科学计算中的量子算法：量子数值线性代数基本算法

安冬

北京大学北京国际数学研究中心（BICMR）

andong@bicmr.pku.edu.cn

24-25 学年第 2 学期

大纲

- 矩阵向量乘
- 向量内积：SWAP 测试与 Hadamard 测试
- 矩阵/向量加法：线性酉组合（LCU）
- 矩阵乘法

回顾：向量与矩阵的量子表示

向量： $|u\rangle = \sum_{j=0}^{N-1} u_j |j\rangle = (u_0, u_1, \cdots, u_{N-1})^\top, \quad \| |u\rangle \| = 1$

$$O_u : |0\rangle \mapsto |u\rangle$$

矩阵： $A \in \mathbb{C}^{2^n \times 2^n}$ 的 (α, a, ϵ)-block-encoding 为酉矩阵 $U_A \in \mathbb{C}^{2^{n+a} \times 2^{n+a}}$：

$$\left\| A - \alpha \left(\langle 0|^{\otimes a} \otimes I \right) U_A \left(|0\rangle^{\otimes a} \otimes I \right) \right\| \leq \epsilon$$

$$U_A \approx \begin{pmatrix} \frac{1}{\alpha} A & * \\ * & * \end{pmatrix}.$$

回顾：矩阵向量乘

Input:

Block-encoding of A:

$$A \approx \alpha \left(\langle 0| \otimes I\right) U_A \left(|0\rangle \otimes I\right)$$

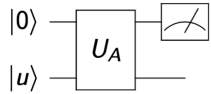
$$U_A \approx \begin{array}{c} \begin{array}{cc} \langle 0| & \langle 1| \end{array} \\ \begin{pmatrix} \frac{1}{\alpha}A & * \\ * & * \end{pmatrix} \end{array} \begin{array}{c} |0\rangle \\ |1\rangle \end{array}$$

or $U_A \approx |0\rangle\langle 0| \otimes \frac{A}{\alpha} + |0\rangle\langle 1| \otimes * + |1\rangle\langle 0| \otimes * + |1\rangle\langle 1| \otimes *$

Quantum state:

$$|u\rangle = \sum_{j=0}^{2^n-1} u_j |j\rangle$$

'Algorithm': applying block-encoding



or $U_A |0\rangle |u\rangle \approx \frac{1}{\alpha} |0\rangle A |u\rangle + c |1\rangle |*\rangle$

or $\begin{pmatrix} \frac{1}{\alpha}A & * \\ * & * \end{pmatrix} \begin{pmatrix} u \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\alpha}Au \\ * \end{pmatrix}$

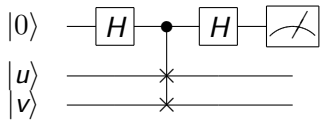
Need to measure the first ancilla qubit

Success probability: $\left(\|A|u\rangle\|/\alpha\right)^2$

Number of repeats (after amplitude amplification): $\mathcal{O}\left(\alpha/\|A|u\rangle\|\right)$

向量内积：SWAP 测试

目标：计算 $|\langle u|v\rangle|$



$$|0\rangle|u\rangle|v\rangle \to \frac{1}{\sqrt{2}}(|0\rangle|u\rangle|v\rangle + |1\rangle|u\rangle|v\rangle) \to \frac{1}{\sqrt{2}}(|0\rangle|u\rangle|v\rangle + |1\rangle|v\rangle|u\rangle)$$
$$\to \frac{1}{2}|0\rangle(|u\rangle|v\rangle + |v\rangle|u\rangle) + \frac{1}{2}|1\rangle(|u\rangle|v\rangle - |v\rangle|u\rangle)$$

$$\mathbb{P}(\textbf{第一个量子比特} = 1) = \left\|\frac{1}{2}(|u\rangle|v\rangle - |v\rangle|u\rangle)\right\|^2 = \frac{1}{2} - \frac{1}{2}|\langle u|v\rangle|^2$$

向量内积：SWAP 测试

随机变量 X: 与第一个量子比特的结果一致（用 $|1\rangle\langle 1|$ 测量）

$$\mathbb{E}X = \frac{1}{2} - \frac{1}{2}|\langle u|v\rangle|^2$$

用 $\frac{1}{M}\sum_{m=1}^{M} X_m$ 来估计 $\frac{1}{2} - \frac{1}{2}|\langle u|v\rangle|^2$.

Q: M 需要取多大？

向量内积：SWAP 测试

Lemma (Hoeffding 不等式)

设 X_m 为相互独立的随机变量，几乎确定满足 $a_m \leq X_m \leq b_m$. 令 $S_M = X_1 + \cdots + X_M$, 那么

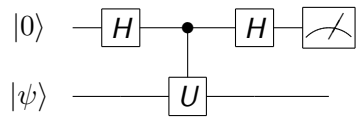
$$\mathbb{P}\left(|S_M - \mathbb{E}S_M| \geq t\right) \leq 2\exp\left(-\frac{2t^2}{\sum_{m=1}^{M}(b_m - a_m)^2}\right)$$

在 SWAP 测试中：

$$\mathbb{P}\left(\left|\frac{1}{M}\sum X_m - \left(\frac{1}{2} - \frac{1}{2}|\langle u|v\rangle|^2\right)\right| \geq \epsilon\right) \leq 2\exp\left(-2M\epsilon^2\right)$$
$$\Longrightarrow \; M = \mathcal{O}\left(1/\epsilon^2\right)$$

酉矩阵的期望：Hadamard 测试

目标：计算 $\langle\psi|U|\psi\rangle$，其中 U 是一个酉矩阵

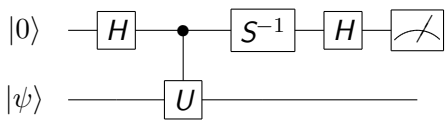


$$|0\rangle|\psi\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle \to \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle)$$
$$\to \frac{1}{2}|0\rangle(I+U)|\psi\rangle + \frac{1}{2}(I-U)|\psi\rangle$$

$$\mathbb{P}(\textbf{第一个量子比特} = 0) = \left\|\frac{1}{2}(I+U)|\psi\rangle\right\|^2 = \frac{1}{2} + \frac{1}{2}\mathrm{Re}(\langle\psi|U|\psi\rangle)$$

酉矩阵的期望：Hadamard 测试

虚部：

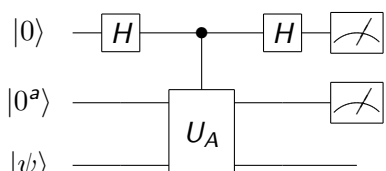


酉矩阵的期望：Hadamard 测试

与内积的关系：取 $U = U_\phi U_\psi^\dagger$ (注意实际量子线路可以简化)

$$\langle\psi|U|\psi\rangle = \langle\psi|\phi\rangle$$

一般矩阵的期望：计算 $\langle\psi|A|\psi\rangle$，其中 A 是一个一般的矩阵，U_A 是它的 $(\alpha, a, 0)$-block-encoding



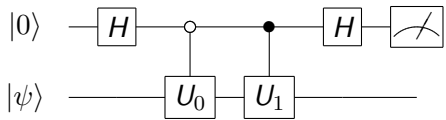
矩阵/向量加法：线性酉组合（Linear Combination of Unitaries）

目标：给定一组酉变换 U_j 和一组正实数 $c_j > 0$，计算 $\sum_{j=0}^{J-1} c_j U_j$

- 一般来说不是酉变换

LCU：例子

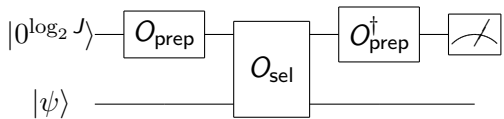
目标：计算 $\frac{1}{2}(U_0 + U_1)$



- $(1, 1, 0)$-block-encoding
- **成功概率**：$\left\| \frac{1}{2}(U_0 + U_1) |\psi\rangle \right\|^2$

LCU：一般形式

目标：给定一组酉变换 U_j 和一组正实数 $c_j > 0$，计算 $\sum_{j=0}^{J-1} c_j U_j$



$$O_{\text{prep}} : |0\rangle \mapsto \frac{1}{\sqrt{\|\vec{c}\|_1}} \sum_{j=0}^{J-1} \sqrt{c_j} |j\rangle , \quad O_{\text{sel}} = \sum_{j=0}^{J-1} |j\rangle \langle j| \otimes U_j$$

- $(\|\vec{c}\|_1, \log_2 J, 0)$-block-encoding
- **成功概率**：$\left\| \left(\sum_j c_j U_j \right) |\psi\rangle / \|\vec{c}\|_1 \right\|^2$

向量加法

目标：给定一组量子态 $|u_j\rangle$ 和一组正实数 $c_j > 0$，计算 $\sum_{j=0}^{J-1} c_j |u_j\rangle$

输入：量子态的态制备 oracle $U_j : |0\rangle \mapsto |u_j\rangle$

$$\sum_{j=0}^{J-1} c_j |u_j\rangle = \left(\sum_{j=0}^{J-1} c_j U_j \right) |0\rangle$$

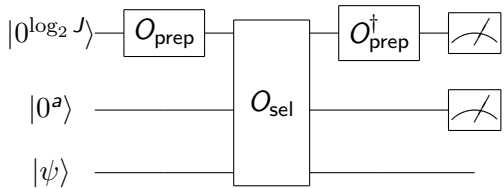
矩阵加法

目标：给定一组矩阵 A_j 和一组正实数 $c_j > 0$，计算 $\sum_{j=0}^{J-1} c_j A_j$

- 输入：矩阵 A_j 的 $(\alpha_j, a, 0)$-block-encoding U_j (等价于矩阵 A_j/α_j 的 $(1, a, 0)$-block-encoding)

$$\sum_{j=0}^{J-1} c_j A_j = \sum_{j=0}^{J-1} \alpha_j c_j (A_j/\alpha_j)$$

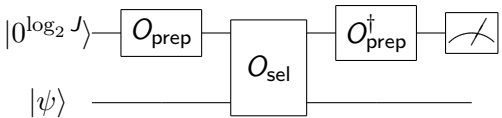
矩阵加法



$$O_{\text{prep}} : |0\rangle \mapsto \frac{1}{\sqrt{\sum \alpha_j c_j}} \sum_{j=0}^{J-1} \sqrt{\alpha_j c_j}\, |j\rangle\,, \quad O_{\text{sel}} = \sum_{j=0}^{J-1} |j\rangle\langle j| \otimes U_j$$

- $(\sum \alpha_j c_j, a + \log_2 J, 0)$-block-encoding
- **成功概率**: $\left\| \left(\sum_j c_j A_j \right) |\psi\rangle \,/\, (\sum \alpha_j c_j) \right\|^2$

LCU 的计算复杂度与局限性



$$O_{\text{prep}} : |0\rangle \mapsto \frac{1}{\sqrt{\|\vec{c}\|_1}} \sum_{j=0}^{J-1} \sqrt{c_j}\,|j\rangle\,,$$

$$O_{\text{sel}} = \sum_{j=0}^{J-1} |j\rangle\langle j| \otimes U_j$$

访问复杂度：$\mathcal{O}\left(\|\vec{c}\|_1^2 / \left\|\left(\sum_j c_j U_j\right)|\psi\rangle\right\|^2\right)$ 次 O_{prep} 和 O_{sel}

- O_{sel} 的计算复杂度
  - 最坏的情况为构造每个 U_j 复杂度之和
  - 如果 U_j 之间有一些联系，那么 O_{sel} 的计算复杂度可能会更低
- 需要控制版本的 U_j 与额外的辅助量子比特
- 线路深度较深

LCU 的混合实现

目标: 计算 $\psi^* H\psi$，其中向量 $\psi = \sum_j c_j U_j |\psi_0\rangle$，$H$ 是一个厄米矩阵

$$\psi^* H\psi = \sum_{j,j'} c_j c_{j'} \langle\psi_0| U_j^\dagger H U_{j'} |\psi_0\rangle$$

混合算法:

1. （经典计算机上）以概率 $c_j c_{j'} / \|\vec{c}\|_1^2$ 概率取样 (j, j')
2. （量子计算机上）对每一个 (j, j') 的样本，分别计算 $\langle\psi_0| U_j^\dagger H U_{j'} |\psi_0\rangle$
3. （经典计算机上）对所有的样本观测值取平均

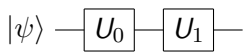
LCU：量子实现 vs 混合实现

	计算任务	总计算复杂度	辅助比特数量	控制操作	线路深度
量子实现	block-encoding	低	多	复杂	深
混合实现	测量值	高	少	简单	浅

矩阵乘法

考虑两个矩阵的矩阵乘法

- 两个酉矩阵 $U_1 U_0$

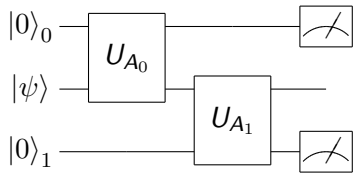


- 两个一般矩阵 A_0 和 A_1，已知它们的 block-encodings U_{A_0} 和 U_{A_1}. 尝试：

- 该线路是不对的，因为 U_{A_1} 会将作用了 U_{A_0} 之后的一些 “垃圾” 部分带回 $|0\rangle$ 对应的子空间

矩阵乘法

思想：使用多份独立的辅助量子比特

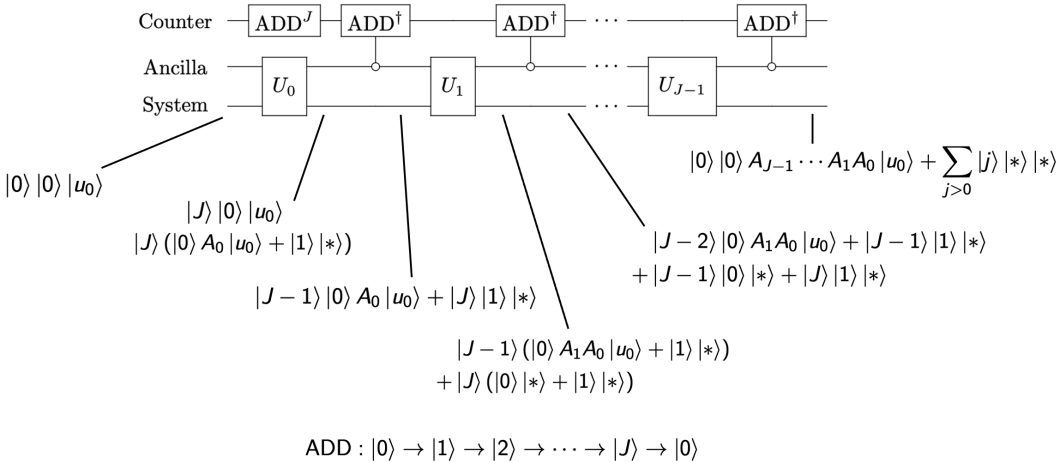


$$
\begin{aligned}
|0\rangle_1 |0\rangle_0 |\psi\rangle &\xrightarrow{U_{A_0}} |0\rangle_1 (|0\rangle_0 A_0 |\psi\rangle + |1\rangle_0 |*\rangle) \\
&= |0\rangle_0 |0\rangle_1 A_0 |\psi\rangle + |1\rangle_0 |0\rangle_1 |*\rangle \\
&\xrightarrow{U_{A_1}} |0\rangle_0 (|0\rangle_1 A_1 A_0 |\psi\rangle + |1\rangle_1 |*\rangle) + |1\rangle_0 |0\rangle_1 |*\rangle + |1\rangle_0 |1\rangle_1 |*\rangle
\end{aligned}
$$

J 个矩阵的乘法：需要 $\mathcal{O}(Ja)$ 额外的辅助量子比特

- **更好的方法**：compression gadget

矩阵乘法: compression gadget



- $a + \log_2 J$ 额外的辅助量子比特

阅读

阅读：

- LL: Chapter 3.1, 7.3
- [arXiv:1806.01838]: Section 4