> A good idea has a way of becoming simpler and solving problems other than that for which it was intended. – Robert Tarjan

# 量子Fourier变换

量子傅里叶变换仅仅改变离散时间傅里叶变换的符号，将其拓展到了量子领域。同时利用量子傅里叶变换的积形式，构造出更加高效的量子线路。

## 量子Fourier变换基本形式

正如引言所述，解决一个问题的好思路可以超越原本问题。傅里叶变换就是其中之一，传统傅里叶变换将时域信号变换到频域。时域上原本杂乱无章的信号波形可能在频域上呈现人们一眼就能看出的规律，大大地简化分析过程。

那么，我们如何将傅里叶变换扩展到量子领域呢?

我们先来观察时域上的离散傅里叶变换公式:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{-2\pi i j \frac{k}{N}}$$

从信号的角度来讲，如果$x_i$是时域上的一组彼此正交的离散数据点，$y_i$是这组数据点经过离散傅里叶变换后表现在频域上的信号，由一组彼此正交的$e^{2\pi ij/N}$基本信号叠加。那么频域上的一个离散点是时域上$N$个数据点的叠加。

简单地用$|k\rangle$替换$x_i$, 用$|j\rangle$替换$y_k$,。在量子语境下，同样的变换则是将一个量子态$|j\rangle$映射到$|0\rangle, |1\rangle, ..., |N-1\rangle$，一共$N$个量子态之和。量子傅里叶变换公式为:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \frac{k}{N}} |k\rangle$$

这两个公式几乎一模一样。值得注意的是，量子傅里叶变换满足酉变换的性质，可以构造酉量子线路。根据酉变换的内积不变性可以证明这一点。
证明：量子傅里叶变换是一个酉变换

## 量子Fourier变换的积形式

为了更加高效地实现量子电路，我们将量子Fourier变换写成如下形式:

$$|j_1,...,j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 \dot{j}_n}|1\rangle)}{2^{n/2}}$$

其中$0.j_1 j_2 ... j_n$是二进制表示，计算方法与二进制小数相同。这个变换的构造过程用到了$e^{2\pi i}$的周期性。

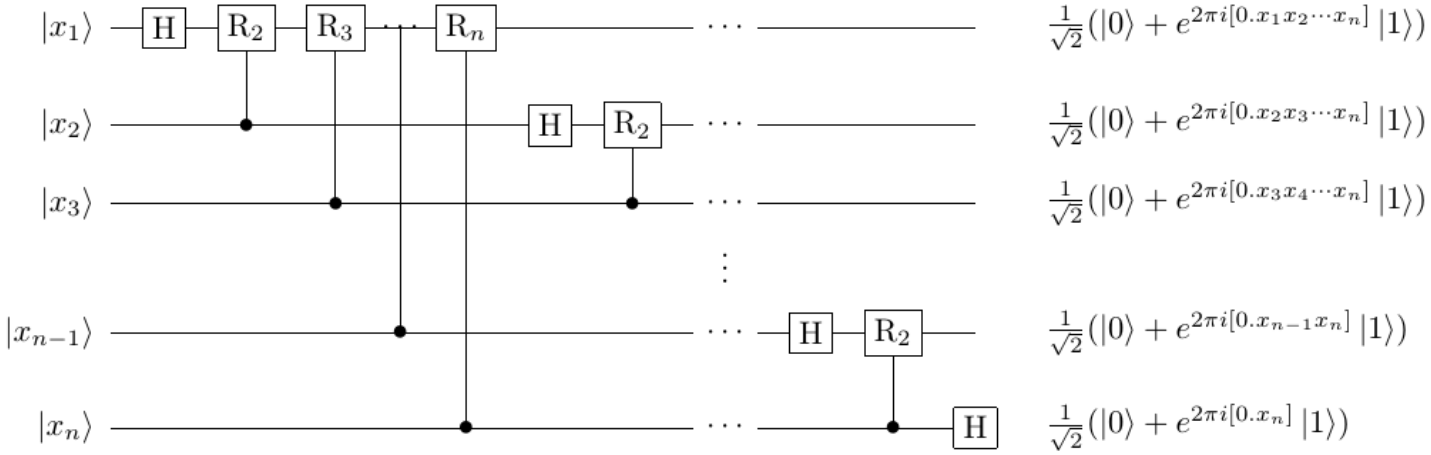
其中$|1\rangle$前面的系数可以写成很多项形如$e^{2\pi i 0.k}$相乘的形式，那么假设有一个$R_k$门:

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2k} \end{bmatrix} = e^{\frac{2\pi i}{2^{k+1}}} X R_z(-\frac{2\pi}{2^{k+1}}) X R_z(\frac{2\pi}{2^{k+1}})$$

这个$R_k$门可以分解成单量子比特门和Pauli-X门的乘积。每个量子态经过一次阿达马变换，然后通过不同数量的与其余量子态有关的受控$R_k$门，可以完成上述公式的操作。

# 量子Fourier变换的量子线路

如图所示是量子傅里叶的量子线路图。




初态为 $|x_i\rangle$ 的量子比特经过如图变换之后，可以转化为乘积的形式。再对这些量子态进行一次逆转顺序，不难得到与上面公式一样的结果。

# 量子傅里叶变换的复杂度

很容易看出，我们一个使用了

| 个数 | 门 |
| --- | --- |
| $n$ | Hadamdard门 |
| $1+2+\cdots+n$ | 受控$R_k$门 |
| $\frac{3}{2}n$ | CNOT门 |

因此量子傅里叶变换的复杂度为$\Theta(n^2)$

# 相位估计

> 酉矩阵的特征值是模为1的复数，不同特征值对应的特征向量两两正交。

相位估计使用初态为 $|0\rangle$ 的量子比特来估计酉算子的相位，这些量子比特经过不同次数的酉变换后，可以变成量子傅里叶变换的积形式。只需要再进行一次量子傅里叶逆变换，可以估计出酉算子的相位。相位估计往往作为其他算法子模块出现。

## 背景

假设酉矩阵 $U$, 其特征向量为$|u\rangle$, 特征值为$e^{2\pi i\varphi}$。那么根据酉矩阵的性质$U|u\rangle = e^{2\pi i\varphi}|u\rangle$。并且对量子态进行变换操作的酉算子可以用酉矩阵来表示。相位估计做的事情，就是把这个$\varphi$估计出来。

相位估计：

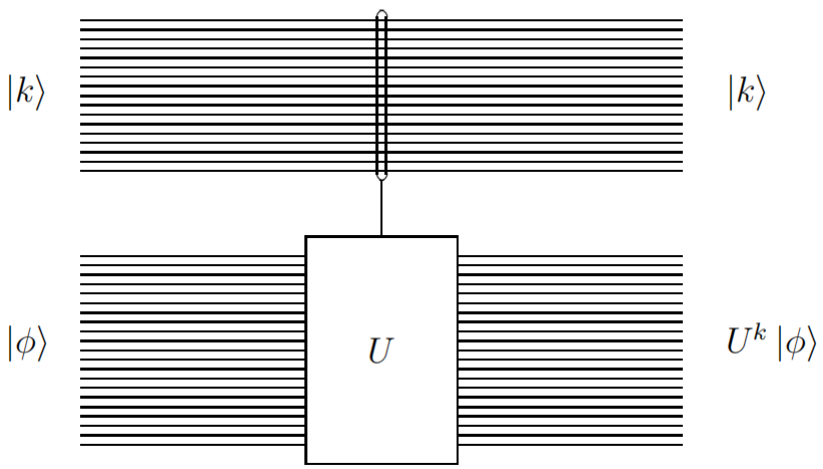
- 输入： 执行酉运算$U$的量子线路$Q$，以及$U$的特征向量$|u\rangle$
- 输出： 估计$U$的相位 $\tilde{\varphi} \in [0,1)$

## 相位估计的量子线路构造

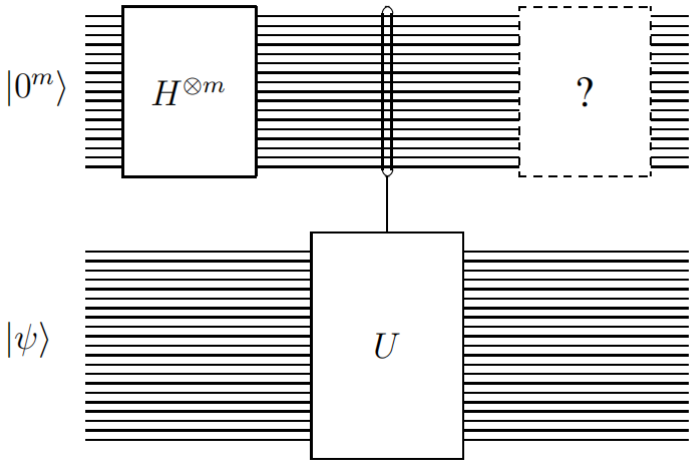
定义 $\Lambda_m(U)$ 为一种对$m+n$个量子比特操作的酉运算，满足

$$\Lambda_m(U)|k\rangle|\psi\rangle = |k\rangle(U^k|\psi\rangle)$$

前面的$m$个量子比特状态决定 $|\psi\rangle$ 进行的酉运算$U$的次数。后一个量子态 $|\psi\rangle$ 是酉矩阵$U$的特征向量。我们用下面这张图来表示 $\Lambda_m(U)$ 这种变换



如图所示，完成相位估计一共需要两个寄存器，显然，得到和测量相位估计的结果需要消耗一个寄存器；除此之外另一个寄存器做什么呢？注意到$U$的特征向量还没有出现，但是实现 $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ 必须要利用特征向量 $|u\rangle$ ,另一个寄存器是不是应该存储$U$矩阵的特征向量呢?




除此之外，我们需要对前$m$个量子比特进行阿达马变换，当 $|0^m\rangle$ 通过一个阿达马门后，我们得到

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}|k\rangle|\psi\rangle$$

再经过一次 $\Lambda_m(U)$ 变换，我们得到

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}|k\rangle(U^k|\psi\rangle)$$

根据特征值和特征向量的关系 $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ 得到，

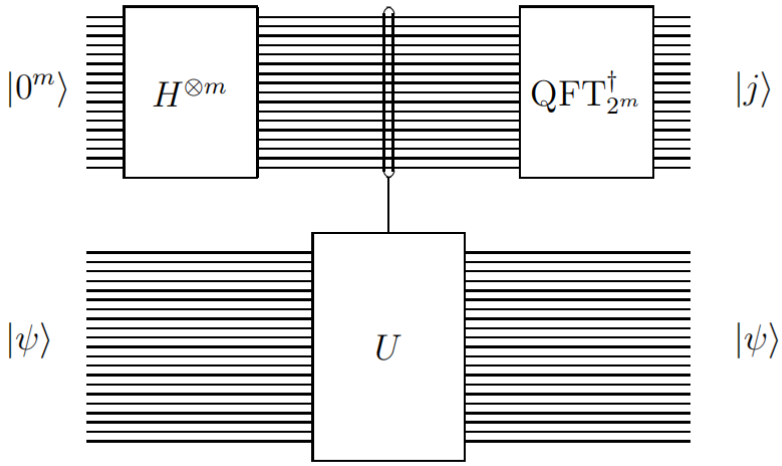
$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle|\psi\rangle$$

因为第二个寄存器始终保持状态 $|\psi\rangle$ , 我们在描述里可以忽略该状态，

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle$$

# 估计 $\varphi$

目前为止我们已经将待估计量 $\varphi$ 放进表达式里，但是还没能估计出具体数字。接下来怎么做呢？本着未知问题向已知问题转化的科学思想，并且上面得到的式子与量子Fourier变换颇有神似。我们试着把剩下的部分交给量子Fourier变换。




如果相位 $\varphi$ 正好能被一个二进制数 $t$ 表示， 数 $t$ 一共有 $m$ 位。那$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle$就恰好可以被表示成Fourier变换的积形式

$$\frac{(|0\rangle+e^{2\pi i0.\varphi_t}|1\rangle)(|0\rangle+e^{2\pi i0.\varphi_{t-1}\varphi_t}|1\rangle)...(|0\rangle+e^{2\pi i0.\varphi_1\varphi_2\dot{\varphi}_t}|1\rangle)}{2^{m/2}}$$

再经过一次逆Fourier变换，得到 $|\varphi_1\varphi_2\dots\varphi_t\rangle$ ，再将二进制数转化为十进制数，得到关于 $\varphi$ 的准确相位。

但是现实往往并非如人所愿， $\varphi$ 不能表示成二进制数又该怎么办呢？同样的算法是不是也行得通的呢？估计的精度是多少？得到满足要求的结果的概率有多大呢？

考虑对一个任意的 $\varphi$ 进行逆Fourier变换，

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}e^{2\pi ik\varphi}|k\rangle\rightarrow\frac{1}{2^m}\sum_{k=0}^{2^m-1}\sum_{j=0}^{2^m-1}e^{2\pi i(k\varphi-kj/2^m)}|j\rangle$$

$$=\sum_{j=0}^{2^m-1}(\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\varphi-j/2^m)}|j\rangle)$$

测量结果为 $|j\rangle$ 的概率为

$$p_j=|\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\varphi-j/2^m)}|^2$$

当 $\varphi$ 正好能被表示成二进制数时，测量出准确结果概率为 $1$ 。但当在更加一般的情况里$p_j\neq1$ ，我们使用等比数列求和公式进行计算

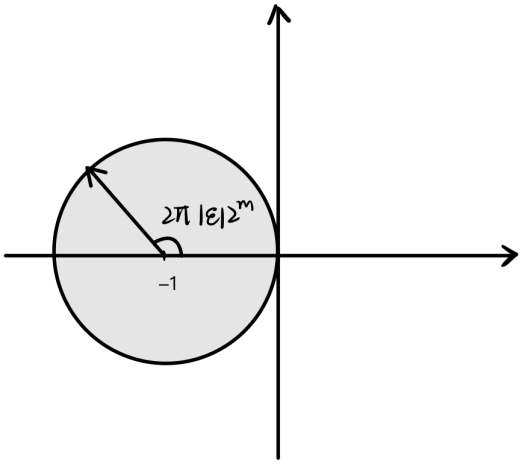
$$p_j=\frac{1}{2^{2m}}|\frac{e^{2\pi i(2^m\varphi-j)}-1}{e^{2\pi i(\varphi-j/2^m)}-1}|^2$$

这下得到正确结果的概率变低，我们试着找一下 $p_j$ 概率的下界，因为这对我们能多大程度上保证估计结果正确有关。假设 $\varphi = \frac{j}{2^m} + \epsilon$ ,其中 $|\epsilon| \leq 2^{-(m+1)}$. 也就是说，测量结果误差在一个量子比特的范围内的概率。

$$p_j = \begin{cases} 1 & ,\epsilon = 0 \\ |\frac{1}{2^m}\sum_{k=0}^{2^m-1} e^{2\pi i k(\varphi - j/2^m)}|^2 & ,\epsilon \neq 0 \end{cases}$$

为了找到 $p_j$ 的下界， 我们对 $p_j$ 的分子分母单独进行变换。

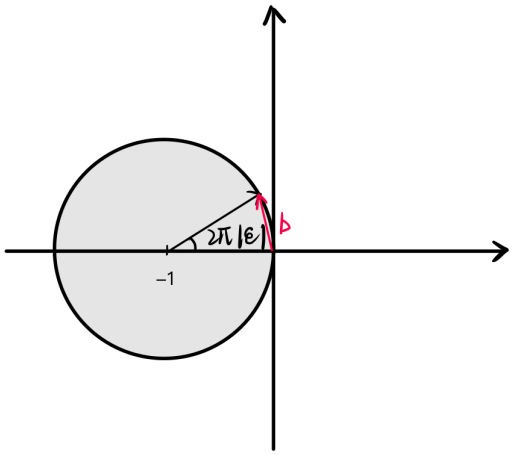
- 分子部分需要找到下界
  令 $a = e^{2\pi i \epsilon 2^m} - 1$ , 这是一个可以被画成如下形式的复数




根据模长与相位的关系，得到 $\frac{2\pi|\epsilon|2^m}{|a|} \leq \frac{\pi}{2}$ 也就是

$$a \geq 4|\epsilon|2^m$$

- 分母部分需要找到上界
  令 $b = e^{2\pi i\epsilon} - 1$ ， 如图所示



我们可以得到 $\frac{2\pi|\epsilon|}{b} \geq 1$ ,即 $b \leq 2\pi|\epsilon|$

因此我们可以得到一个不出错的下界

$$p_j \geq \frac{4}{\pi^2}$$

# 相位估计的应用：求阶和质因数分解

目前看来，相位估计本身似乎没有什么用处，我们得到了一个酉变换的相位。这个相位可以拿来做什么呢?

接下来，我们要介绍相位估计的一个大应用和几个小缺点。

## 数论补充

首先，需要亿点数论知识
假设 $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$, 并且 $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$。

- Euler $\varphi$-function:

  $$\varphi(N) = |\mathbb{Z}_N|$$

  函数返回 $1, 2, \ldots, N$ 中与 $N$互质的元素个数。若 $N$ 为素数，$\varphi(N) = N - 1$.
- Fermat's Little Theorem: 当 $a \in \mathbb{Z}$ , $p$ 是素数时，

  $$a^p \equiv a \mod p$$

- Euler Theorem：当 $a, N$ 互质时，

  $$a^{\varphi(N)} \equiv 1 \mod N$$

- Theorem 1:若 $x$ 是

  $$x^2 = 1 \mod N$$

  的非平凡解，则至少在 $\gcd(x-1, N)$ 和 $\gcd(x+1, N)$ 中有一个是 $N$ 的非平凡因子。
- Theorem 2: 若整数 $r$ 使得，

  $$a^r = 1 \mod N$$

  ，则 $r$ 是 $a$ 的阶。
- Theorem 3：整数 $N = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_m^{\alpha m}$ 可以分解成以上形式。若在整数 $[1, N-1]$ 中随机找一个整数 $x$ ，且 $X$ 与 $N$ 互质， $r$ 是 $x$ 的阶，则

  $$P(r\text{是偶数且}x^{\frac{r}{2}} \neq -1 \mod N) \geq 1 - \frac{1}{2^m}$$

- Theorem 4：令 $a_0, a_2, \ldots, a_N$ 为一正整数数列，那么

$$[a_0, a_2, \ldots, a_N] = \frac{p_n}{q_n}$$

使得 $p_n \equiv a_n p_{n-1} + p_{n-2}, q_n \equiv a_n q_{n-1} + q_{n-2}$

# 背景

求阶：

- 输入： 整数 $N, a \in \mathbb{Z}_N^*$
- 输出： $a, N$ 的阶 $r$

质因数分解：

- 输入：整数 $N$
- 输出：整数 $N$ 的因子

# 求阶

假设 $x$ 是一个整数，$N$ 是一个大于 $x$ 的整数。求阶就是估算如下酉算子的相位

$$U|y\rangle \equiv |xy \mod N\rangle$$

，其中 $x \in (0, N)$ ， $y \in \{0,1\}^L$。

要怎么做呢？注意到如果这里的 $y$ 是 $U$ 的特征向量，那么我们就可以利用相位估计进行分析

假设 $|u_s\rangle$ 是酉算子 $U$ 的特征向量， $s \in [0, r-1]$

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s k}{r}] |x^k \mod N\rangle$$

因为，

$$U|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s k}{r}] |x^{k+1} \mod N\rangle$$

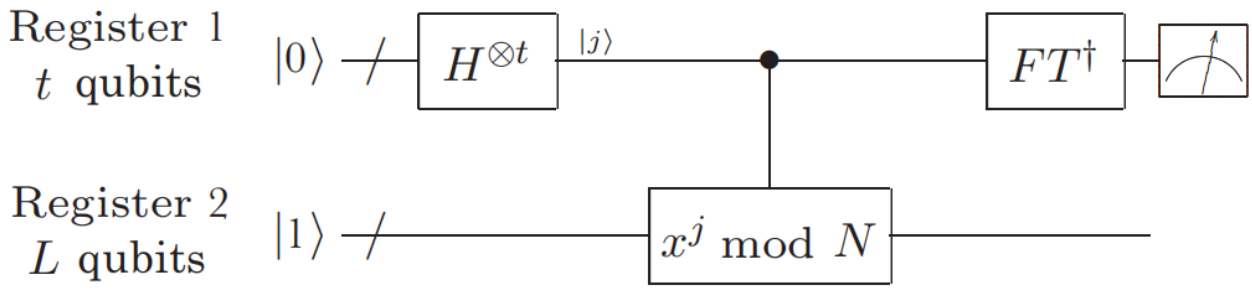
$$= \exp[\frac{2\pi i s}{r}] \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp[\frac{-2\pi i s (k+1)}{r}] |x^{k+1} \mod N\rangle$$

其中的复指数以 $r$ 为周期，因此

$$= \exp[\frac{2\pi i s}{r}] |u_s\rangle$$

因此进行相位估计，我们可以得到 $s/r$ , 然后经过连分式展开，正如定理4所描述的那样。通过数学上的递推关系，我们得到 $s, r$ 的值。

求阶的量子线路图可以表示为如下形式




| 个数 | 门 |
| --- | --- |
| $n$ | Hadamdard门 |
| $n^3$ | 模幂 |
| $n^2$ | 量子逆傅里叶变换 |
| $n^3$ | 连分式算法 |

# 几个小缺点

求阶在什么情况下会出错?

- 相位估计时以一个很小的概率出错
- $r$ 和 $s$ 有公因子，连分式展开时返回 $r'$ 与真实的 $r$ 相差一个因子。

第一种情况很好理解，相位估计在给出近似值的同时以一个很小的概率可能出错。但是这样的概率较低，并且可以通过增加量子比特的数目来减小。

第二种情况也不难理解。连分式算法要求分子分母彼此互质，但是 $s, r$ 不一定彼此互质。不过，据说有三种方法可以解决这个问题。

1. 重复算法 $2\log(r)$ 次：这是因为小于 $r$ 的素数个数至少为 $r/2\log(r)$, 多次重复可以以较高的概率保证至少有一次 $s, r$ 彼此互质。
2. 每次用求得的阶降低求阶对象的大小，直到结果为原对象的阶为止。
3. 进行两次相位估计，结果为 $r_1', s_1'$ 和 $r_2', s_2'$。若两次相位估计的结果 $s_1', s_2'$ 没有公因子，则 $r$ 的估计值可以通过去 $r_1', r_2'$ 最小公倍数得到。借助书上的Box 5.4和下面的图片可以更好的理解这一点

| $\frac{l}{2^t}$ | $\frac{0}{2048}$ | $\frac{512}{2048}$ | $\frac{1024}{2048}$ | $\frac{1536}{2048}$ |
|---|---|---|---|---|
| $\frac{\tilde{s}}{r}$ | | $\frac{1}{4}$ | $\frac{1}{2}$ | $\frac{3}{4}$ |
| $r'$ | | 4 | 2 | 4 |
| 最小公倍数即为 r | $r = 4$ | | | |



## 质因数分解

质因数分解所需的全部知识就是求阶和数论

- 根据定理1，如果我们能找到 $x^2 = 1 \mod N$ 的非平凡解，那我们至少能在$\gcd(x-1, N)$ 和 $\gcd(x+1, N)$ 中的一个找到 $N$ 的非平凡因子。
- 如果一个与 $N$ 互质的 $y$ 的阶是偶数，那么 $y^{r/2} = x$ 是一个可能的解。

# 量子搜索

量子搜索可以加速经典搜索。在大多数情况下，经典条件下如果需要进行 $O(n)$ 次搜索，在量子搜索条件下搜索次数会被开二次方根，仅仅需要 $O(\sqrt{n})$ 次搜索

## 背景

- 输入： $n+1$ 个处于 $|0\rangle$ 的的量子比特；可以进行搜索结果识别的Oracle黑箱
- 输出： 搜索结果 $x_0$

## 从Oracle描述量子搜索

假设搜索范围是 $[1, N]$，其中 $N = 2^n$，在搜索范围内有 $M$ 个元素是我们的搜索目标。构造一个可以识别搜索解的酉算子Oracle，

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

其中 $f(x)$ 可以识别搜索的解， $|q\rangle = |0\rangle$，

$$f(x)=\begin{cases}1 & x是解\\ 0 & x不是解\end{cases}$$

我们只需要观察 $|q\rangle$ 是否发生反转，能够知道搜索解的位置。

再进一步，如果 $|q\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$。 $|q\rangle$ 的值通过Oracle后只会有一个相位的变化。将相位的变化与 $|q\rangle$ 分离，省略没有变化的部分，上面的式子进一步被化简成，

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

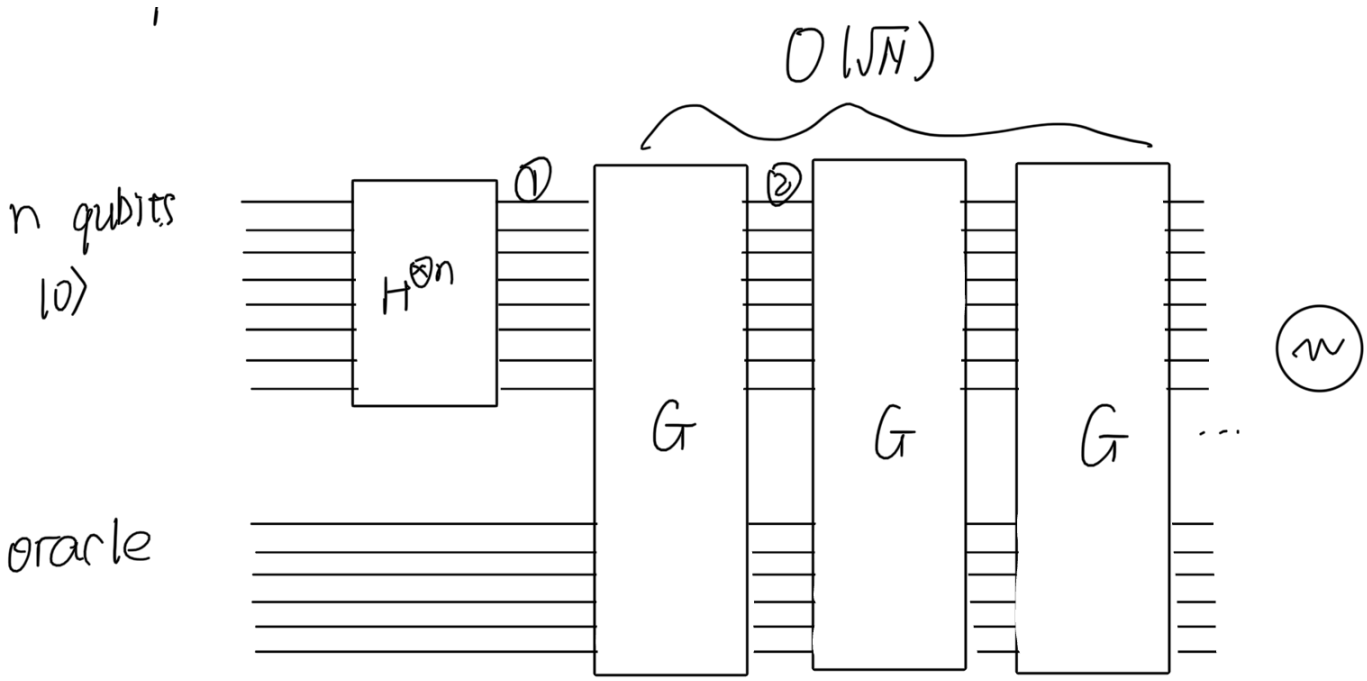
对量子比特相位进行测量，可以得到搜索解的位置。

# 从过程描述量子搜索

量子包括两个阶段:

- 第一阶段将第一个寄存器的 $n$ 个量子比特进行一个阿达马的变换
- 第二阶段将两个寄存器的量子比特一起送进 Grover 门，并且这个过程可能一共会进行 $O(N)$ 次迭代

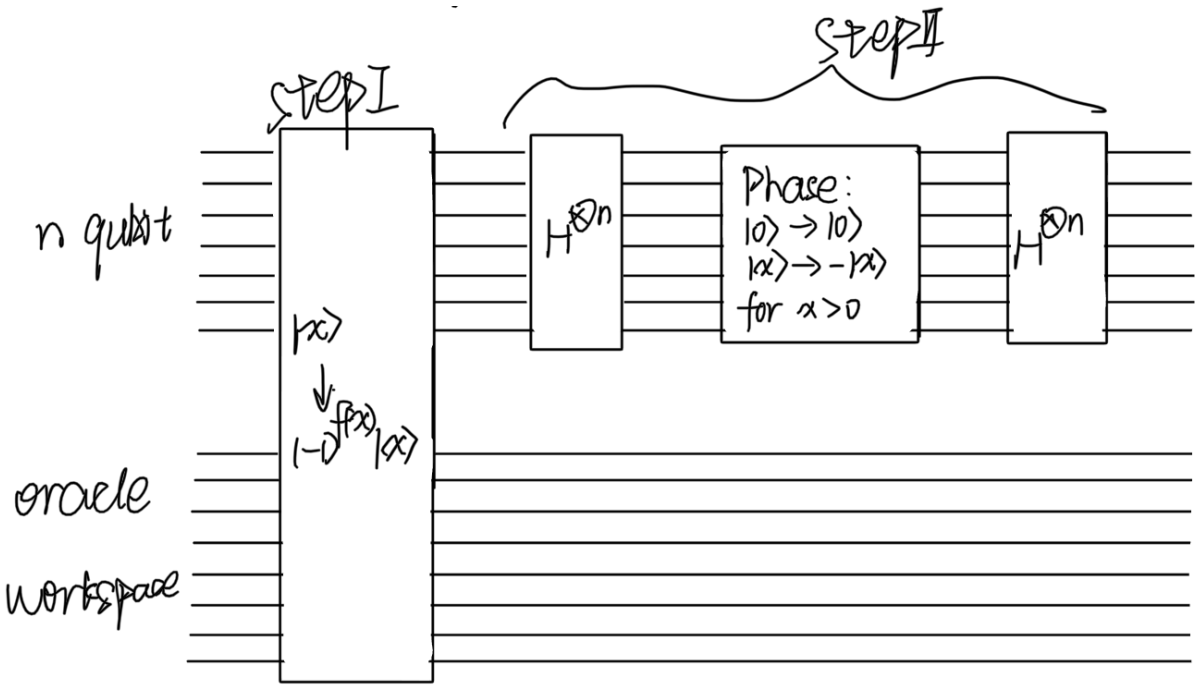
## 第一阶段




$n$ 个处于 $|0\rangle$ 的量子比特通过阿达马门，

$$H^{\otimes n}|0\rangle=\frac{1}{n^{\frac{1}{2}}}\sum_{x=0}^{n-1}|x\rangle=|\psi\rangle$$

# 第二阶段




一次Grover包括两个过程:

- 过程一：应用Oracle，搜索目标发生相位变化
- 过程二：分别应用两次阿达马变换，其间进行一次有选择地相位改变

首先针对相移部分的酉算子，当输入量子比特不为 $|0\rangle$ 时，输入量子比特的相位会被反转； 输入 $|0\rangle$ 时保持不变。因此该酉算子的形式如下

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{bmatrix}$$

这个酉算子等同于

$$2|0\rangle\langle 0| - I$$

相移前后的阿达马变换分别作用于 $|0\rangle\langle 0|$ 上， 过程二可以被表达为：

$$G = 2|\psi\rangle\langle\psi| - I$$

# 形象化描述Grover

> Grover变换始终在一个平面内

Grover变换可以通过作图来形象表达。为此，我们先引入一些符号，然后借助图像加深对Grover的理解

# 符号说明

在搜索范围 $N$ 中一共有 $M$ 个解，$\sum_x'$ 表示搜索的解的和；$\sum_x''$表示搜索的非解的和；为了满足归一性，定义 $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$ ，$|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$
故初态为

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$$= \frac{1}{\sqrt{N}} (\sum_x^{'} |x\rangle + \sum_x^{''} |x\rangle)$$

$$= \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

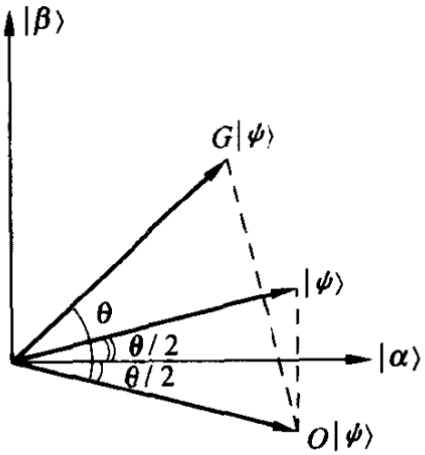
满足 $1 = (\sqrt{\frac{N-M}{N}})^2 + (\sqrt{\frac{M}{N}})^2$

# 几何描述

首先通过一个Oracle，解的相位增加 $\pi$ ，非解的相位不变，体现在符号上是解前增加一个符号

$$|\psi\rangle = a|\alpha\rangle + b|\beta\rangle \xrightarrow{O} O|\psi\rangle = a|\alpha\rangle - b|\beta\rangle$$

然后通过 $2|\psi\rangle\langle\psi| - I$, 该变换将 $O|\psi\rangle$ 以 $|\psi\rangle$ 为对称轴向上翻折




如果 $|\psi\rangle$ 与 $|\alpha\rangle$ 夹角最初为 $\frac{\theta}{2}$ 那么经过一次上述变换后，夹角增大为 $\frac{3\theta}{2}$。 $G|\psi\rangle$ 距离 $|\beta\rangle$ 更近。用一个公式来描述这种关系是

$$G^k|\psi\rangle = \cos(\frac{2k+1}{2}\theta)|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)|\beta\rangle$$

我们已经知道最初 $|\psi\rangle$ 与 $|\beta\rangle$ 夹角为 $\arccos(\sqrt{\frac{M}{N}})$。故旋转次数在 $\frac{\arccos(\sqrt{\frac{M}{N}})}{\theta}$ 左右进行一个取整，系统就接近 $|\beta\rangle$ 状态

下面我们来计算 $\theta$ 的值

$$\sin\theta = \sin(\frac{\theta}{2}+\frac{\theta}{2})$$

$$= \sin(\frac{\theta}{2})\cos(\frac{\theta}{2}) + \cos(\frac{\theta}{2})\sin(\frac{\theta}{2})$$

$$= 2\sqrt{\frac{N-M}{N}}\sqrt{\frac{M}{N}} = 2\frac{\sqrt{(N-M)M}}{N}$$

因此， $\theta = \arcsin(2\frac{\sqrt{(N-M)M}}{N})$。根据均值不等式， 当 $M = N/2$ 时， $\theta$ 取到最大值，此时搜索次数最小。但是当解的数目增多，$\theta$ 减小，搜索次数反而会增加。量子搜索的难度并不是随着解的数量增多而单调递减的。

如果考虑最坏情况 $M \ll N, \theta \approx \sin\theta \approx 2\sqrt{M/N}$，最后的迭代次数不会超过 $\frac{\arccos(\sqrt{\frac{M}{N}})}{2\sqrt{M/N}} \leq \frac{\pi/2}{2\sqrt{M/N}}$