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 3 月 10 月







1. 相位估计

2. 求本征值

3. 大数质因式分解



□ 相位估计

- 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

六氯六羟

≠ 相位估计的目的

■ 酉变换与薛定谔方程等价

$$\begin{split} i\hbar\frac{d\left|\Psi\right\rangle}{dt} &= H\left|\Psi\right\rangle\\ \left|\Psi'\right\rangle &= U\left|\Psi\right\rangle\\ \left|\Psi(t_2)\right\rangle &= U(t_1,t_2)\left|\Psi(t_2)\right\rangle\\ U(t_1,t_2) &= exp[\frac{-iH(t_2-t_1)}{\hbar}] \end{split}$$

- $lacksymbol{lack}$ 设 $lacksymbol{lack}$ 有本征矢 |u
 angle, 对应本征值为 $exp(2\pi iarphi)$
- ullet 相位估计的目的是求 arphi

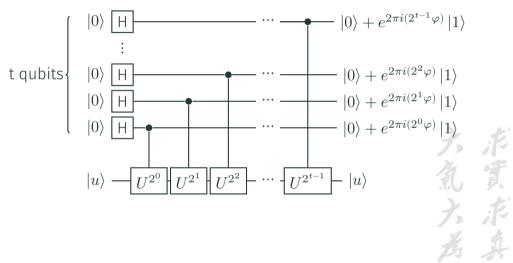


≠ 相位估计三步走

- 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. 反傳里叶变换得到 $\varphi_1\varphi_1 \cdots \varphi_t$
- 3. 测量得到 φ



□ 混合量子线路





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

$$\cdot |0\rangle U |u\rangle = |0\rangle |u\rangle$$

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

• 线路工作原理

$$H |0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}U|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle |u\rangle + e^{2\pi i\varphi} |1\rangle |u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i\varphi} |1\rangle)|u\rangle$$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} U^{2^n} |u\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i (2^n \varphi)|1\rangle}) |u\rangle$$



● 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:

$$\begin{split} \varphi &= 0.\varphi_1\varphi_2\cdots\varphi_t = \frac{\varphi_1}{2^1} + \frac{\varphi_2}{2^2} + \cdots + \frac{\varphi_t}{2^t} \\ 2^{t-1}\varphi &= \varphi_1\varphi_2\cdots\varphi_{t-1}.\varphi_t = 0.\varphi_t \\ 2^{t-2}\varphi &= \varphi_1\varphi_2\cdots\varphi_{t-2}.\varphi_{t-1}\varphi_t = 0.\varphi_{t-1}\varphi_t \end{split}$$

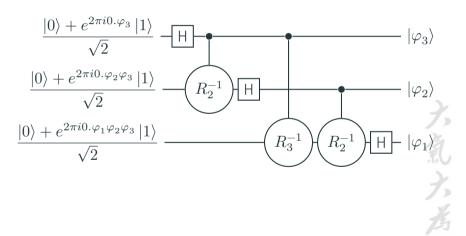
上式可写成

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

正是傅里叶变换乘积式!

≠ 傅里叶反变换

以三量子比特线路为例:





● 第一个量子比特过 H 门

$$\varphi_3 = 0; \quad \frac{|0\rangle + e^{2\pi i 0.\varphi_3} |1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H\frac{|0\rangle + |1\rangle}{\sqrt{2}} = |0\rangle = |\varphi_3\rangle$$

$$\varphi_3 = 1; \quad \frac{\sqrt{2}}{\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2}}; \quad H = \frac{\sqrt{2}}{\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2}}; \quad H = \frac{\sqrt{2}}{\sqrt{2}} = |1\rangle = |\varphi_3\rangle$$

惡之

$$\cdot \ H \frac{|0\rangle + e^{2\pi i 0.\varphi_3} \, |1\rangle}{\sqrt{2}} = |\varphi_3\rangle$$



● 第二个量子比特过四分之一反转门

$$\varphi_{3} = 0; \quad \frac{|0\rangle + e^{2\pi i 0.\varphi_{2}\varphi_{3}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i 0.\varphi_{2}}|1\rangle}{\sqrt{2}}$$
$$\varphi_{3} = 1; \quad R_{2}^{-1} \frac{|0\rangle + e^{2\pi i 0.\varphi_{2}\varphi_{3}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i 0.\varphi_{2}}|1\rangle}{\sqrt{2}}$$

再过日门

$$\cdot \ H \frac{|0\rangle + e^{2\pi i 0.\varphi_2} \, |1\rangle}{\sqrt{2}} = |\varphi_2\rangle$$



● 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 $\varphi = 0.\varphi_1\varphi_2\varphi_3$

六乳六鸡



1. 相位估计

2. 求本征值

3. 大数质因式分解



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

$$\Psi = \sum_{k} \alpha_k \left| u_k \right\rangle$$

相位估计完成映射

$$\left|0\right\rangle \Psi = \sum_{k} \alpha_{k} \left|0\right\rangle \left|u_{k}\right\rangle \rightarrow \sum_{k} \alpha_{k} F[\left|\varphi_{k}\right\rangle] \left|u_{k}\right\rangle$$

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







1. 相位估计

2. 求本征值

3. 大数质因式分解



╱ 因数分解

● 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。

♬ 阶的定义

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 \times 和 N $(x \le N)$, 无公因子。则 \times 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

$$x^r = 1 (mod N)$$

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

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

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!





≠ 量子求阶

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

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

对上式做傅里叶逆变换

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

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

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

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



♦ u。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:

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



证明: 相位估计算子 U 在余子式有如下作用效果

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

$$\begin{split} &= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^r e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle \\ &= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i\frac{2\pi}{r}sr} \left| x^r \mod N \right\rangle \\ &= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i2\pi s} \left| x^0 \mod N \right\rangle \\ &= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle \\ &= \exp[i2\pi \frac{s}{r}] \left| u_s \right\rangle \\$$
 延毕!

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

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



□ 连分数算法

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

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}}}} \qquad \frac{1}{1} \quad \frac{3}{2} \quad \frac{7}{5} \quad \frac{1}{1}$$

- 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







Thanks for your attention!

A & Q

