北京邮電大學

# 第5讲 量子Fourier变换与相位估计

高　飞
网络空间安全学院

# 提纲

- Shor 算法
  - 量子Fourier变换
  - 相位估计
  - 求阶
  - 因子分解
- 实例和推广

## 离散Fourier变换

- 任务: 将一个复向量 $x_0, \ldots, x_{N-1}$ 变换为另一个复向量 $y_0, \ldots, y_{N-1}$ 其中

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

等价于幺正矩阵

$$F\begin{bmatrix} x_0 \\ \vdots \\ x_{N-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ \vdots \\ y_{N-1} \end{bmatrix}, \quad F_{jk} = \frac{1}{\sqrt{N}} e^{2\pi ijk/N}$$

## 量子Fourier变换

- 任务: 在量子态幅度上执行离散Fourier变换

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

- 等价地，转换为“基态作用”表示形式

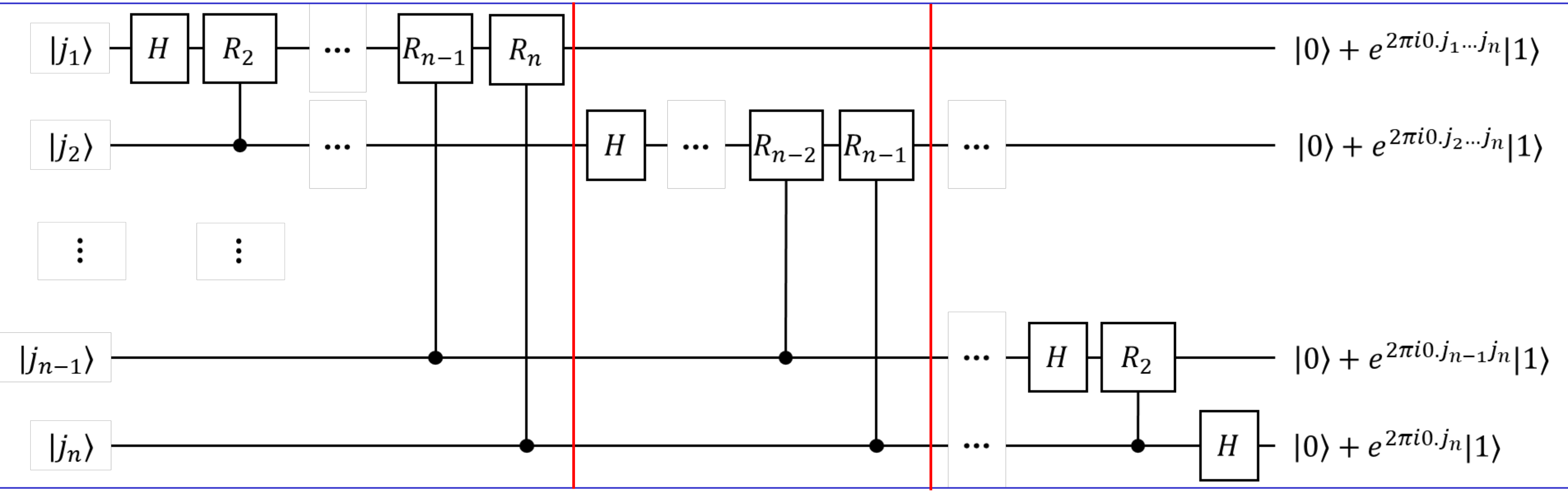
$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

注：这里$x_j$满足归一化条件，若不满足则相当于变换前后的向量各差一个常数倍数

北京邮电大学
Beijing University of Posts and Telecommunications

# 量子Fourier变换线路图

➢ 设$N=2^n$，则 $N*N$ 的幺正矩阵代表作用在 $n$ 量子比特上的一个操作




注：省略了线路末端逆序操作和归一化因子

输出（逆序后）就是QF变换末态的逐比特表示

二进制表示：$0.j_l j_{l+1} \cdots j_m = j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$

➢ 复杂度：$n+(n-1)+\ldots+1=(n+1)n/2=O(n^2)$

❑ 统计可有效实现的简单门（控制U和一位门）个数

➢ 离散Fourier变换的最优经典算法的复杂度：$O(n2^n)$

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

# 小结

| 目标 | 复杂度 | 加速效果 |
|---|---|---|
| 输入 $\sum_{j=0}^{N-1} x_j\vert j\rangle$，输出 $\sum_{k=0}^{N-1} y_k\vert k\rangle$，其中$y_k$是$x_j$的离散傅立叶变换值 | $O(\log^2 N)$ | 指数加速 |

- 是"态到态"的离散Fourier变换：并没有加速计算"经典数据的Fourier变换"
  - 给定一个向量 $x_0,\cdots,x_{N-1}$ ,目前还没有通用的有效方法制备$\sum_{j=0}^{N-1} x_j|j\rangle$
  - Fourier变换的值编码在输出量子态的幅度上：若用量子层析输出所有的 $y_k$，复杂度至少为$\Omega(N)$，不再具有指数加速效果
- 运用量子Fourier变换能为解决某些问题提供指数加速效果

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

开脑洞：如果能把要求的值放到叠加态的相位(差)上（或者说到得了上面线路图中的末态），则一个逆变换就能导出来！ ---相位估计

# 提纲

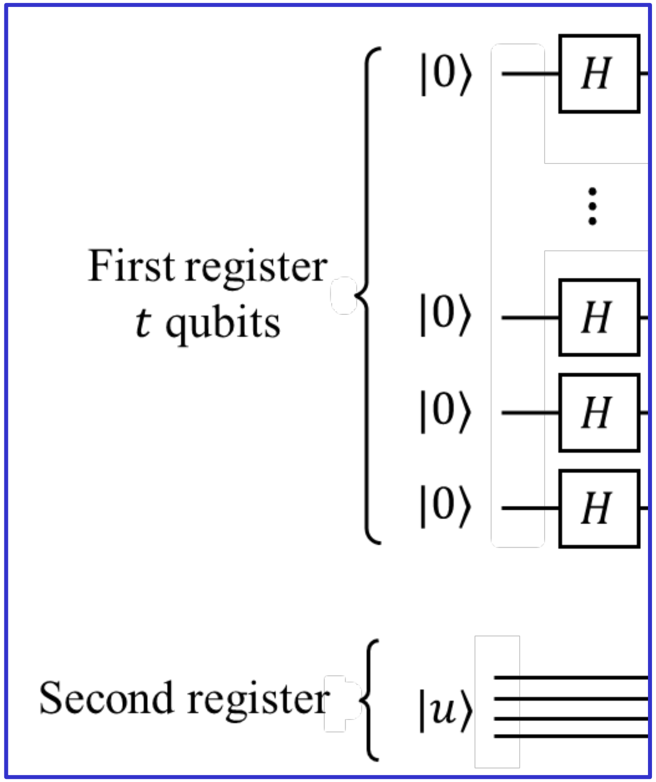
- Shor 算法
  - 量子Fourier变换
  - 相位估计
  - 求阶
  - 因子分解
- 实例和推广

# 问题

$U|u\rangle = e^{2\pi i\varphi}|u\rangle$

- 若幺正矩阵$U$具有一个特征值为$e^{2\pi i\varphi}$的特征向量$|u\rangle$，其中$\varphi \in [0,1)$ 是未知的，有如下条件时可估计它的值
  - 前提条件1：有量子态$|u\rangle$
  - 前提条件2：可以进行受控 $U^{2^j}$运算

- 初始化：使用两个寄存器
  - 第一个：包含初态为$|0\rangle$的$t$量子比特。$t$是与求解的精度和成功概率有关的参数
  - 第二个：初态为$|u\rangle$（量子比特数由$|u\rangle$决定）

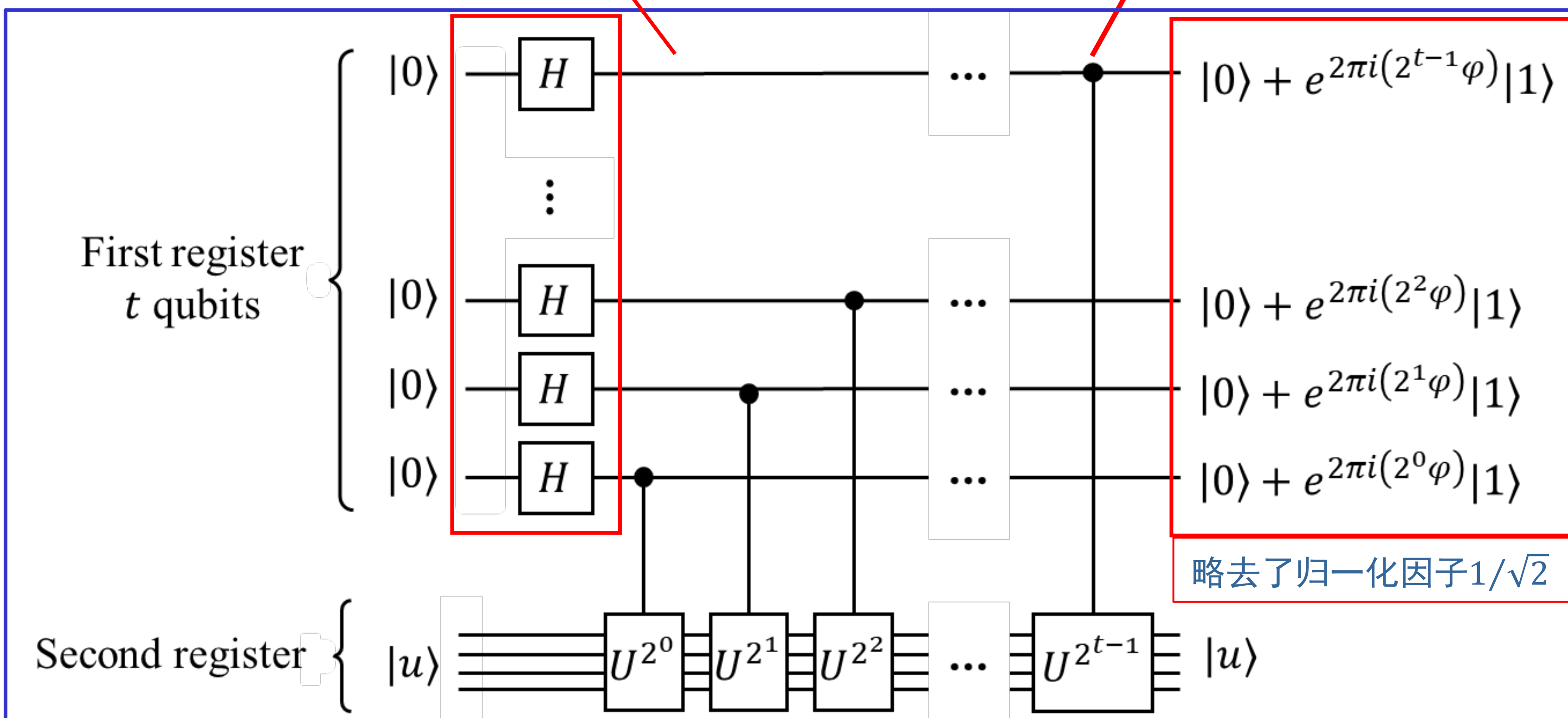


# 求解流程

## 第一阶段：产生均匀叠加态，并执行受控$U^{2^j}$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)^{\otimes t}=\sum_{j=0}^{2^t-1}\frac{1}{\sqrt{2^t}}|j\rangle$$

$$(|0\rangle+|1\rangle)|u\rangle \xrightarrow{CU^{2^j}} |0\rangle|u\rangle+|1\rangle U^{2^j}|u\rangle$$
$$=|0\rangle|u\rangle+e^{2\pi i\cdot 2^j\varphi}|1\rangle|u\rangle=(|0\rangle+e^{2\pi i\cdot 2^j\varphi}|1\rangle)|u\rangle$$



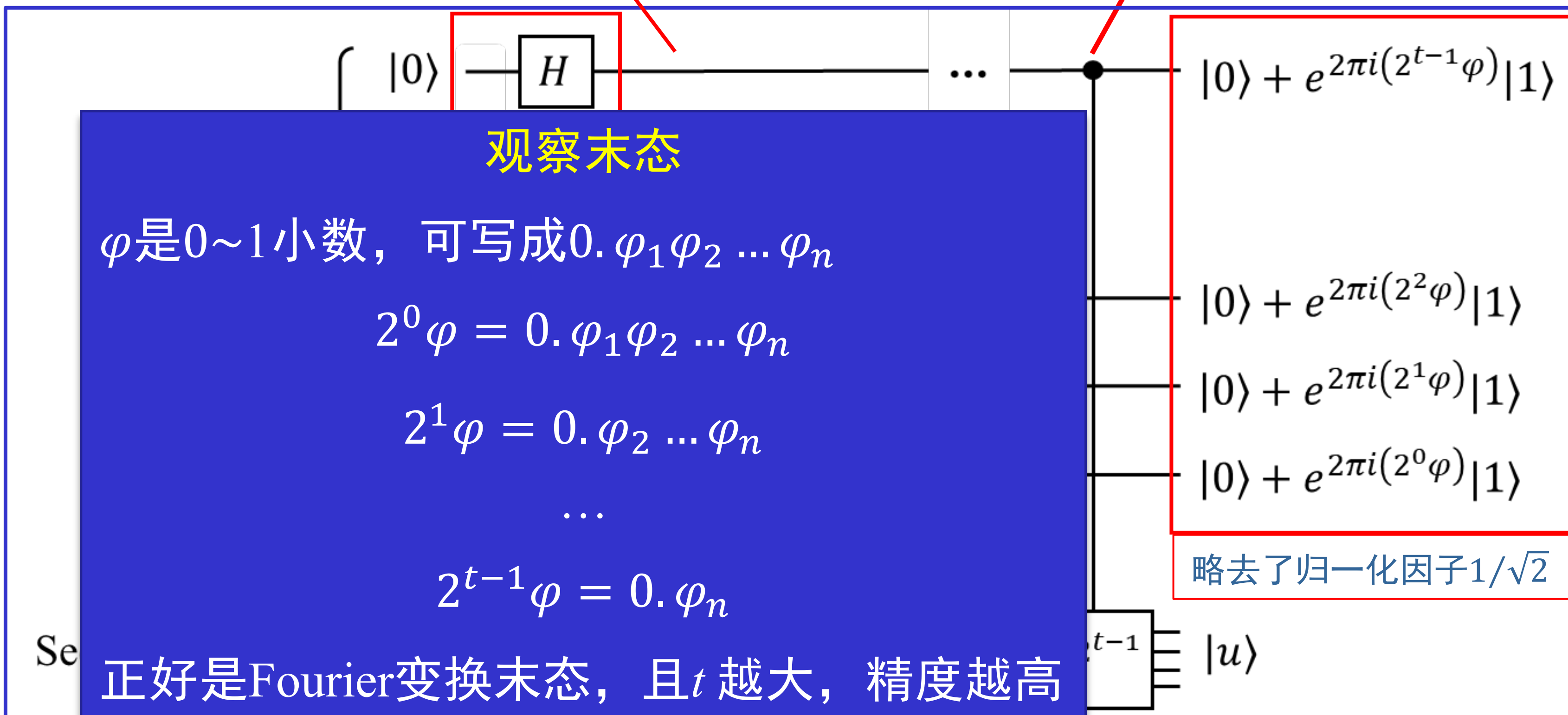
# 求解流程

## 第一阶段：产生均匀叠加态，并执行受控$U^{2^j}$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)^{\otimes t}=\sum_{j=0}^{2^t-1}\frac{1}{\sqrt{2^t}}|j\rangle$$

$$(|0\rangle+|1\rangle)|u\rangle \xrightarrow{CU^{2^j}} |0\rangle|u\rangle+|1\rangle U^{2^j}|u\rangle$$

$$=|0\rangle|u\rangle+e^{2\pi i\cdot 2^j\varphi}|1\rangle|u\rangle=(|0\rangle+e^{2\pi i\cdot 2^j\varphi}|1\rangle)|u\rangle$$




### 观察末态

$\varphi$是0~1小数，可写成$0.\varphi_1\varphi_2\ldots\varphi_n$

$$2^0\varphi=0.\varphi_1\varphi_2\ldots\varphi_n$$

$$2^1\varphi=0.\varphi_2\ldots\varphi_n$$

$$\cdots$$

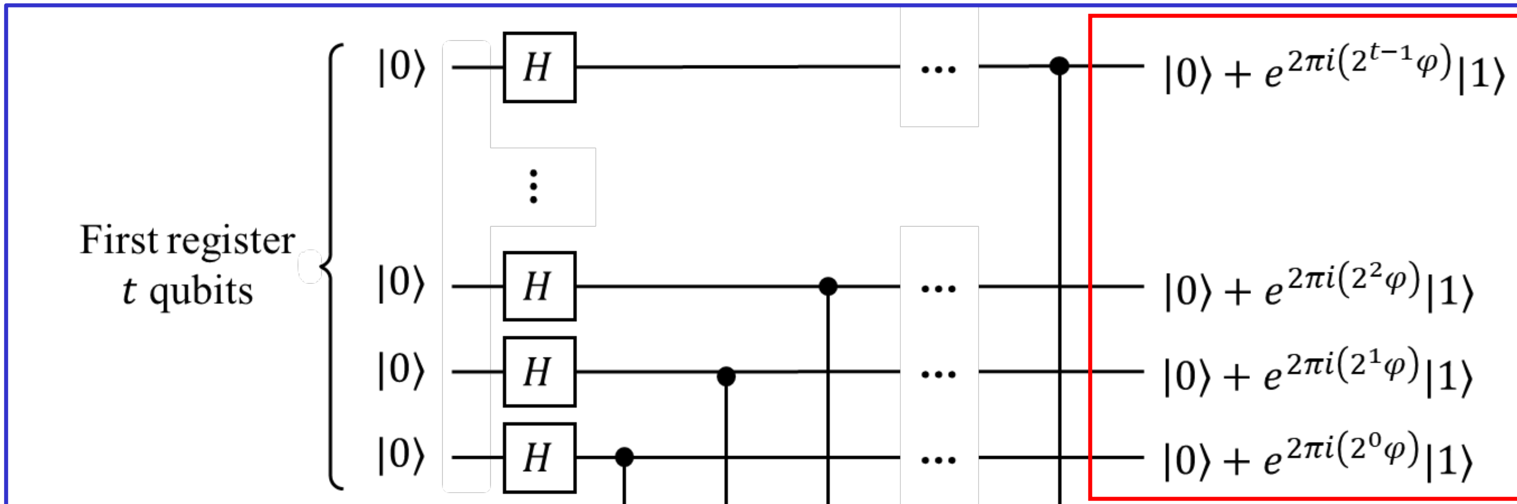
$$2^{t-1}\varphi=0.\varphi_n$$

正好是Fourier变换末态，且$t$越大，精度越高

# 求解流程

## 第二阶段：对第一寄存器执行逆Fourier变换，再测之，可得 $2^t\varphi$

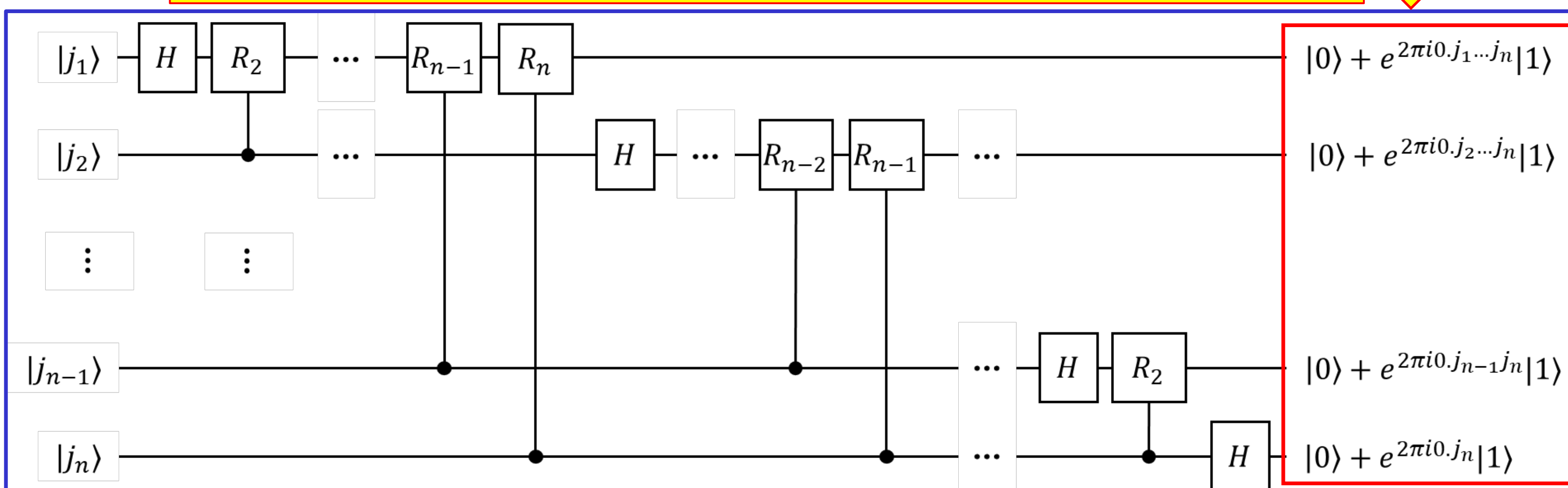
这里




逆F变换

完全相同（逆序一下），即已构造出傅里叶变换的末态！

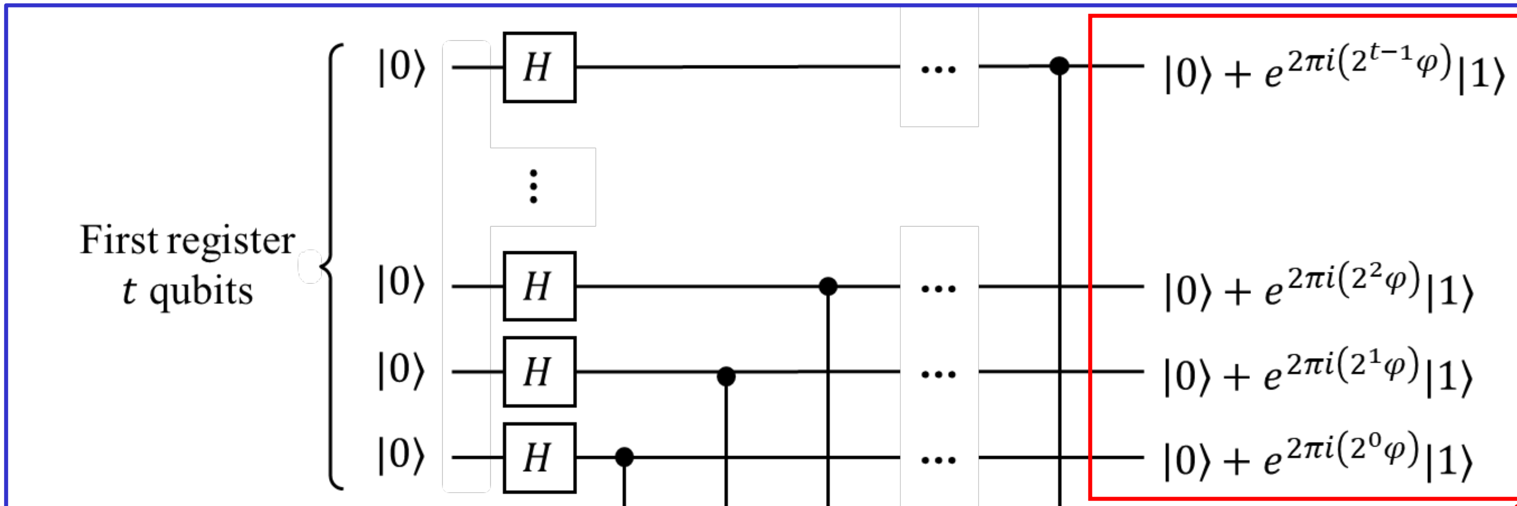
傅里叶变换



# 求解流程

## 第二阶段：对第一寄存器执行逆Fourier变换，再测之，可得 $2^t\varphi$

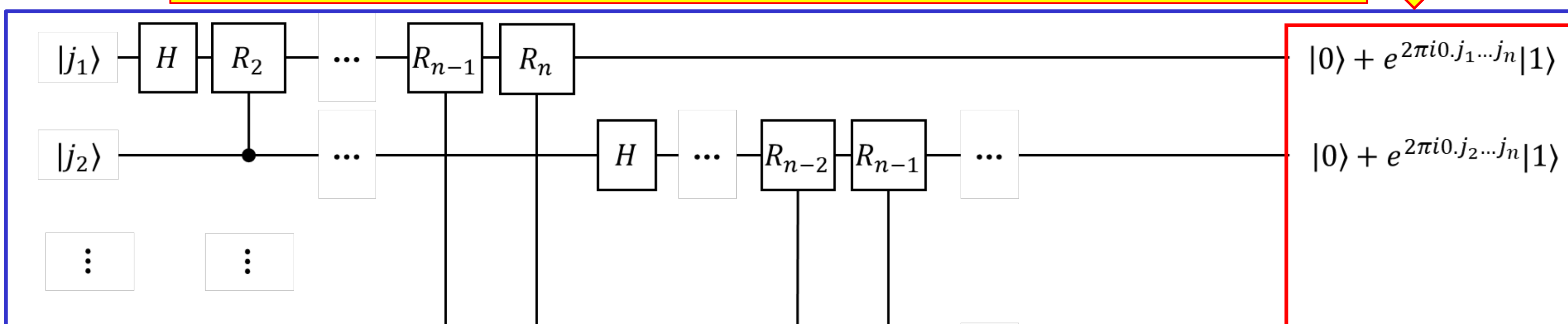
这里




逆F变换

完全相同（逆序一下），即已构造出傅里叶变换的末态！

傅里叶变换




- 若$\varphi$恰好为$t$比特，即$\varphi=0.\varphi_1\cdots\varphi_t$，显然逆F变换可精确测得$\varphi$值
- 若$\varphi$的有效比特数大于$t$比特，仍可大概率得到$t$比特$\varphi$的近似值（证明略）

# 算法描述

Procedure:

$U^j|u\rangle = e^{2\pi i j\varphi}|u\rangle$

1. $|0\rangle|u\rangle$ initial state

2. $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$ create superposition

3. $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle$ apply black box

全部受控U操作

$= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi i j\varphi}|j\rangle|u\rangle$ result of black box

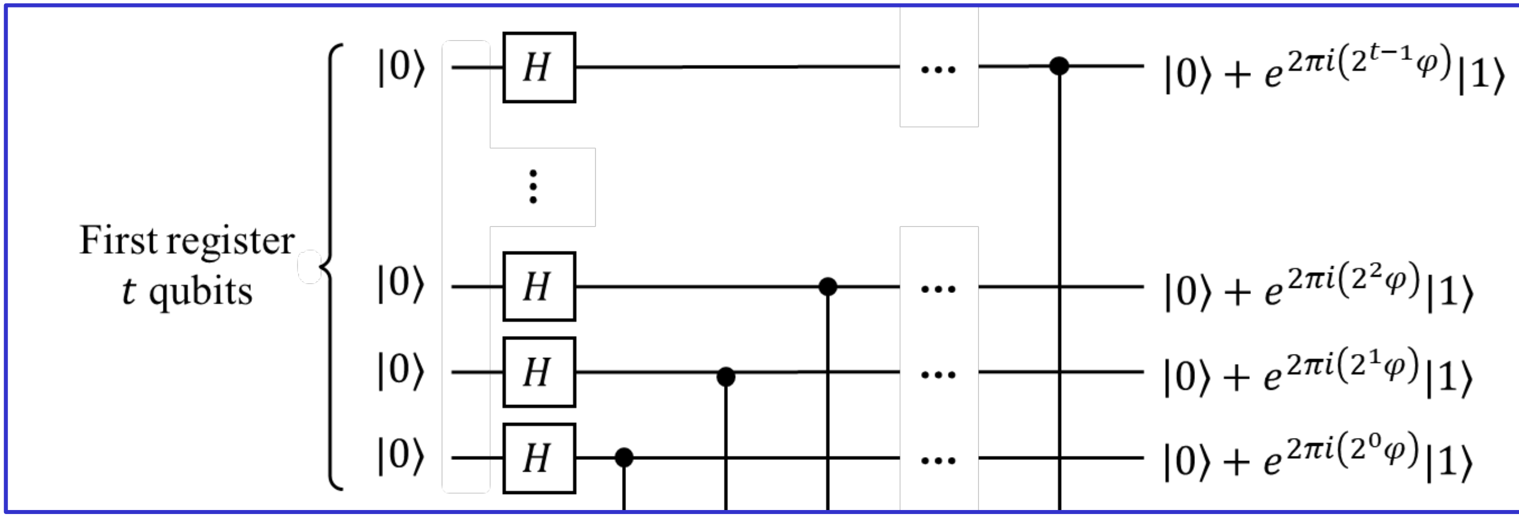
4. $\rightarrow |\widetilde{\varphi}\rangle|u\rangle$ apply inverse Fourier transform

5. $\rightarrow \widetilde{\varphi}$ measure first register

$\approx 2^t\varphi$

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

# 复杂度




逆F变换

- 第一阶段
  - 产生均匀叠加态：$t$个Hadamard门
  - 受控$U^j$需要$U$的个数：$2^0+2^1+\cdots+2^{t-1}=2^t-1=2^n\left(2+\frac{1}{2\eta}\right)-1=\mathcal{O}(\frac{1}{\epsilon}(2+\frac{1}{2\eta}))$
- 第二阶段：逆傅立叶变换需要$\mathcal{O}(t^2)$个门
- 总复杂度：$\mathcal{O}(\frac{1}{\epsilon}\left(2+\frac{1}{2\eta}\right)T_U)$，其中

**$T_U$为实现$U$所需要的时间**

为了以至少$1-\eta$的成功概率得到精确到$n$比特（也即精度$\epsilon=2^{-n}$）的$\varphi$，$t$满足：

$$t=n+\left\lceil\log(2+\frac{1}{2\eta})\right\rceil$$

# 重要推广

➢ 没有本征态$|u\rangle$的话，可以用其叠加态代替！

本征态：$|0\rangle|u\rangle \rightarrow \otimes_{j=0}^{t-1}\left(|0\rangle + e^{2\pi i(2^j\varphi)}|1\rangle\right) \otimes |u\rangle$ 

一个$|u\rangle$，不纠缠

$\rightarrow |\tilde{\varphi}\rangle \otimes |u\rangle$ 测第一寄存器，概率1测得$\varphi$的近似值

叠加态：以$\sum_u c_u|u\rangle$代替$|u\rangle$, 最终的输出量子态为

多个$|u\rangle$，纠缠

$$|0\rangle\sum_u c_u|u\rangle \rightarrow \sum_u c_u \otimes_{j=0}^{t-1}\left(|0\rangle + e^{2\pi i(2^j\varphi_u)}|1\rangle\right) \otimes |u\rangle$$

$\rightarrow \sum_u c_u|\tilde{\varphi}_u\rangle|u\rangle$ 测第一寄存器，概率$|c_u|^2$测得$\varphi_u$的近似值

注：找到易制备的叠加态不难，但最好每个$\varphi_u$中都应该蕴含要求解的值！

# 小结

| 目标 | 输入 | 输出 | 精度 | 复杂度 |
|---|---|---|---|---|
| 给定一个酉矩阵 $U$,<br>和它的一个特征向量 $\|u\rangle$,<br>估计 $\varphi$，其中$\varphi$满足$U\|u\rangle = e^{2\pi i\varphi}\|u\rangle$ | $\|0\rangle\|u\rangle$ | $\|\tilde{\varphi}\rangle \approx \|2^t\varphi\rangle$ | $\epsilon = 2^{-n}$ | $O(\frac{1}{\epsilon}\left(2+\frac{1}{2\eta}\right)T_U)$ |

- 是一个求问题解的方法，但条件很苛刻，需要构造满足下述条件的$U$
  - 必须将问题的解嵌在 $U$ 的（某个）本征值的相位上
  - 可有效制备$U$的对应于上述本征值的本征态$|u\rangle$。但这里本征值未知，本征态一般也是未知，因此只能是用多个本征态的叠加态，暗含2个要求：
    - 需要每个（或者大多数、大概率的）对应的本征值都蕴含问题的解
    - 这多个本征态的叠加正好是一个非常容易制备的态
  - 可有效实现受控$U^{2^j}$操作

# 提纲

- Shor 算法
  - 量子Fourier变换
  - 相位估计
  - 求阶
  - 因子分解
- 实例和推广

# 问题与思路

- 阶的定义：对满足$x < N$，且互素的正整数 $x$ 和 $N$，$x$ 模 $N$ 的阶定义为最小正整数$r$，使得$x^r = 1(\mathrm{mod}N)$
- 问题描述：对给定的 $x$ 和 $N$，确定相应的阶
- 思路：用相位估计，构造$U$和本征态
  - 酉算子：$U|y\rangle = \begin{cases} |xy(\mathrm{mod}N)\rangle, & 当 y < N \\ |y\rangle, & 当 y \geq N \end{cases}$

$N$的长度为 $L = \lceil \log N \rceil$ 比特，$y \in \{0,1\}^L$，$U$作用在$L$个qubit上

存在性：$U$的作用相当于的计算基的一个重排列（$x$和$N$互素，$x$的整倍数mod$N$可遍历所有0~$N$-1之间的整数），容易验证它是酉的

计算基上的置换操作：可写作 U=$\sum|i_a\rangle\langle i_b|$，因为 $U^+=\sum|i_b\rangle\langle i_a|$，两者互逆（相乘得 $\sum|i_a\rangle\langle i_a| = I$）；

把$y>N$的函数值定义为=$y$，也是要保证U的酉性（对基态均为1对1置换）

# 问题与思路

- 阶的定义：对满足$x < N$，且互素的正整数 $x$ 和 $N$，$x$ 模 $N$ 的阶定义为最小正整数$r$，使得$x^r = 1(\mathrm{mod} N)$
- 问题描述：对给定的 $x$ 和 $N$，确定相应的阶
- 思路：用相位估计，构造$U$和本征态
  - 酉算子：$U|y\rangle = \begin{cases} |xy(\mathrm{mod} N)\rangle, & 当 y < N \\ |y\rangle, & 当 y \geq N \end{cases}$
  - 对整数$s$（$0 \leq s \leq r-1$）定义的状态

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

$r$ 未知，但不影响这种态的存在性

$r$ 嵌在了本征值的相位上

用相位估计即可测得 $s/r$

易验证是$U$的本征态：

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

北京邮电大学
Beijing University of Posts and Telecommunications

# 问题与思路

$$\frac{1}{\sqrt{r}}\sum_{t=1}^{r}\exp\left[\frac{-2\pi is(t-1)}{r}\right]|x^t \bmod N\rangle$$
$$=\frac{1}{\sqrt{r}}\sum_{t=1}^{r}\exp\left[\frac{2\pi is}{r}\right]\exp\left[\frac{-2\pi ist}{r}\right]|x^t \bmod N\rangle$$
$$=\exp\left[\frac{2\pi is}{r}\right]\cdot\frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}\exp\left[\frac{-2\pi ist}{r}\right]|x^t \bmod N\rangle$$
$$=\exp\left[\frac{2\pi is}{r}\right]|u_s\rangle$$

的正整数 $x$ 和 $N$，$x$ 模

$r = 1(\bmod N)$

相应的阶

态

$< N$

$|y\rangle$, 当 $y \geq N$

- 对整数 $s$（$0 \leq s \leq r-1$）定义的状态

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^k \bmod N\rangle$$

$r$ 未知，但不影响这种态的存在性

$r$ 嵌在了本征值的相位上

用相位估计即可测得 $s/r$

易验证是 $U$ 的本征态：

$$U|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^{k+1} \bmod N\rangle = \exp\left[\frac{2\pi is}{r}\right]|u_s\rangle$$

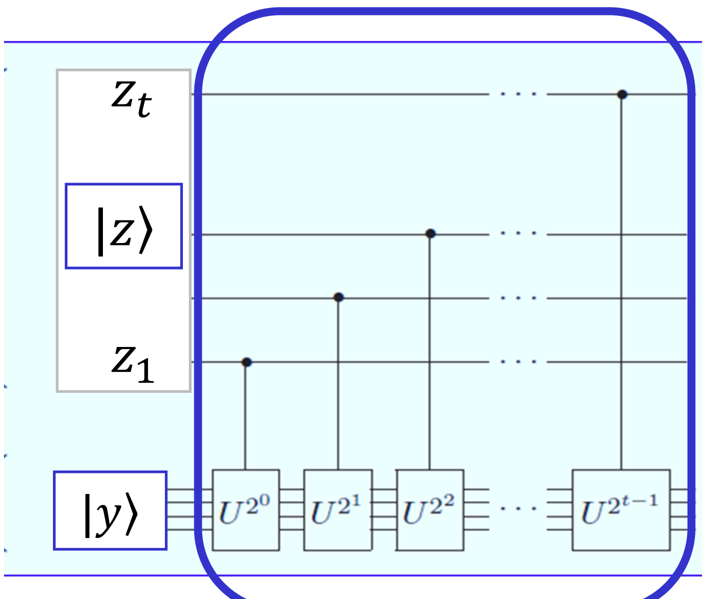
## ➢ 应用相位估计的另外两个要求：

❑ 实现受控$U^{2^j}$运算序列（篮筐内）：可用求模幂来整体实现！

为了简单，以输入态的一个分量为例来看这些运算的整体效果

$$
\begin{aligned}
|z\rangle|y\rangle \rightarrow & |z\rangle U^{z_t 2^{t-1}} \ldots U^{z_1 2^0}|y\rangle \\
= & |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y(\bmod N)\rangle \\
= & |z\rangle|x^z y(\bmod N)\rangle .
\end{aligned}
$$

$z$是整数，$z_i$是其（从右数）第 $i$ 比特



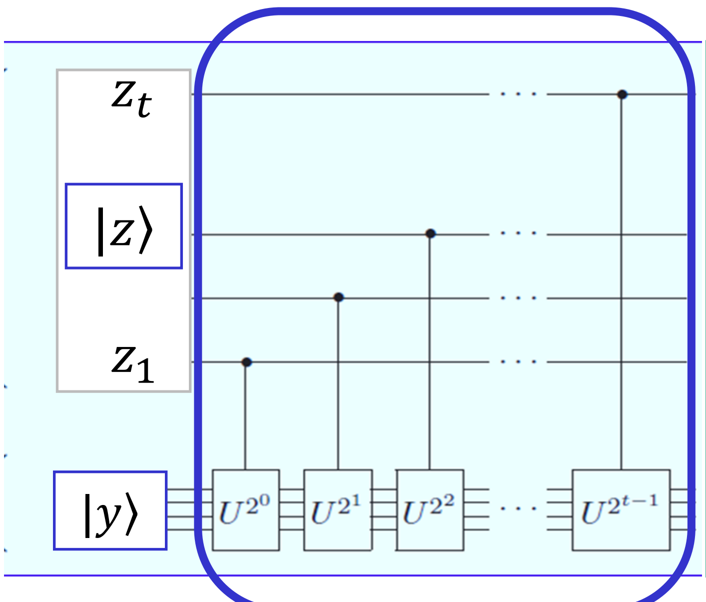
## ➢ 应用相位估计的另外两个要求：

❑ 实现受控$U^{2^j}$运算序列（篮筐内）：可用求模幂来整体实现！

大大降低实现复杂度
标准实现：$\Omega(N)$
求模幂：$O(\log^3 N)$

$$
\begin{aligned}
|z\rangle|y\rangle &\rightarrow |z\rangle U^{z_t 2^{t-1}} \ldots U^{z_1 2^0}|y\rangle \\
&= |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y(\bmod N)\rangle \\
&= |z\rangle|x^z y(\bmod N)\rangle.
\end{aligned}
$$

$z$是整数，$z_i$是其（从右数）第 $i$ 比特




1.模幂计算：$x^2\ (\bmod N), \cdots, x^{2^{t-1}}\ (\bmod N)$

2. $x^z\ (\bmod N) = x^{z_t 2^{t-1}}\ (\bmod N) \cdots x^{z_1 2^0}\ (\bmod N)$

3. 构造经典可逆线路$(z, y) \rightarrow \left(z, x^z y(\bmod N)\right)$，然后将其转换为量子线路$|z\rangle|y\rangle \rightarrow |z\rangle|x^z y(\bmod N)\rangle$

（注：不可逆变可逆、经典变量子，不提高复杂度）

## ➢ 应用相位估计的另外两个要求：

- ❑ 实现受控$U^{2^j}$运算序列（篮筐内）：可用求模幂来整体实现！

大大降低实现复杂度
标准实现：$\Omega(N)$
求模幂：$O(\log^3 N)$

$$
\begin{aligned}
|z\rangle|y\rangle \rightarrow & |z\rangle U^{z_t 2^{t-1}} \ldots U^{z_1 2^0}|y\rangle \\
= & |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y(\bmod N)\rangle \\
= & |z\rangle|x^z y(\bmod N)\rangle .
\end{aligned}
$$

- ❑ 制备本征态：不知道$r$，不能制备$|u_s\rangle$；但可制备其叠加态！

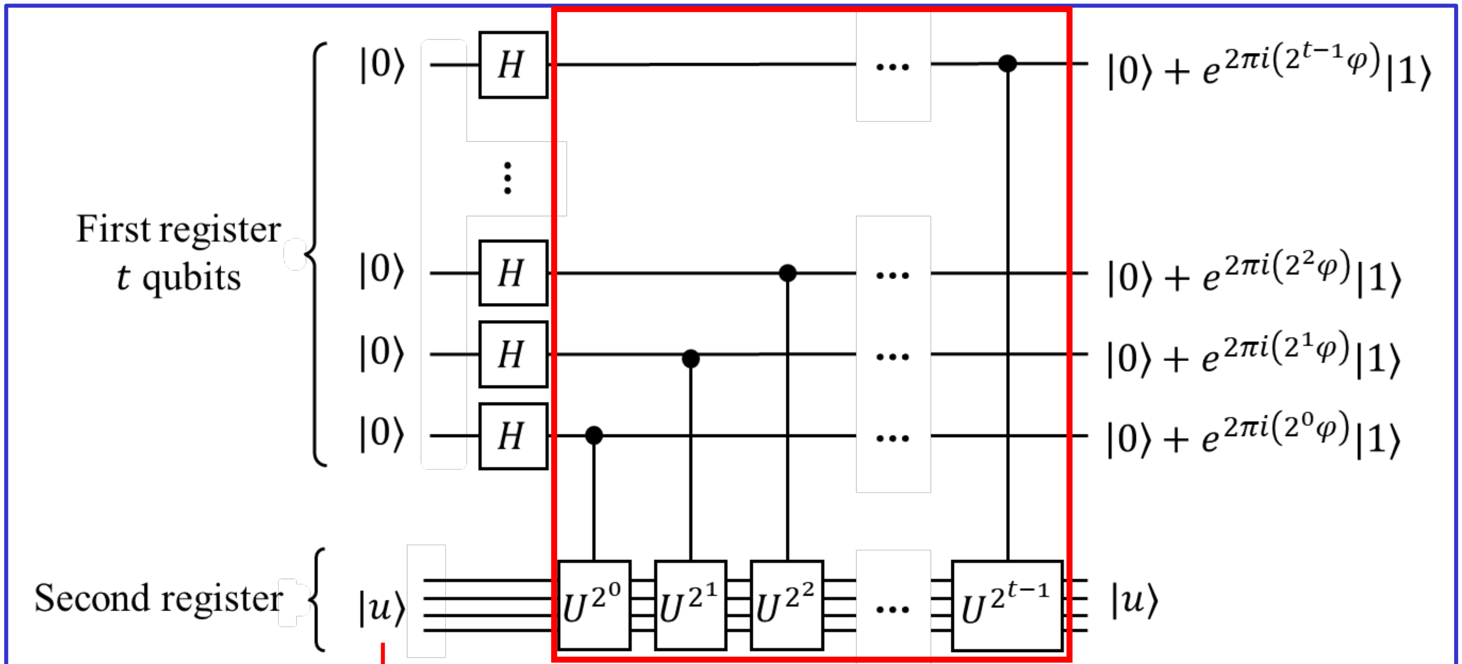
$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]|x^k \bmod N\rangle$$

$$= \frac{1}{r}\sum_{k=0}^{r-1}|x^k \bmod N\rangle\left(\sum_{s=0}^{r-1}\exp\left[\frac{-2\pi isk}{r}\right]\right) = \frac{1}{r}\sum_{k=0}^{r-1}|x^k \bmod N\rangle r\delta_{k,0} = |1\rangle$$

构造巧妙，所有$r$个本征态的均匀叠加正好是$|1\rangle$态！

最后随机测得某个$s$比$r$的值！

# 整体算法流程




逆F变换

$|00\ldots.01\rangle$

用模幂运算整体实现

简洁、漂亮！

$r$ 个特征向量对应的特征值分别为 $\exp\left[\frac{2\pi i s}{r}\right]$（$0 \le s \le r-1$），因此逆F变换后测量结果为某一个 $\frac{s}{r}$ 的近似值（小数），能否从中求出 $r$？

# 连分式算法：把小数还原成分数

- 用整数把有理数描述为如下形式

$$[a_0, \ldots, a_M] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_M}}}},$$

- 其中$a_0 \cdots a_M$是正整数（允许$a_0 = 0$），定义这个连分式的第$m$个渐进值$(0 \le m \le M)$为$[a_0 \cdots a_m]$

- 例：$\frac{427}{512}$的连分式展开

分子是测的值
分母是$2^t$

$$\frac{427}{512} = \frac{1}{\frac{512}{427}} = \frac{1}{1 + \frac{85}{427}} = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{2}{85}}} = \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{42 + \cfrac{1}{2}}}}$$

- 渐进值

$$1, \quad \frac{1}{1 + \frac{1}{5}} = \frac{5}{6}, \quad \frac{1}{1 + \frac{1}{5 + \frac{1}{42}}} = \frac{211}{253}$$

如上，$s/r$ 是这些渐进值之一，这些分母即为$r$的可能值或因子

# 辅助比特数$t$

如果结果达到一定精度（如下），则可以用连分式方法确定$r$：

定理：设$s/r$是一个使得$\left|\frac{s}{r}-\varphi\right| \le \frac{1}{2r^2}$的有理数，则$s/r$是$\varphi$的连分式的一个渐近值，计算连分式展开的复杂度为$O(L^3)$。

据上，估计 $\frac{s}{r}$ 的精度应达到 $\epsilon \le \frac{1}{2r^2}$。因为 $r$ 未知，而$r < N$，因此可取 $\epsilon = \frac{1}{2N^2}$

为了以至少$1-\eta$的成功概率得到精确到$n$比特（即精度$\epsilon = 2^{-n}$）的$\varphi$，初始化的量子比特数量$t$满足：

$$t = n + \left\lceil \log(2 + \frac{1}{2\eta}) \right\rceil$$

根据相位估计的误差分析，为了至少以$1-\eta$的成功概率得到误差不超过 $\epsilon$ 的 $\frac{s}{r}$，需要的辅助量子比特数为：

$$t = -\log\epsilon + \left\lceil \log\left(2 + \frac{1}{2\eta}\right) \right\rceil = \log 2N^2 + \left\lceil \log\left(2 + \frac{1}{2\eta}\right) \right\rceil$$
$$= 2\log N + 1 + \left\lceil \log\left(2 + \frac{1}{2\eta}\right) \right\rceil$$

# 整体算法流程

输入: (1)黑盒$U_{x,N}$：对$L$比特数$N$和与之互素的$x$执行$|j\rangle|k\rangle \rightarrow |j\rangle|x^j k \bmod N\rangle$；
(2) $t = 2L + 1 + \lceil log(2 + (2\eta)^{-1})\rceil$个初态为$|0\rangle$的Qubit；(3) L个初态为$|1\rangle$的Qubit

输出：$x$在mod$N$下的阶$r$；执行时间：$O(L^3)$个操作，成功概率$O(1)$

(1) $|0\rangle|1\rangle$ 初态：$t$个$|0\rangle$；后面是$|000\ldots.01\rangle$

(2) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle$ 产生叠加态

(3) $\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle$ 应用$U_{x,N}$

$$= \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{2\pi isj/r}|j\rangle|u_s\rangle$$

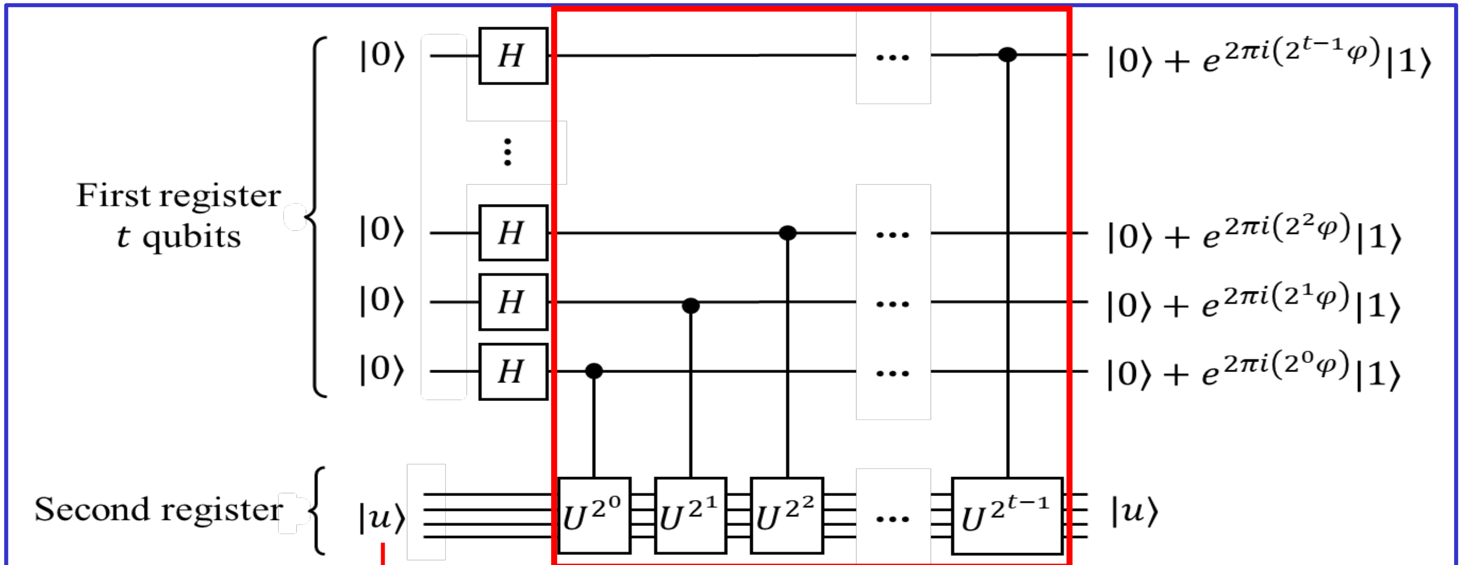
$$|x^j \bmod N\rangle = U^j|1\rangle = \frac{1}{\sqrt{r}}U^j\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp\left[\frac{2\pi isj}{r}\right]|u_s\rangle$$

(4) $\rightarrow\approx \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\widetilde{s/r}\rangle|u_s\rangle$ 对R1做逆傅里叶变换

(5) $\rightarrow \widetilde{s/r}$ 测R1

(6) $\rightarrow r$ 应用连分式算法

# 复杂度




逆F变换

$|00\ldots.01\rangle$

用模幂运算整体实现

- 整个量子线路的门数是 $O(L^3)$
  - ❑ Hadamard变换需要$O(L)$个门
  - ❑ 逆Fourier变换需要$O(L^2)$ 个门
  - ❑ 求模幂需要$O(L^3)$个门

$L = \lceil \log N \rceil$

- 求阶算法可能失败的情况
  - ❑ 相位估计的$s/r$不够准：通过扩大线路规模可忽略
  - ❑ $s$ 和 $r$可能有公因子：多试几次就好了，不影响复杂度

# 提纲

- Shor 算法
  - ❑ 量子Fourier变换
  - ❑ 相位估计
  - ❑ 求阶
  - ❑ 因子分解
- 实例和推广

# 因子分解

- 能求阶则可以求因子分解

随机选小于$N$-1的整数$x$，求其阶$r$

↓

大概率可得到 $y^2 = 1(\mathrm{mod} N)$的不平凡解

↓

得到$N$的因子

# 因子分解

➢ 能求阶则可以求因子分解

随机选小于$N$-1的整数$x$，求其阶$r$

↓

大概率可得到 $y^2=1(\mathrm{mod}N)$的不平凡解

↓

得到$N$的因子

一个随机选择与$N$互质的$x$很可能具有偶数的阶$r$使得$x^{r/2}\neq\pm1(\mathrm{mod}N)$，即$x^{r/2}(\mathrm{mod}\ N)$是$y^2=1(\mathrm{mod}N)$的一个不平凡解

定理: 设 $N=p_1^{\alpha_1}\ldots p_{1m}^{\alpha_m}$ 是一个正奇合数的素因子分解，$x$是在$[1,N-1]$内随机选出的整数，且$x$与$N$互质，令 $r$ 是 $x$ 模 $N$ 的阶，则

$$p\left(r\text{ 是偶数，且 }x^{r/2}\neq-1(\mathrm{mod}\ N)\right)\geq1-\frac{1}{2^m}$$

# 因子分解

➢ 能求阶则可以求因子分解

随机选小于$N$-1的整数$x$，求其阶$r$

⇩

大概率可得到 $y^2 = 1(\mathrm{mod}N)$的不平凡解

⇩

得到$N$的因子

如果能够找到方程$y^2 = 1(\mathrm{mod}\ N)$的一个不平凡解$y \neq \pm 1(\mathrm{mod}\ N)$，则可以计算出$N$的一个因子

因为 $y^2 = 1(\mathrm{mod}\ N)$，$N$必整除 $y^2 - 1 = (y+1)(y-1)$，因此 $N$ 与 $(y+1)$ 或者 $(y-1)$必有公因子。利用Euclid算法计算 $\gcd(y+1, N)$和 $\gcd(y-1, N)$，于是可以得到$N$的一个不平凡因子

# 算法流程

**Algorithm: Reduction of factoring to order-finding**

**Inputs:** A composite number $N$

**Outputs:** A non-trivial factor of $N$.

**Runtime:** $O((\log N)^3)$ operations. Succeeds with probability $O(1)$.

**Procedure:**

1. If $N$ is even, return the factor 2.
2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor $a$ 存在复杂度为$O((\log N)^3)$的经典算法
3. Randomly choose $x$ in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.
4. Use the order-finding subroutine to find the order $r$ of $x$ modulo $N$.
5. If $r$ is even and $x^{r/2} \neq -1 (\mathrm{mod}\ N)$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails.

# 提纲

- Shor 算法
  - 量子Fourier变换
  - 相位估计
  - 求阶
  - 因子分解
- 实例和推广

# 例：分解15

**盒子 5.4　以量子力学方式因子分解 15**

通过对 $N=15$ 分解因子，来说明利用求阶、相位估计和连分式展开的量子因子分解算法．首先，选择与 $N$ 没有公因子的一个随机数，假设选 $x=7$．接下来，我们用量子求阶算法计算 $x$ 相对 $N$ 的阶：从状态 $|0\rangle|1\rangle$ 开始，并通过应用 $t=11$，Hadamard 变换到第一寄存器产生状态

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|1\rangle=\frac{1}{\sqrt{2^t}}[|0\rangle+|1\rangle+|2\rangle+\cdots+|2^t-1\rangle]|1\rangle \qquad (5.61)$$

选择这样的 $t$，保证了误差概率 $\epsilon$ 至多为 1/4．然后，计算 $f(k)=x^k \bmod N$，并把结果放在第二寄存器中

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \bmod N\rangle \qquad (5.62)$$

$$=\frac{1}{\sqrt{2^t}}[|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle$$

$$+|4\rangle|1\rangle+|5\rangle|7\rangle+|6\rangle|4\rangle+\cdots]$$

# 例：分解15

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \bmod N\rangle \tag{5.62}$$

$$=\frac{1}{\sqrt{2^t}}[|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle$$

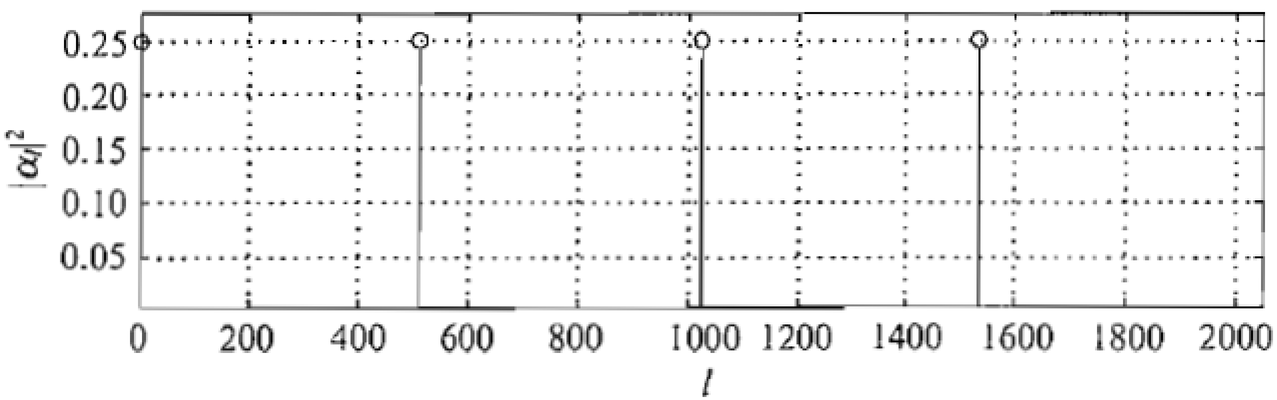
$$+|4\rangle|1\rangle+|5\rangle|7\rangle+|6\rangle|4\rangle+\cdots]$$

再应用逆 Fourier 变换 $FT^\dagger$ 到第一寄存器，并测量它. 分析所得结果分布的一个方法是，计算第一寄存器的约化概率密度函数，并对它应用 $FT^\dagger$，然后计算测量统计量. 不过，因为第二寄存器上没有进一步的运算，我们可以代之以应用隐含测量原理(4.4 节)，而假设第二寄存器也被测量，得到 1,7,4,13 的随机结果. 设我们得到 4(任何结果都可以)，这意味着输入到 $FT^\dagger$ 的状态应该是 $\sqrt{\frac{4}{2^t}}[|2\rangle+|6\rangle+|10\rangle+|14\rangle+\cdots]$. 应用 $FT^\dagger$ 后，我们对 $2^t=2048$ 绘出的概率分布如下图所示.

变化：测一下R2，以减少叠加项，简化运算

# 例：分解15

得到 4(任何结果都可以)，这意味着输入到 $FT^\dagger$ 的状态应该是 $\sqrt{\frac{4}{2^t}}[|2\rangle+|6\rangle+|10\rangle+|14\rangle+\cdots]$. 应用 $FT^\dagger$ 后，我们对 $2^t=2048$ 绘出的概率分布如下图所示.




得到某个状态 $\sum_l \alpha_l|l\rangle$. 最终测量于是以几乎恰好每个 1/4 的概率给出 0，512，1024 或 1536 中的一个结果. 假设我们得到 $l=1536$，那么计算连分式展开就给出 $1536/2048=1/(1+(1/3))$，这样 3/4 成为展开的一个渐近值，$r=4$ 就是 $x=7$ 的阶. 碰巧的是，$r$ 是偶数，且 $x^{r/2} \bmod N=7^2 \bmod 15=4\neq -1 \bmod 15$，于是算法奏效：计算最大公因子 $\gcd(x^2-1,15)=3$ 和 $\gcd(x^2+1,15)=5$ 给出 $15=3\times 5$.

# 总结

- 相位估计是对Shor算法的一种理解
  - ❑ 另一种理解：求模幂函数$f(z) = x^z \bmod N$ 的周期
- 推广
  - ❑ 定义域、值域是整数的周期函数的周期
  - ❑ 很多可归结为隐含子群问题的函数周期问题
    - Detsch
    - Simon
    - 求周期
    - 求阶
    - 离散对数
    - 置换的阶
    - 隐含线性函数
    - Abel稳定子
- 不能求解：非Abel群上的函数周期问题

Email: gaof@bupt.edu.cn
Tel:  86 -10 -62283192
Web: www.bupt.edu.cn

# 谢 谢！