и реальность. R&C Москва. Ижевск 2001.

Таким образом последовательность чисел $a^x \equiv 2^x$ по модулю 15 представляется в следующем виде: $1, 2, 4, 8, 1, 2, 4, 8 \ldots$, то есть имеет период по x равный $r = 4$ и удовлетворяет состояние $2^r \equiv 1 \, mod \, 15$. В общем случае $a^r \equiv 1 \, mod \, M$, а параметр r называется порядком функции $a^x \, mod \, M$, когда $a < M$ и не имеет общих множителей с M.

Если известен период r, множители числа M определяются с помощью классического Алгоритма Евклида как наибольшие общие делители чисел $2^{r/2} \pm 1$ и M. В рассматриваемом примере $2^{4/2} \pm 1 = (5, 3)$. Другими словами $15 = 5 \cdot 3$.

Алгоритм поиска наибольшего общего делителя для пары чисел $n_0 \geqslant n_1$ состоит в вычислении последовательных делений.

$$
\begin{aligned}
n_0 &= d_1 \times n_1 + n_2 \\
n_1 &= d_2 \times n_2 + n_3 \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
n_{m-2} &= d_{m-1} \times n_{m-1} + n_m \\
n_{m-1} &= d_m \times n_m + 0.
\end{aligned}
$$

где d_m—целая часть от деления $n_{m-1} \geqslant n_m$ на каждом шаге. Последний не нулевой сомножитель n_m является ответом алгоритма. Например последовательность:

$$
\begin{aligned}
91 &= 3 \times 28 + 7 \\
28 &= 4 \times 7 + 0
\end{aligned}
$$

показывает, что наибольший общий делитель пары чисел (91, 28) равен 7. Как видно для определения наибольшего общего делителя потребовалось два шага. В общем случае число шагов порядка $\sim \log \log n_1$.

Квантовый алгоритм Шора[†] использует два квантовых регистра X и Y, первоначально находящихся в нулевом булевском состоянии $|0\rangle$. В регистре X размещаются аргументы функции $y_m(x)$, то есть N состояний $|x\rangle = |x_{L-1}, x_{L-2} \ldots x_0\rangle \equiv |x_{L-1}\rangle \otimes |x_{L-2}\rangle \otimes \cdots \otimes |x_0\rangle$. Вспомогательный регистр Y используется для размещения значений самой функции $y_m(x)$ с подлежащим определению периодом r. Число состояний регистра $N = 2^L \geqslant M^2 \gg r^2$.

1-й этап рассматриваемого алгоритма состоит в переводе начального состояния $|0\rangle$ регистра X в равновероятную суперпозицию всех булевских состояний $N = 2^L \, |x\rangle = |x_{L-1}, x_{L-2} \ldots x_0\rangle$, путем применения операции Уолша-Адамара. Регистр Y не меняется. В результате, для системы двух регистров X и Y получается состояние

$$
|\Phi(x, 0)\rangle = \sqrt{\frac{1}{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |0\rangle = \sqrt{\frac{1}{N}} \sum_{x=0}^{N-1} |x, 0\rangle \, .
$$

[†]Shor P. Polinomial-Time Algorithms for Prime Factorization and Descreete Logarithms on a Quantum Computer. SIAM Your Comp., 1997, V.26, N5, p. 1484-1509.

Если, например $M = 15$ данное состояние есть

$$|\varphi[x, y_m(x)]\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |y_m(x)\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |2^x mod 15\rangle =$$
$$= \frac{1}{\sqrt{N}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |2\rangle + |2\rangle \otimes |4\rangle + |3\rangle \otimes |8\rangle + |4\rangle \otimes |1\rangle + |5\rangle \otimes |2\rangle +$$
$$+ |6\rangle \otimes |4\rangle + |7\rangle \otimes |8\rangle + \ldots |N-1\rangle \otimes \left|2^{N-1} mod 15\right\rangle) \quad (9.3)$$

т.е. последовательность функций $y_{15}(x)$ имеет период $r = 4$.

Каждому фиксированному состоянию второго регистра (Y) соответствует последовательность амплитуд, оставшихся в первом (X)-регистре. Например, если зафиксировано состояние второго регистра $|y\rangle$, то в первом регистре соответствующие числа отличаются на период $r = 4$.

$$|\varphi[x, y]\rangle = \frac{1}{\sqrt{N}} (|2\rangle + |6\rangle + |10\rangle + \cdots + |4A + \ell\rangle) \otimes |4\rangle = \frac{1}{\sqrt{A + \ell}} \sum_{j=0}^{A} |rj + \ell\rangle \otimes |4\rangle \quad (9.4)$$

где $0 \leqslant \ell \leqslant r < M$; $A =$ целая часть $[\frac{N}{2} - 1]$. В рассматриваемом случае $\ell = 2$—начальное значение (определяемое выбором фиксированного значения состояния второго регистра). Таким образом второй регистр служит для приготовления периодического состояния в первом регистре.

На втором этапе выделения периода r. Над состоянием первого регистра производится операция Фурье-преобразования. Для простоты пусть N точно делится на r, так что $A = N/2 - 1$. В этом случае Фурье-преобразование есть:

$$QFT_N : \sqrt{\frac{r}{N}} \sum_{j=0}^{A} |rj + \ell\rangle \Rightarrow \sum_{k=0}^{N-1} f_\ell(k) |k\rangle \quad (9.5)$$

где

$$f_\ell(k) = (\sqrt{r}/N) \sum_{j=0}^{A} \exp\left(\frac{2\pi i(jr + \ell)}{N} k\right). \quad (9.6)$$

Вероятность получить состояние $|k\rangle$ определяется выражением:

$$p(k) = |f_\ell(k)|^2 = \left(\frac{r}{N^2}\right) \left| \sum_{j=0}^{A} \exp(2\pi i jrk/N) \right|^2 \quad (9.7)$$

которое как видно не зависит от l. Так как основной вклад в (9.7) дают слагаемые, у которых $rk/N \to$ близко к целому числу, точнее

$$-\frac{r}{2} \leqslant rk \mod N \leqslant r/2, \quad (9.8)$$

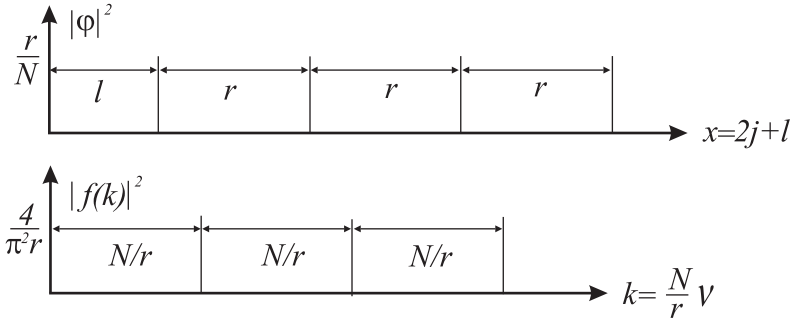
в случае малых значений r/N для каждого r, которое удовлетворяет (9.8), можно получить оценку для вероятности в виде:

$$p(k) \geqslant 4/(\pi^2 r) \tag{9.9}$$

Из(9.9) следует, что по крайней мере с вероятностью $4/\pi^2 \simeq 0,405$ измеренное значение принимает дискретные значения

$$k = \frac{N}{2}\nu, \text{ где } \nu = 0, 1, \ldots r-1.$$

То есть в результате квантового Фурье-преобразования суперпозиция (9.3) преобразуется в равновероятную суперпозицию (9.6) с периодом N/r.



Измерение вероятности (9.7) позволяет определить значения $k \equiv \nu\frac{N}{r}$, имея которые при известном k/N, можно найти отношение ν/r. Если ν и r не имеют общих множителей, можно определить период r путем преобразования отношения ν/r к виду, когда числитель и знаменатель не имеют общих наибольших делителей. После этого с помощью алгоритма Евклида легко найти и множители числа M.

9.3 Алгоритм Гровера (поиск в базе данных).

Пусть несортированная база данных состоит из N записей $S(0), S(1) \ldots S(x) \ldots S(N-1)$, представленных $N = 2^L$ состояниями квантового регистра из L-кубитов. Одна из записей, соответствующих состоянию $x = v$ $S(v) \equiv a$–маркирована. Ее и требуется найти. В квантовом алгоритме Гровера выполняются такие шаги:

1. Первый шаг: создание равновероятной (с равными амплитудами) суперпозиции $|S\rangle$ всех $N = 2^L$ булевских состояний.

$$|y\rangle = |y_{L-1}, y_{L-2} \ldots y_0\rangle$$

Все амплитуды равны $1/\sqrt{N}$. Такая суперпозиция достигается применением гейта Уолша-Адамара, действующего на каждый из L кубитов в состоянии $|0\rangle$.

$$|S\rangle = \hat{W}\,|0\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle \tag{9.10}$$

2. Второй шаг.
Сопоставим x-му начальному состоянию регистра цепочку состояний кубитов $|0\rangle$ и $|1\rangle$

$$|y\rangle = |y_{N-1}, y_{N-2} \dots y_0\rangle$$

и аналогичную цепочку x-му результирующему состоянию, получаемую в результате второй унитарной операции Уолша-Адамара. Фаза результирующей конфигурации изменится на π каждый раз, когда преобразование действует на кубит в состоянии $|1\rangle$, оставляя его в том же состоянии

$$x \cdot y = \sum_{n=0}^{N-1} x_n \wedge y_n. \tag{9.11}$$

3. Третий шаг: выборочное вращение фазы амплитуды в определенных состояниях.
—инверсия U_0, сохраняющая вектор $|0\rangle$, но изменяющая знак состояний ортогональных $|0\rangle$.

$$U_0 \equiv 2\,|0\rangle\,\langle 0| - 1 \tag{9.12}$$

или

$$U_S \equiv 2\,|S\rangle\,\langle S| - 1 \tag{9.13}$$

Такое преобразование называется **преобразованием диффузии**.

Учитывая, что $\langle S\,|S\rangle = 1/N$ и $\langle S\,|x\rangle = 0$ при $S \neq x$ получим:

$$U_S\,|x\rangle = \frac{2}{N}\,|S\rangle - |x\rangle \tag{9.14}$$

Основной алгоритм Гровера является повторением над начальным состоянием двух унитарных операций:

-инверсии амплитуды только у искомого состояния v

$$\hat{U}_v = 1 - 2\,|v\rangle\,\langle v| \tag{9.15}$$

- применения преобразования диффузии для всех амплитуд состояния U_S.

Операция диффузии действует на вектор состояния, у которого все составляющие имеют одинаковые амплитуды, равные среднему значению $\sim 1/\sqrt{N}$, кроме одной, соответствующей искомому состоянию, амплитуда которой после первой операции стала отрицательна. Амплитуды $N-1$ составляющих практически не изменят своей величины, а отрицательная амплитуда станет положительной и увеличит свою величину до $\sim 2/\sqrt{N}$.

Таким образом, необходимо повторение указанных операций $\sim \sqrt{N}$ раз для того, чтобы амплитуда искомого состояния достигла значений $\sim 1 \gg 1/\sqrt{N}$, при которых она может быть измерена.