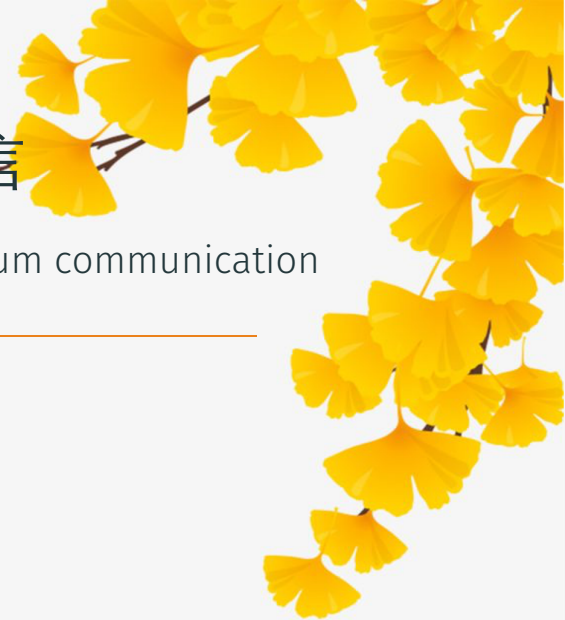
量子信息与量子通信

Quantum information and quantum communication

李小飞

光电科学与工程学院

2022 年 4 月 2 日



第 7 讲： 量子算法 (3)

Contents

求實求真
大氣大方

- 量子傅里叶变换是相位估计的关键
- 相位估计是许多量子算法的基础
- 比如：求本征值，大数质因式分解

- 酉变换与薛定谔方程等价

$$i\hbar\frac{d\left|\Psi\right\rangle}{dt}=H\left|\Psi\right\rangle$$

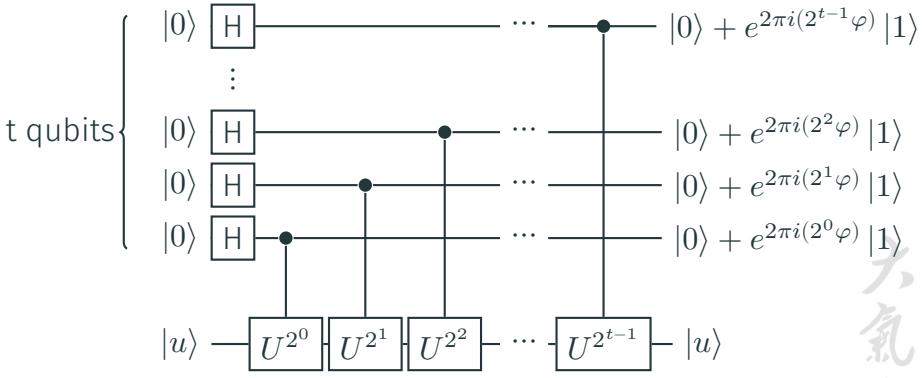
$$\left|\Psi'\right\rangle=U\left|\Psi\right\rangle$$

$$\left|\Psi(t_2)\right\rangle=U(t_1,t_2)\left|\Psi(t_2)\right\rangle$$

$$U(t_1,t_2)=exp[\frac{-iH(t_2-t_1)}{\hbar}]$$

- 设 U 有本征矢 $|u\rangle$, 对应本征值为 $exp(2\pi i\varphi)$
- 相位估计的目的是求 φ

1. 混合：把 $|u\rangle$ 的相位 φ 与 t 个叠加态混合成傅里叶乘积式
2. 反傅里叶变换得到 $\varphi_1\varphi_1\cdots\varphi_t$
3. 测量得到 φ


t qubits
$|0\rangle$
H
$|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^{2}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^{1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^{0}\varphi)}|1\rangle$
$|u\rangle$
U^{2^0}
U^{2^1}
U^{2^2}
$U^{2^{t-1}}$
$|u\rangle$

受控 U 门的做作用效果，作用到本征态 $|u\rangle$，得到本征值 $e^{2\pi i\varphi}$

- $|0\rangle U|u\rangle = |0\rangle|u\rangle$
- $|1\rangle U|u\rangle = |1\rangle e^{2\pi i\varphi}|u\rangle$

- 线路工作原理
  - $H|0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$
  - $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} U|u\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle|u\rangle + e^{2\pi i\varphi}|1\rangle|u\rangle) = \dfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\varphi}|1\rangle)|u\rangle$
  - $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} U^{2^n}|u\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^n\varphi)|1\rangle})|u\rangle$

- 混合之后，t-qubits 为：

$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{2\pi i(2^{t-1}\varphi)|1\rangle}][|0\rangle + e^{2\pi i(2^{t-2}\varphi)|1\rangle}]\cdots[|0\rangle + e^{2\pi i(2^0\varphi)|1\rangle}]$$

考虑到 φ 的二进制形式：

$$\varphi = 0.\varphi_1\varphi_2\cdots\varphi_t = \frac{\varphi_1}{2^1} + \frac{\varphi_2}{2^2} + \cdots + \frac{\varphi_t}{2^t}$$

$$2^{t-1}\varphi = \varphi_1\varphi_2\cdots\varphi_{t-1}.\varphi_t = 0.\varphi_t$$

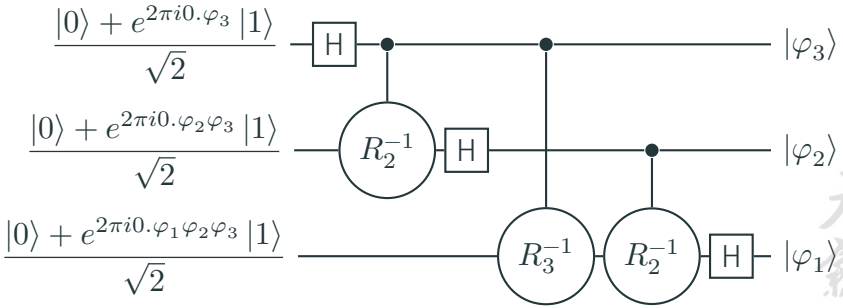
$$2^{t-2}\varphi = \varphi_1\varphi_2\cdots\varphi_{t-2}.\varphi_{t-1}\varphi_t = 0.\varphi_{t-1}\varphi_t$$

上式可写成

$$\frac{1}{\sqrt{2^t}}[|0\rangle + e^{2\pi i 0.\varphi_t)}\,|1\rangle][|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}\,|1\rangle]\cdots[|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}\,|1\rangle]$$

正是傅里叶变换乘积式!

以三量子比特线路为例:



- 第一个量子比特过 H 门
  - $\varphi_3 = 0;\quad \dfrac{|0\rangle + e^{2\pi i 0.\varphi_3}|1\rangle}{\sqrt{2}} = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}};\quad H\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} = |0\rangle = |\varphi_3\rangle$
  - $\varphi_3 = 1;\quad \dfrac{|0\rangle + e^{2\pi i/2}|1\rangle}{\sqrt{2}} = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}};\quad H\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} = |1\rangle = |\varphi_3\rangle$

总之

- $H\dfrac{|0\rangle + e^{2\pi i 0.\varphi_3}|1\rangle}{\sqrt{2}} = |\varphi_3\rangle$

- 第二个量子比特过四分之一反转门
  - $\varphi_3 = 0;\quad \dfrac{|0\rangle + e^{2\pi i 0.\varphi_2\varphi_3}|1\rangle}{\sqrt{2}} = \dfrac{|0\rangle + e^{2\pi i 0.\varphi_2}|1\rangle}{\sqrt{2}}$
  - $\varphi_3 = 1;\quad R_2^{-1}\dfrac{|0\rangle + e^{2\pi i 0.\varphi_2\varphi_3}|1\rangle}{\sqrt{2}} = \dfrac{|0\rangle + e^{2\pi i 0.\varphi_2}|1\rangle}{\sqrt{2}}$

再过 H 门

- $H\dfrac{|0\rangle + e^{2\pi i 0.\varphi_2}|1\rangle}{\sqrt{2}} = |\varphi_2\rangle$

- 第三个量子比特过八分之一反转门

$$R_3^{-1}\frac{|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\varphi_3}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2}|1\rangle}{\sqrt{2}}$$

过四分之一反转门

$$R_2^{-1}\frac{|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i 0.\varphi_1}|1\rangle}{\sqrt{2}}$$

再过 H 门

$$H\frac{|0\rangle + e^{2\pi i 0.\varphi_1}|1\rangle}{\sqrt{2}} = |\varphi_1\rangle$$

- 测量 $|\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle$

获得相位 $\varphi = 0.\varphi_1\varphi_2\varphi_3$

对于本征态，相位估计完成如下映射:

$$|0\rangle |u_k\rangle \to F[|\varphi_k\rangle] |u_k\rangle$$

对于任意态，有展开式

$$\Psi = \sum_k \alpha_k |u_k\rangle$$

相位估计完成映射

$$|0\rangle \Psi = \sum_k \alpha_k |0\rangle |u_k\rangle \to \sum_k \alpha_k F[|\varphi_k\rangle] |u_k\rangle$$

基此，可得到每一个本态的相位 φ_k, 及本征值 $e^{2\pi i \varphi_k}$

例-试问，下面这个数能不能做质因式分解:

$$N = 39772916239307209103$$

解: (1) 求 $\sqrt{N}$, 并取整 $P = [\sqrt{N}]$

(2) 求 N/P, 并取整 $Q = [N/P]$

(3) 扫描 1-min(P,Q) 之间的所有质数，判断是否存在两个质数 p, q, 有

$$p \times q = N$$

工作量指数增长，当 N 很大时，目前的计算机就很难完成。

相反，当我们知道 $p = 6257493337$ 时，就很容易验证 $q = 6356046119$

现化的密码学就是基于这个原理设计的。

量子算法，可以有效进行大数质因式分解，从而破解现有密码。
基本思想为求阶!

阶的定义

对于正整数 x 和 N $(x \leq N)$, 无公因子。则 x 模 N 有阶 r 定义为使

$$x^r = 1(modN)$$

成立的最小正整数。

例-试求 x=11 和 N=21 的阶 r:

解:(1) 取 $r = 1, 2, 3, \cdots$, 依次计算 11^r

(2) 依次计算 $\frac{11^r}{21}$ 的余数

(3) 第一个余数为 1 的 r=6，得解

左表表明，阶就是余子式（完全集）的自由度

r	x^r(x=11)	x^r mod 21
0	1	1
1	11	11
2	121	16
3	1331	8
4	14641	4
5	161051	2
6	1771561	1
7	19487171	11
8	214358881	16
9	2357947691	8
10	25937424601	4
11	2.85312E+11	2
12	3.13843E+12	1
13	3.45227E+13	11

例-试证明求阶问题与因式分解问题等价:

证明:设 N 可以作因子分解 $N = n_1 \times n_2$ 若阶 r 为偶数，有

$$x^r = 1(modN)$$

$$x^r - 1 = M \times N$$

$$(x^{r/2} - 1)(x^{r/2} + 1) = M \times N = M \times n_1 \times n_2$$

上式表明，求最大公约数

$$gcd(x^{r/2} - 1, N); \quad gcd(x^{r/2} + 1, N)$$

很可能就能得到因子 n_1 和 n_2
因此，因式分解问题就转化求阶问题，它们是等价的!

- 阶 r 就是余子式（完全集）的自由度。
- 量子傅里叶变换公式中，N 就是基矢数目

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

- 量子力学表明这个数目就是体系的自由度，即上式可取 $N = r$

余子式 $\{|x^k \ mod \ N\rangle\}$ 构成完全集，任意态函数可在其上展开，比如本征态 S

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk} |x^k \ mod \ N\rangle$$

对上式做傅里叶逆变换

$$\left|x^k \ mod \ N\right\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-i\frac{2\pi}{r}sk} \left|u_s\right\rangle$$

取 k=0，得到余子式 1 态在量子本征函数系 $\{|u_s\rangle\}$ 的展开式

$$\left|x^0 \ mod \ N\right\rangle = \sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} \left|u_s\right\rangle = \sum_{s=0}^{r-1} a_s \left|u_s\right\rangle$$

其振幅 (展开系数)$a_s = \frac{1}{\sqrt{r}}$, 完全由阶 (r) 决定!

u_s 的本征值

试证明相位估计算子 U 的本征态 u_s 的本征值为 $\exp[i2\pi\varphi] = \exp[i2\pi\frac{s}{r}]$

即要证明其本征方程为:

$$U\left|u_s\right\rangle = \exp[i2\pi\frac{s}{r}]\left|u_s\right\rangle$$

证明：相位估计算子 U 在余子式有如下作用效果

$$U\left|y\right\rangle = \left|xy \mod N\right\rangle$$

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}\left|x^k \mod N\right\rangle$$

$$\begin{aligned} U\left|u_s\right\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}U\left|x^k \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}\left|x^{k+1} \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k'=1}^{r} e^{-i\frac{2\pi}{r}s(k'-1)}\left|x^{k'} \mod N\right\rangle \end{aligned}$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i\frac{2\pi}{r}sr} \left| x^{r} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i2\pi s} \left| x^{0} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=0}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle$$

$$= \exp[i2\pi\frac{s}{r}] \left| u_s \right\rangle$$

证毕!

$$U\left|u_s\right\rangle = \exp[i2\pi\frac{s}{r}]\left|u_s\right\rangle = \exp[i2\pi\varphi]\left|u_s\right\rangle$$

因此

$$\varphi = \frac{s}{r}$$

φ 可通过傅里叶逆变换求得，则阶 r 可通过连分数算法求得

$$S_n = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}} \qquad \pi = \cfrac{1}{3 + \cfrac{1}{7 + \cfrac{1}{15 + \dots}}}$$

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}}}$$

$\frac{1}{1}$ $\frac{3}{2}$ $\frac{7}{5}$ $\frac{17}{12}$

- 有理数的连分数表示是有限的
- 任一有理数的连分数表示是唯一的
- “简单”有理数的连分数表示是简短的

(1) 给出 Grover 算法量子线路

(2) 推导算法过程

Thanks for your attention!

A & Q