



北京邮电大学

第8讲 量子线性方程组求解算法

高 飞

网络空间安全学院





➤ 量子线性方程组求解算法

- 问题描述

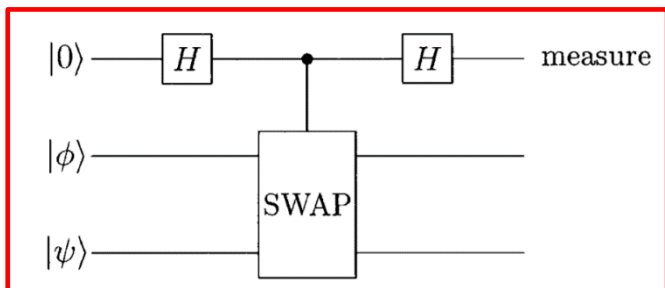
- HHL 算法

- 复杂度分析和参数讨论

- 问题：找出满足线性方程组 $A\vec{x} = \vec{b}$ 的向量 \vec{x}
- 不同：输出结果是量子态 $|x\rangle$ ，也即 \vec{x} 的归一化向量对应的量子态
 - 如果要算出解向量 \vec{x} ，则将失去加速效果
 - 先对 $|x\rangle$ 做层析，得到解 \vec{x} 的归一化后的向量
 - 再选 A 的某些行和 $|x\rangle$ 层析后所得向量作内积，并和 \vec{b} 相应值作比较，得到归一化系数
 - 量子态形式解 $|x\rangle$ 的用途
 - 若需要的是输出结果的全局信息，此时可直接从输出量子态中提取
 - 可以作为子程序嵌入到其他量子算法中，如数据拟合和支持向量机[1][2]
 - 应用举例：验证两个随机过程 $\vec{x}_t = A\vec{x}_{t-1} + \vec{b}$ 和 $\vec{x}'_t = A'\vec{x}'_{t-1} + \vec{b}'$ 是否具有相同的稳定态

解 $|x\rangle = (I - A)^{-1}|b\rangle$ 和 $|x'\rangle = (I - A')^{-1}|b'\rangle$ ，然后用 Swap-test 可以快速判断 $|x\rangle$ 和 $|x'\rangle$ 是否相同（量子解即可，具有指数加速效果）

- 给定多份量子态 $|\phi\rangle$ 、 $|\psi\rangle$ ，如何判断这两个量子态的接近程度（或者说，如何计算两个量子态的内积）？



$$|0\rangle|\phi\rangle|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\phi\rangle|\psi\rangle$$

$$\rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\phi\rangle|\psi\rangle + |1\rangle|\psi\rangle|\phi\rangle)$$

$$\rightarrow \frac{1}{2}(|0\rangle|\phi\rangle|\psi\rangle + |1\rangle|\phi\rangle|\psi\rangle + |0\rangle|\psi\rangle|\phi\rangle - |1\rangle|\psi\rangle|\phi\rangle)$$

$$= \frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$$

➤ Swap-test 结果

- ❑ 测量结果为0的概率 $\frac{1}{4}(2 + 2|\langle\phi|\psi\rangle|^2) = \frac{1}{2} + \frac{1}{2}|\langle\phi|\psi\rangle|^2$ ，输入态相同时为100%
- ❑ 执行多次Swap-test，估计测到0的概率，进而可求得两个态的内积（的模）
 - 复杂度为 $O(1/\epsilon^2)$ ，即需要重复执行 $O(1/\epsilon^2)$ 次Swap-test
 - 注：一定是多份态才能执行多次test，不能一份态重复执行



➤ 量子线性方程组求解算法

- 问题描述

- HHL 算法

- 复杂度分析和参数讨论

Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth., Quantum algorithm for solving linear systems of equations, Physical Review Letters. 103 (15): 150502, 2009

➤ 态 $|b\rangle = \sum_{j=1}^N b_j |j\rangle$ (b_j 为 \vec{b} 归一化后的第 j 个元素) 能被有效制备

□ 有效: 对于 N 维 (即 $n = \log N$ 比特) 量子态, 制备复杂度为 $O(\text{poly } \log N)$

□ 一般态并不能有效制备: 用 QRAM 制备量子态, 复杂度为 $O(\text{poly } N)$

QRAM[1]: 如果 b_i 以经典信息的形式存储在特定结构的寄存器中, QRAM 可以实现

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |b_i\rangle$$

如果想制备量子态 $\frac{1}{\sqrt{B}} \sum_{i=0}^{N-1} b_i |i\rangle$, 需要先进行 QRAM, 再进行受控旋转, 然后测量[2], 即:

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle |0\rangle \xrightarrow{\text{QRAM}} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |b_i\rangle |0\rangle \xrightarrow{\text{CR}} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |b_i\rangle (\sqrt{1 - c^2 b_i^2} |0\rangle + c b_i |1\rangle)$$

c : 满足下式的常数
 $c * \max(|b_i|) \leq 1$

$$\xrightarrow{\text{测量第三寄存器, 结果为1}} \frac{1}{\sqrt{B}} \sum_{i=0}^{N-1} b_i |i\rangle |b_i\rangle \xrightarrow{\text{逆QRAM}} \frac{1}{\sqrt{B}} \sum_{i=0}^{N-1} b_i |i\rangle$$

$\frac{1}{\sqrt{B}}$ 为归一化系数,
若 b_i 本身是已经归一化的, 则 $B=1$

[1] V. Giovannetti, S. Lloyd, L. Maccone, Phys. Rev. Lett. 100, 160501 (2008).

[2] Anupam Prakash, Quantum Algorithms for Linear Algebra and Machine Learning.



➤ 态 $|b\rangle = \sum_{j=1}^N b_j |j\rangle$ (b_j 为 \vec{b} 归一化后的第 j 个元素) 能被有效制备

□ 有效: 对于 N 维 (即 $n = \log N$ 比特) 量子态, 制备复杂度为 $O(\text{poly } \log N)$

□ 一般态并不能有效制备: 用 QRAM 制备量子态, 复杂度为 $O(\text{poly } N)$

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |0\rangle |0\rangle \xrightarrow{\text{QRAM}} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |b_i\rangle |0\rangle \xrightarrow{\text{CR}} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |b_i\rangle (\sqrt{1 - c^2 b_i^2} |0\rangle + c b_i |1\rangle)$$

$O(\log N)$

测量第三寄存器, 结果为 1

$$\xrightarrow{\text{测量第三寄存器, 结果为 1}} \frac{1}{\sqrt{B}} \sum_{i=0}^{N-1} b_i |i\rangle |b_i\rangle \xrightarrow{\text{逆 QRAM}} \frac{1}{\sqrt{B}} \sum_{i=0}^{N-1} b_i |i\rangle$$

$O(a)$, a 为 b_i 的比特数, 可认为是常数

□ 为使测到 $|1\rangle$ 的概率尽可能大 (降低复杂度), c 可取 $1/\max(|b_i|)$ 。测量结果为 $|1\rangle$ 的概率为 $p(1) = \sum_i \frac{c^2 |b_i|^2}{N} = \frac{c^2 B}{N (\max |b_i|)^2} \leq \frac{B}{N (\max |b_i|)^2}$, 对应算法复杂度为 $O(\frac{N (\max |b_i|)^2}{B} \log N)$

● 如果 b_i 均匀 [振幅主要分布在 CN 个分量上 (C 为常数), 即对这些分量振幅 b_j , 有

$|b_j| = \Theta(\max |b_i|)$, 其它分量接近 0], 此时 $\frac{B}{N (\max |b_i|)^2} \leq \frac{CN (\max |b_i|)^2}{N (\max |b_i|)^2} = C$, 因此需测次数为 $O(1)$, 算法整体复杂度 $O(\log N)$

● 如果 b_i 不均匀 (振幅主要分布在常数 C 个分量上), 则测得 $|1\rangle$ 的概率为

$\frac{B}{N (\max |b_i|)^2} \leq \frac{C (\max |b_i|)^2}{N (\max |b_i|)^2} = \frac{C}{N}$, 需测 $\frac{N}{C}$ 次, 整体复杂度 $O(N \log N)$ (不考虑幅度放大)



定理^[1]: 令 $\theta \in [0,1)$, $\tilde{\theta}$ 是 θ 的 d 比特有限精度表示, 则存在酉矩阵 U_θ , 满足:

$$U_\theta: |\tilde{\theta}\rangle|0\rangle \rightarrow |\tilde{\theta}\rangle(\cos 2\pi\tilde{\theta}|0\rangle + \sin 2\pi\tilde{\theta}|1\rangle)$$

具体实现: $U_\theta = \sum_{\tilde{\theta} \in \{0,1\}^d} |\tilde{\theta}\rangle\langle\tilde{\theta}| \otimes \exp(-i2\pi\tilde{\theta}\sigma_y)$, 其中

绕Y轴旋转 $2\pi\tilde{\theta}$ 角

$$\exp(-i\gamma\sigma_y) = \begin{pmatrix} \cos \gamma & -\sin \gamma \\ \sin \gamma & \cos \gamma \end{pmatrix}$$

复杂度: 实现 U_θ 需 (以 $\tilde{\theta}$ 的每个比特 $\tilde{\theta}_k$ 做控制位) 执行 d 个受控 $\exp(-i2\pi 2^{-k}\sigma_y)$, $k = 1, 2, \dots, d$ 。受控单比特旋转门复杂度是 $O(1)$, 因此 U_θ 的复杂度为 $O(d)$ 。

$$\text{比特表示: } \tilde{\theta} = 0.\tilde{\theta}_1\tilde{\theta}_2\cdots\tilde{\theta}_{d-1}\tilde{\theta}_d = \tilde{\theta}_12^{-1} + \tilde{\theta}_22^{-2} + \cdots \tilde{\theta}_{d-1}2^{-d+1} + \tilde{\theta}_d2^{-d}$$

想让概率幅变为 $\tilde{\theta}$ 的其它实函数 (而不是 \sin) 行不行? 可以!

$$\text{若取 } \gamma = \arcsin cf(\tilde{\theta}), \text{ 可以实现 } |\tilde{\theta}\rangle|0\rangle \rightarrow |\tilde{\theta}\rangle(\sqrt{1 - c^2 f(\tilde{\theta})^2}|0\rangle + cf(\tilde{\theta})|1\rangle)$$

注: 由于 $|f(\tilde{\theta})|$ 可能大于 1, 一般需要加实常数 c 使 $c * \max[|f(\tilde{\theta})|] \leq 1$

前提假设: 1. 要求实函数 f 可有效计算; 2. 知道 $\max[|f(\tilde{\theta})|]$ 的大概范围 (应用时需特别注意)

[1] Dervovic D, et al. Quantum linear systems algorithms: a primer[J]. arXiv preprint arXiv:1802.08227, 2018. [2]

Iris Cong and Luming Duan 2016 New J. Phys. 18 073011

文献[2]给出另一种实现受控旋转的方式



➤ 态 $|b\rangle = \sum_{j=1}^N b_j |j\rangle$ (b_j 为 \vec{b} 归一化后的第 j 个元素) 能被有效制备

前提: b_j 较均匀; 或 $|b\rangle$ 本来就量子态形式给出

➤ A 是稀疏的厄米矩阵

□ 厄米: 若 A 不是厄米的, 可将解 $A\vec{x} = \vec{b}$ 转化为系数矩阵为厄米的情形

构造新方程组: 1.其系数矩阵是厄米的;
2.其解包含我们想要解

$$\begin{bmatrix} 0 & A \\ A^\dagger & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \vec{x} \end{bmatrix} = \begin{bmatrix} \vec{b} \\ 0 \end{bmatrix}$$

□ 稀疏: 关于稀疏的假设并非必要

- 算法用到量子模拟, 之前只能有效模拟稀疏矩阵 (有效: 对 N 维矩阵, 模拟复杂度为 $O(\text{poly log } N)$)
- 现在, 某些类型的非稀疏矩阵也可以进行量子模拟
- 只要可进行有效模拟, 就能用该算法求解线性方程组

□ 矩阵元素读取: 通过访问矩阵元素的、矩阵非零元素位置的两个 Oracle 来实现



➤ 态 $|b\rangle = \sum_{j=1}^N b_j |j\rangle$ (b_j 为 \vec{b} 归一化后的第 j 个元素) 能被有效制备

➤ A 是稀疏的厄米矩阵

注：等于0时 A 是奇异矩阵，方程组没有唯一解
 κ 是 A 的条件数，即 $\kappa = \text{最大奇异值} / \text{最小奇异值}$

➤ A 的特征值 λ_j 满足 $|\lambda_j|_{\max} = 1, |\lambda_j|_{\min} \neq 0$, 且 κ 已知。此时 $\lambda_j^2 \in \left[\frac{1}{\kappa^2}, 1\right]$

□ 方阵的谱（特征）分解：若 $B \in C^{N \times N}$ 是正规矩阵，则可特征分解

$$B = \sum_{j=1}^N \lambda_j u_j u_j^\dagger$$

正规矩阵： $A^\dagger A = A A^\dagger$

其中 $\lambda_j, u_j, j = 1, 2, \dots, N$ 分别为矩阵 A 的特征值和特征向量。

□ 矩阵奇异值：设 $A \in C_r^{m \times n}$ ，且 $A^\dagger A$ 的特征值为

$$\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_r > \gamma_{r+1} = \dots = \gamma_m = 0$$

$A^\dagger A$ 为半正定算子，
特征值是 ≥ 0 的实数

称 $\sigma_i = \sqrt{\gamma_i}$ ($i = 1, 2, \dots, m$)为矩阵 A 的奇异值(r 是 A 的秩)。

□ 若 A 是厄米矩阵，则可特征分解 $A = \sum_{j=1}^N \lambda_j u_j u_j^\dagger$ ， $A^\dagger A$ 的特征值为 $|\lambda_j|^2$ ，因此 A 的奇异值等于 $|\lambda_j|$ 。此时 $\kappa = \text{最大奇异值} / \text{最小奇异值} = |\lambda|_{\max} / |\lambda|_{\min}$

- 态 $|b\rangle = \sum_{j=1}^N b_j |j\rangle$ (b_j 为 \vec{b} 归一化后的第 j 个元素) 能被有效制备
- A 是稀疏的厄米矩阵
- A 的特征值 λ_j 满足 $|\lambda_j|_{\max} = 1, |\lambda_j|_{\min} \neq 0$, 且 κ 已知。此时 $\lambda_j^2 \in \left[\frac{1}{\kappa^2}, 1\right]$
 - 这个假设和相位估计有关 (后面讨论)
 - 若不满足 $|\lambda_j|_{\max} = 1$, 可用 $|\lambda|_{\max}$ 做预处理, 即把 $A/|\lambda|_{\max}$ 做输入矩阵
 - 若已知 $|\lambda|_{\max}$, 预处理可在读取矩阵元素时进行, 不影响算法复杂度
 - 若未知 $|\lambda|_{\max}$, 需要估计其值 (后面讨论估计有误差时对算法的影响)
 - 直接的想法: 求 $A^\dagger A$ 对角线元素之和作为 $|\lambda|_{\max}^2$ 的上界(Schur不等式)[1]:

$$|\lambda|_{\max}^2 \leq \sum_i |\lambda_i|^2 \leq \text{tr}(A^\dagger A) = \sum_{i,j} A_{ij}^2$$

但该方法需要 $O(N^2)$ 次加法和 N^2 次乘法, 复杂度太高, 因此并不可行

[1] 程云鹏, 张凯院, 徐仲, 《矩阵论》, 西北工业大学出版社。

厄米矩阵 A 谱分解: $A = \sum_{j=1}^N \lambda_j |u_j\rangle\langle u_j|$, 设 $|b\rangle$ 在 A 的特征空间展开为 $\sum_j \beta_j |u_j\rangle$, 则

$$|x\rangle = cA^{-1}|b\rangle = c \sum_{j=1}^N \frac{1}{\lambda_j} |u_j\rangle\langle u_j| \sum_j \beta_j |u_j\rangle = c \sum_{j=1}^N \beta_j / \lambda_j |u_j\rangle$$

(A 非酉, 所以有归一化系数 c , 对算法无影响)

目标: 把 A 的特征值 λ_j 放到 $|b\rangle$ 的各项概率幅的分母上

量子模拟: 处理(厄米)矩阵数据的常见方法

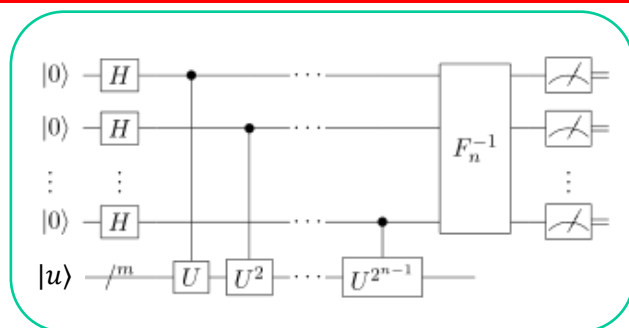
观察 $e^{iAt} = \sum_{j=1}^N e^{i\lambda_j t} |u_j\rangle\langle u_j|$: λ_j 是酉算子 e^{iAt} 特征值的相位! (t 是常数)

量子模拟+相位估计: 常被用来处理与(厄米)矩阵特征值相关的计算

回顾: 相位估计

酉操作 U : $U|u\rangle = e^{2\pi i \phi_u} |u\rangle$

初态: $\sum_u c_u |u\rangle$ 利用 U , 相位估计 $\rightarrow \sum_u c_u |\tilde{\phi}_u\rangle |u\rangle$



HHL算法中: U 对应 $e^{iAt_0} = \sum_j e^{i\lambda_j t_0} |u_j\rangle\langle u_j|$, $\sum_u c_u |u\rangle$ 对应 $|b\rangle = \sum_j \beta_j |u_j\rangle$

易验证 u_j 是本征态: $U|u_j\rangle = \sum_{j'} e^{i\lambda_{j'} t_0} |u_{j'}\rangle\langle u_{j'}||u_j\rangle = e^{i\lambda_j t_0} |u_j\rangle$

厄米矩阵 A 谱分解: $A = \sum_{j=1}^N \lambda_j |u_j\rangle\langle u_j|$, 设 $|b\rangle$ 在 A 的特征空间展开为 $\sum_j \beta_j |u_j\rangle$, 则

$$|x\rangle = cA^{-1}|b\rangle = c \sum_{j=1}^N 1/\lambda_j |u_j\rangle\langle u_j| \sum_j \beta_j |u_j\rangle = c \sum_{j=1}^N \beta_j / \lambda_j |u_j\rangle$$

(A 非酉, 所以有归一化系数 c , 对算法无影响)

目标: 把 A 的特征值 λ_j 放到 $|b\rangle$ 的各项概率幅的分母上

量子模拟: 处理(厄米)矩阵数据的常见方法

观察 $e^{iAt} = \sum_{j=1}^N e^{i\lambda_j t} |u_j\rangle\langle u_j|$: λ_j 是酉算子 e^{iAt} 特征值的相位! (t 是常数)

量子模拟+相位估计: 常被用来处理与(厄米)矩阵特征值相关的计算

(1) 相位估计: 在 $|b\rangle$ 上做酉算子 e^{iAt} (量子模拟) 的相位估计, 将 λ_j 放到qubit值上, 得

$$\sum_j \beta_j \left| \frac{\tilde{\lambda}_j t}{2\pi} \right\rangle |u_j\rangle$$

$|b\rangle$ 是 A 本征态的叠加
可实现 $U \rightarrow$ 可实现受控 U (见后)

(2) 受控旋转: 将qubit值上的 λ_j 放到各项概率幅的分母上, 得下式, 即方程组的解

$$c \sum_{j=1}^N \beta_j / \tilde{\lambda}_j |u_j\rangle$$



1. 制备初态 $H^{\otimes m}|0^{\otimes m}\rangle \otimes |b\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle \otimes (\sum_j \beta_j |u_j\rangle)$
2. 做相位估计：U用稀疏Hamiltonian模拟 $e^{iAt_0} = \sum_{j=1} e^{i\lambda_j t_0} |u_j\rangle\langle u_j|$ 实现（从U到受控U在下页讨论），得量子态

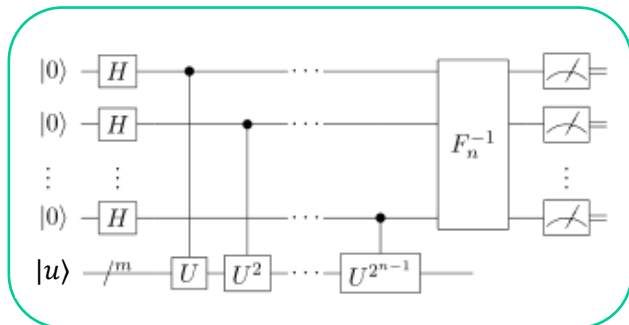
$$\approx \sum_{j=1} \beta_j \left| \frac{\tilde{\lambda}_j t_0}{2\pi} \right\rangle |u_j\rangle$$

注： $\tilde{\lambda}_j$ 在狄拉克符号中时，表示 $2^m \lambda_j$ 的近似值；在狄拉克符号外时，表示 λ_j 的近似值（下面的 $\tilde{\varphi}_u$ 也类似）

相位估计：

酉操作U: $U|u\rangle = e^{2\pi i \varphi_u} |u\rangle$

初态: $\sum_u c_u |u\rangle$ 利用U，相位估计 $\rightarrow \sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle$



HHL算法中：U对应 $e^{iAt_0} = \sum_j e^{i\lambda_j t_0} |u_j\rangle\langle u_j|$ ， $\sum_u c_u |u\rangle$ 对应 $|b\rangle = \sum_j \beta_j |u_j\rangle$

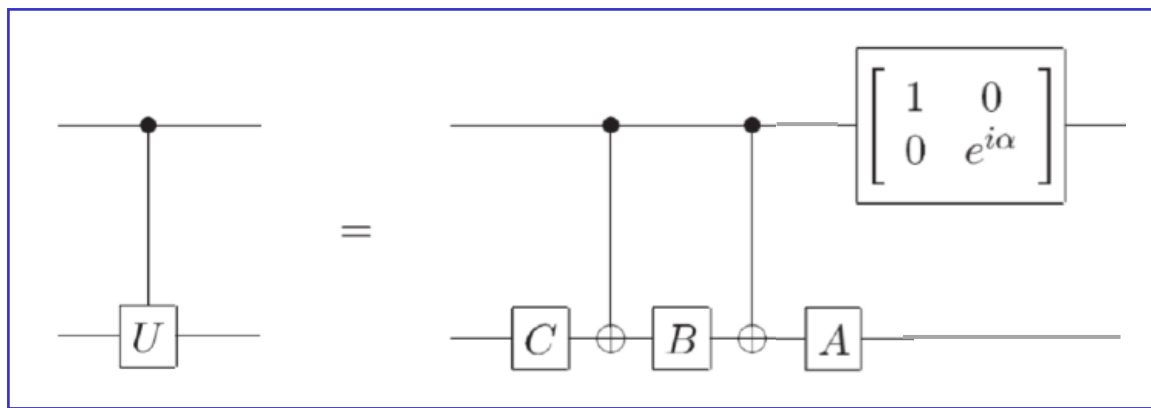
易验证 u_j 是本征态： $U|u_j\rangle = \sum_{j'} e^{i\lambda_{j'} t_0} |u_{j'}\rangle\langle u_{j'}||u_j\rangle = e^{i\lambda_j t_0} |u_j\rangle$



➤ 用模拟可以实现 U ，如何从 U 实现相位估计中用到的是受控 U ，即 $C(U)$ ？

□ 如果 U 是（以矩阵或基本门电路形式）明确给出：容易实现 $C(U)$

- 若 U 是单比特门：根据ABC分解很容易实现 $C(U)$
- 若 U 是多比特门： U 可被分解成单比特门和CNOT门的组合 $A_1A_2A_3 \dots A_m$ ，因此 $C(U) = C(A_1)C(A_2) \dots C(A_m)$ 。如果 A_i 是单比特门，显然 $C(A_i)$ 易实现；如果 A_i 是CNOT门， $C(A_i)$ 即为Toffoli门，易实现。
- 本算法中， U 以电路形式给出（即模拟电路），所以可用上面第2种方法实现



1控制 U 门的分解



1. 制备初态 $H^{\otimes m}|0^{\otimes m}\rangle \otimes |b\rangle = (\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle) \otimes (\sum_j \beta_j |u_j\rangle)$

2. 做相位估计：U用稀疏Hamiltonian模拟 $e^{iAt_0} = \sum_{j=1} e^{i\lambda_j t_0} |u_j\rangle\langle u_j|$ 实现，得量子态

$$\approx \sum_{j=1} \beta_j e^{i\frac{\tilde{\lambda}_j t_0}{2\pi}} |u_j\rangle$$

3. 在量子态后面附加单比特量子态 $|0\rangle$, 并执行受控旋转操作

$$\sum_j \beta_j e^{i\frac{\tilde{\lambda}_j t_0}{2\pi}} |u_j\rangle \left(\sqrt{1 - \left| \frac{c}{\tilde{\lambda}_j} \right|^2} |0\rangle + \frac{c}{\tilde{\lambda}_j} |1\rangle \right)$$

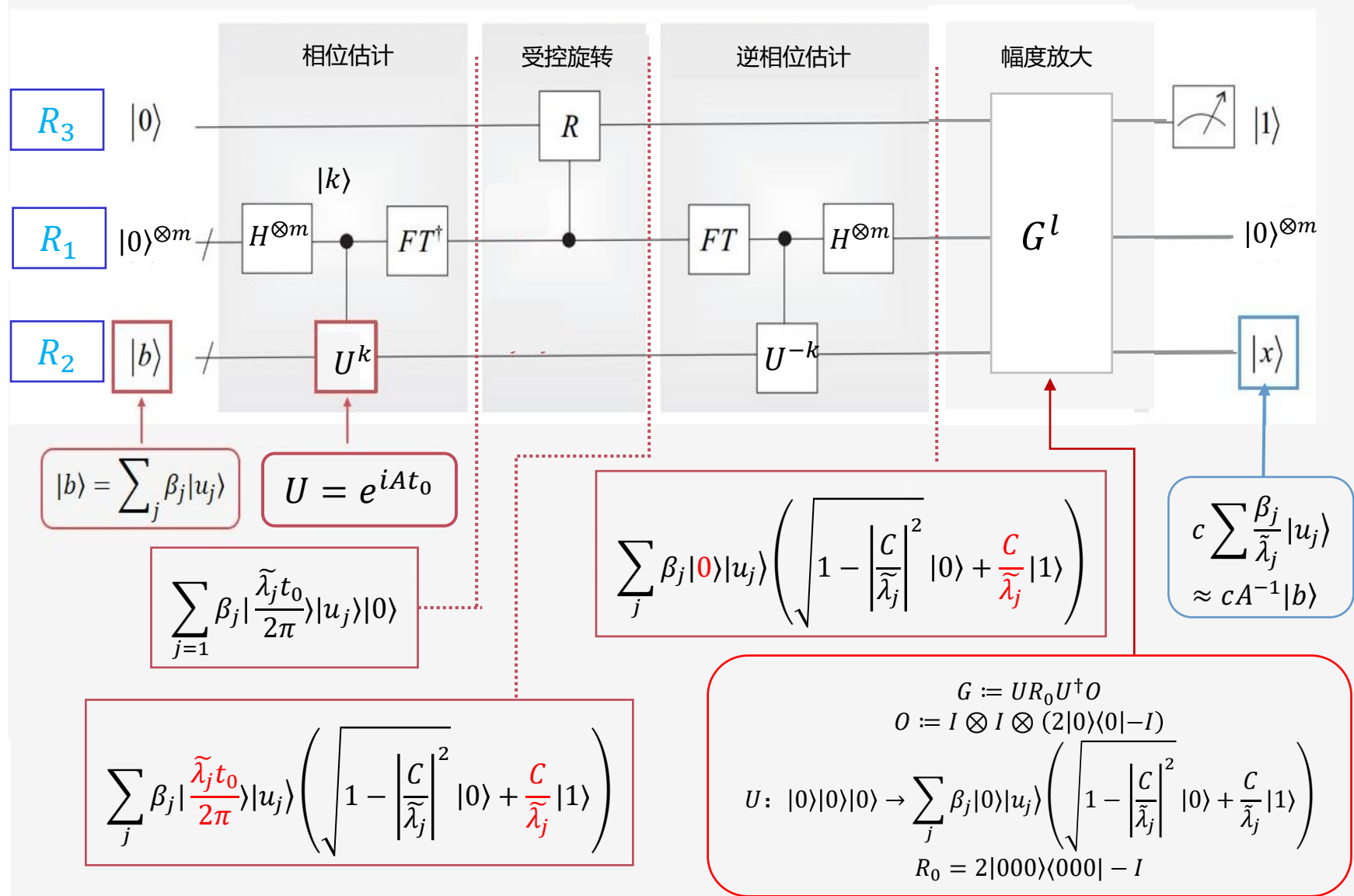
4. 执行相位估计逆操作（为了简洁，包括 $H^{\otimes m}$ ）

$$\sum_j \beta_j |0\rangle |u_j\rangle \left(\sqrt{1 - \left| \frac{c}{\tilde{\lambda}_j} \right|^2} |0\rangle + \frac{c}{\tilde{\lambda}_j} |1\rangle \right)$$

5. 幅度放大使得最后一个qubit获得 $|1\rangle$ 的结果，得

$$|x\rangle = c \sum \frac{\beta_j}{\tilde{\lambda}_j} |u_j\rangle = cA^{-1}|b\rangle$$

C 在能保证 $|\frac{c}{\lambda_j}| \leq 1$ 的前提下取最大的常数（使随后测得1的概率最大）。因此，如果满足矩阵A假设 $\lambda_j^2 \in [\frac{1}{\kappa^2}, 1]$ ，注意到此时 $|\lambda|_{\max} = 1$ ，那么 $C = |\lambda|_{\min} = \frac{|\lambda|_{\min}}{|\lambda|_{\max}} = 1/\kappa$ （注：根据前提假设 $|\lambda|_{\min}$ 已知；如果 $|\lambda|_{\max}$ 估计不准，则 C 要足够小，见后面讨论）





➤ 量子线性方程组求解算法

- 问题描述

- HHL 算法

- 复杂度分析和参数讨论

Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth., Quantum algorithm for solving linear systems of equations, Physical Review Letters. 103 (15): 150502, 2009



1. 制备初态 $H^{\otimes m}|0^{\otimes m}\rangle \otimes |b\rangle = (\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle) \otimes (\sum_j \beta_j |u_j\rangle)$

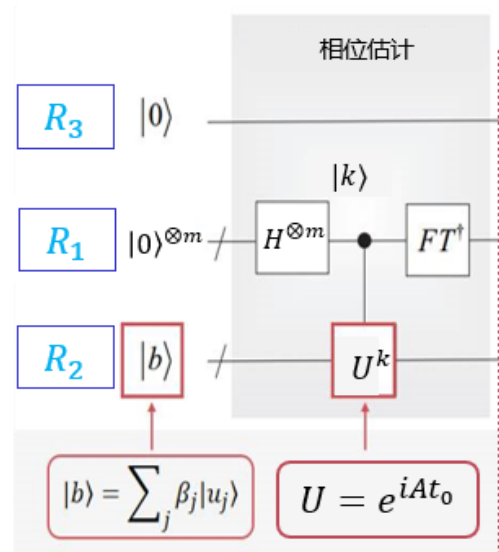
复杂度: $O(m + \log N)$, 其中 $\log N$ 是在 R2 制备量子态 $|b\rangle$ 的复杂度

2. 做相位估计: U 用稀疏 Hamiltonian 模拟 $e^{iAt_0} = \sum_{j=1} e^{i\lambda_j t_0} |u_j\rangle\langle u_j|$ 实现, 得量子态:

$$\approx \sum_{j=1} \beta_j \left| \frac{\tilde{\lambda}_j t_0}{2\pi} \right\rangle |u_j\rangle$$

相关参数需要讨论

相位估计对 λ_j 与 t_0 取值范围提出了要求
算法复杂度与参数 m 取值有关





与标准的相位估计做类比：

$$\frac{\lambda_j t_0}{2\pi} \sim \varphi_u$$

酉操作 $U: U|u\rangle = e^{2\pi i \varphi_u} |u\rangle$

初态: $\sum_u c_u |u\rangle \xrightarrow{\text{相位估计}} \sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle$

- 相位估计中 $\varphi_u \in [0, 1)$ ，也就是取了一个周期，在这个范围以外的值会被投影到这个范围内。相应地，我们把 $\frac{\lambda_j t_0}{2\pi}$ 的范围限制为 $[-\frac{1}{2}, \frac{1}{2})$ ，因为特征值 λ_j 可以取负数且 $t_0 > 0$
- λ_j ：如果不对 $|\lambda_j|$ 的取值进行限制，那么无论 t_0 取任何值， $\frac{\lambda_j t_0}{2\pi}$ 总有可能超出区间 $[-\frac{1}{2}, \frac{1}{2})$ ，导致算法输出错误的结果。为确保结果的正确性，算法假设 $|\lambda_j| \in [\frac{1}{\kappa}, 1]$ ，或需要做预处理 $A/|\lambda|_{\max}$ 来达到该要求
- 先确定 t_0 ： t_0 是做模拟 e^{iAt} 的最小时长。因为 $|\lambda_j|$ 的取值范围为 $[\frac{1}{\kappa}, 1]$ ，当 $t_0 \leq \pi$ 时可使得 $\frac{\lambda_j t_0}{2\pi} \in [-\frac{1}{2}, \frac{1}{2})$ 。一般取 $t_0 = \pi$ ，此时 $\frac{\lambda_j t_0}{2\pi}$ 分布最广，可使相位估计的结果更为精确

➤ **再确定 m** 。相位估计中 U 是 e^{iAt_0} ，其特征值是 $e^{i\lambda_j t_0}$ 。相位估计后，R2的态是 $\left| \frac{\tilde{\lambda} t_0}{2\pi} \right\rangle$

相位估计误差为 $\epsilon' = \frac{1}{2^m}$ (即 $\frac{\lambda_j t_0}{2\pi}$ 的误差)，所以 λ_j 的误差为 $\frac{2\pi}{2^m t_0}$ 。

相位估计后，若要求特征值的倒数（这里需要计算 $\frac{1}{\lambda}$ 的误差）的**相对误差**不超过 ϵ ，即：

$$\frac{|1/\lambda - 1/\tilde{\lambda}|}{|1/\lambda|} = \frac{|\lambda - \tilde{\lambda}|}{|\tilde{\lambda}|} < \frac{2\pi}{2^m t_0} \kappa \leq \epsilon。 \quad \text{因此 } 2^m t_0 \geq \frac{2\pi \kappa}{\epsilon}。 \quad \text{因为 } t_0 = \pi, \text{ 因此 } m \geq \log\left(\frac{2\kappa}{\epsilon}\right)。$$

由 $m \geq \log\left(\frac{2\kappa}{\epsilon}\right)$ 可推知 $\epsilon' = \frac{1}{2^m} \leq \frac{\epsilon}{2\kappa}$ ，绝对值小于 $\frac{\epsilon}{2\kappa}$ 的特征值在相位估计时可能会被丢掉。但这里一般 $\frac{\epsilon}{2\kappa} < \frac{1}{\kappa}$ ，而特征值都满足 $\lambda^2 \in [\frac{1}{\kappa^2}, 1]$ ，所以一般不会有特征值被丢弃。

即：若 κ 已知，为保证（估计的特征值）精度而选择的 m 足以保证每个特征值都不会被丢弃

反之若 κ 未知，无论取多大的 m ，都有可能有很小的特征值被丢弃，进而无法求 $Ax = b$ 的精确解，但一般认为太小的特征值是噪声引起的，本就应该忽略掉（即求的是**TSVD解**）

➤ **复杂度**：相位估计本身复杂度为 $O\left(\frac{1}{\epsilon'} T_U\right)$ ，在这里 $\frac{1}{\epsilon'} = 2^m$ ， T_U 即实现 e^{iAt_0} 的复杂度，为 $\tilde{O}(\log(N) s^4 t_0)$ [1]，其中 s 为矩阵 A 的稀疏度。综合两部分，该步复杂度为

$$\tilde{O}(\log(N) s^4 2^m t_0) = \tilde{O}(\log(N) s^4 \frac{\kappa}{\epsilon})$$

\tilde{O} ： O 的近似，忽略了一些增长较慢的项



λ_{max} 和 κ 的估计值对结果的影响

- 若明确知道 κ 以及 $|\lambda|_{max}$ （或知道它们的一个比较紧致的上界），则能用算法求“完整”解（不会有特征值被丢弃）
- 假设 $|\lambda|_{max}$ 取值是准确的，则 κ 的估计值
 - ❑ 偏大时：需要更大的 m 值，复杂度变大，算法可以求“完整”解
 - ❑ 偏小时：1.可能会导致一些小的特征值被丢弃，求出的是类似TSVD解；
2.受控旋转 C 取得偏大，导致算法出错
- 假设 κ 的取值是准确的，则 $|\lambda|_{max}$ 估计值
 - ❑ 偏大时：1.可能会导致一些小的特征值被丢弃，求出的是类似TSVD解；
2.受控旋转 C 取得偏大，导致算法出错（所以为了保险 C 要相比 $|\lambda|_{min}$ 足够小才行）
 - ❑ 偏小时：此时 $\frac{\lambda_j t_0}{2\pi}$ 有可能超出周期范围，相位估计输出错误结果，错误解



3. 在量子态后面附加单比特量子态 $|0\rangle$, 并执行受控旋转操作

$$\sum_j \beta_j |\frac{\tilde{\lambda}_j t_0}{2\pi}\rangle |u_j\rangle \left(\sqrt{1 - \left| \frac{c}{\tilde{\lambda}_j} \right|^2} |0\rangle + \frac{c}{\tilde{\lambda}_j} |1\rangle \right)$$

复杂度为 $O(m)$

4. 执行相位估计逆操作: $\sum_j \beta_j |u_j\rangle \left(\sqrt{1 - \left| \frac{c}{\tilde{\lambda}_j} \right|^2} |0\rangle + \frac{c}{\tilde{\lambda}_j} |1\rangle \right)$

复杂度: $\tilde{O}(\log(N) s^4 \frac{\kappa}{\epsilon})$

5. 幅度放大使得最后一个qubit获得 $|1\rangle$ 的结果, 获得量子态 $|x\rangle = c \sum \frac{\beta_j}{\lambda_j} |u_j\rangle = cA^{-1}|b\rangle$

若直接测量最后一量子比特, 测到 $|1\rangle$ 的概率为:

$$P(1) = \sum_j \frac{\beta_j^2 C^2}{\tilde{\lambda}_j^2} = \sum_j \frac{\beta_j^2 |\lambda|_{\min}^2}{\tilde{\lambda}_j^2} \geq \sum_j \frac{\beta_j^2 |\lambda|_{\min}^2}{|\tilde{\lambda}_j|_{\max}^2} \approx 1/\kappa^2$$

如前所述:

$$C = |\lambda|_{\min} = 1/\kappa$$

需要重复执行算法 $O(\kappa^2)$ 次即可以接近1的概率获得正确结果。通过幅度放大, 可使算法重复次数降为 $O(\kappa)$ 。因此, 算法总复杂度为:

$$\tilde{O}\left(\log(N) s^4 \times \frac{\kappa}{\epsilon} \times \kappa\right) = \tilde{O}(\log(N) s^4 \kappa^2 / \epsilon)$$

目标	输入	输出	复杂度
求解线性方程组 $Ax = b$	$ 0\rangle$	$\approx x\rangle$	$\tilde{O}(\log(N) s^4 \kappa^2 / \epsilon)$ 指数加速

要想达到指数加速效果，需要注意以下条件：

1. 量子态 $|b\rangle$ 可有效制备
2. 可有效实现 e^{iAt} ：对于稀疏矩阵 A ，如果存在一个QRAM可以存储行 i 中非0元素的位置和值，那么可以有效实现 e^{iAt} （当然还有其他类型的 A 可以有效模拟 e^{iAt} ，但 A 往往也需要满足特殊条件）
3. 若要实现指数加速，条件数 κ 的大小需要限制，其数量级应为 $O(\text{poly log } N)$ ，即随着维数 N 的增长，条件数 κ 的增长速度应为 $O(\text{poly log } N)$
4. 输出是一个量子态，要想得到 x 每个分量，需要进行多次测量，将失去指数加速
5. 需要知道稀疏矩阵的条件数 κ 和 $|\lambda|_{\max}$ ，或至少知道他们的大概范围



谢谢!

