科学计算中的量子算法：
量子搜索、量子振幅放大与量子振幅估计

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

- 量子搜索（Quantum Unstructured Search/Grover's algorithm）
- 振幅放大（Amplitude Amplification）
- 振幅估计（Amplitude Estimation）

量子搜索

Q: $N = 2^n$ 个外表完全一样的盒子，其中一个里面有一个苹果，找出这个盒子

考虑函数 $f(x) : [N] \mapsto \{0, 1\}$，满足存在唯一的 $x_0 \in [2^n]$ 使得

$$f(x) = \begin{cases} 1, & x = x_0, \\ 0, & x \neq x_0 \end{cases}$$

经典复杂度：$\mathcal{O}(N)$

量子搜索：oracle

量子 oracle：

$$U_f|x\rangle|y\rangle \mapsto |x\rangle|y\oplus f(x)\rangle, \quad x\in[N], y\in\{0,1\}$$

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle, \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

对于任意一个量子态 $|\psi\rangle = \sum c_j |x_j\rangle$,

$$U_f|\psi\rangle|-\rangle = U_f\left(c_0|x_0\rangle + \sum_{x\in[N],x\neq x_0} c_j|x_j\rangle\right)|-\rangle = \left(-c_0|x_0\rangle + \sum_{x\in[N],x\neq x_0} c_j|x_j\rangle\right)|-\rangle$$

忽视掉最后一个量子比特，U_f 便“等价于”一个 Householder 变换 R_{x_0}：

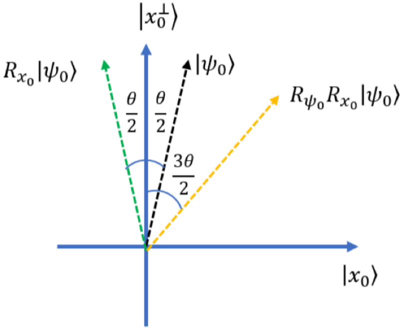
$$R_{x_0}|x\rangle = \begin{cases} |x\rangle, & x\in[N], x\neq x_0, \\ -|x\rangle, & x = x_0, \end{cases} \qquad R_{x_0} = I - 2|x_0\rangle\langle x_0|$$

量子搜索：Grover 算法

从 $|\psi_0\rangle = H^{\otimes n}|0\rangle$ 出发，

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{x\in[N]}|x\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \frac{1}{\sqrt{N}}\sum_{x\in[N],x\neq x_0}|x\rangle$$

思路：通过旋转不断放大 $|x_0\rangle$ 的振幅



$|x_0\rangle$：目标态

$$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\in[N],x\neq x_0}|x\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{x\in[N]}|x\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|x_0^\perp\rangle$$

$$\theta = 2\arcsin(1/\sqrt{N})$$

量子搜索：Grover 算法

量子 oracle：关于 $|x_0^\perp\rangle$ 的对称变换

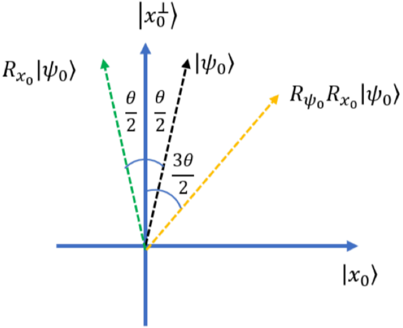
$$R_{x_0} = I - 2\,|x_0\rangle\langle x_0|$$

关于 $|\psi_0\rangle$ 的对称变换（仅在二维子空间内）：

$$R_{\psi_0} = -(I - 2\,|\psi_0\rangle\langle\psi_0|)$$

Grover 算法：做 k 次旋转 $R_{\psi_0}R_{x_0}$

$$(R_{\psi_0}R_{x_0})^k H^{\otimes n}|0\rangle = \sin((2k+1)\theta/2)\,|x_0\rangle + \cos((2k+1)\theta/2)\,|x_0^\perp\rangle$$



量子搜索：Grover 算法理论验证

1. 验证 span$\{|x_0\rangle, |x_0^\perp\rangle\}$ 是 R_{x_0} 和 R_{ψ_0} 的不变子空间

$$R_{\psi_0}|x_0\rangle = -\cos(\theta)|x_0\rangle + \sin(\theta)|x_0^\perp\rangle$$
$$R_{\psi_0}|x_0^\perp\rangle = \sin(\theta)|x_0\rangle + \cos(\theta)|x_0^\perp\rangle$$

2. 对于量子态 $\sin(\alpha)|x_0\rangle + \cos(\alpha)|x_0^\perp\rangle$,

$$\begin{aligned}
&R_{\psi_0}R_{x_0}(\sin(\alpha)|x_0\rangle + \cos(\alpha)|x_0^\perp\rangle) \\
&= R_{\psi_0}(-\sin(\alpha)|x_0\rangle + \cos(\alpha)|x_0^\perp\rangle) \\
&= -\sin(\alpha)(-\cos(\theta)|x_0\rangle + \sin(\theta)|x_0^\perp\rangle) + \cos(\alpha)(\sin(\theta)|x_0\rangle + \cos(\theta)|x_0^\perp\rangle) \\
&= \sin(\alpha+\theta)|x_0\rangle + \cos(\alpha+\theta)|x_0^\perp\rangle
\end{aligned}$$

量子搜索：Grover 算法理论验证

R_{x_0} 和 R_{ψ_0} 在不变子空间 $V = \mathrm{span}\{|x_0\rangle, |x_0^{\perp}\rangle\}$ 内的矩阵表示：

$$R_{x_0} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}_V,$$

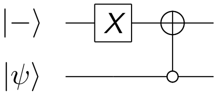
$$R_{\psi_0} = \begin{pmatrix} -\cos(\theta) & \sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}_V$$

量子搜索：Grover 算法实现

$$(R_{\psi_0} R_{x_0})^k H^{\otimes n} |0^n\rangle$$

$$R_{\psi_0} = -(I - 2|\psi_0\rangle\langle\psi_0|) = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}$$

$2|0^n\rangle\langle 0^n| - I$:



量子搜索：Grover 算法复杂度

$$(R_{\psi_0} R_{x_0})^k H^{\otimes n} |0\rangle = \sin((2k+1)\theta/2) |x_0\rangle + \cos((2k+1)\theta/2) |x_0^\perp\rangle$$

$$\theta = 2\arcsin(1/\sqrt{N}) \sim 1/\sqrt{N}$$

为了 $\sin((2k+1)\theta/2) \approx 1$，取

$$(2k+1)\theta/2 \approx \pi/2$$

$$k \sim \frac{1}{\theta} \sim \sqrt{N}$$

量子搜索：小结

$$\text{量子复杂度}\mathcal{O}(\sqrt{N}) \quad \text{vs} \quad \text{经典复杂度}\mathcal{O}(N)$$

- 下界：$\Omega(\sqrt{N})$
- 若有 M 个目标，需要找到其中任意一个，量子复杂度 $\mathcal{O}(\sqrt{N/M})$（需要事先知道 M 的值）

振幅放大

考虑量子态

$$|\psi\rangle = \sqrt{p}\,|\psi_{\mathsf{good}}\rangle + \sqrt{1-p}\,|\psi_{\mathsf{bad}}\rangle\,, \quad \langle\psi_{\mathsf{good}}|\psi_{\mathsf{bad}}\rangle = 0$$

直接测量：概率 p，需要重复 $\mathcal{O}(1/p)$ 次

振幅放大

$$|\psi\rangle = \sqrt{p}\,|\psi_{\text{good}}\rangle + \sqrt{1-p}\,|\psi_{\text{bad}}\rangle\,, \quad \langle\psi_{\text{good}}|\psi_{\text{bad}}\rangle = 0$$

思路：仿照 Grover 先放大 $|\psi_{\text{good}}\rangle$ 的振幅

- 在 Grover 里，$|\psi_{\text{good}}\rangle = |x_0\rangle$，$p = 1/N$

$$\begin{aligned} R_{\text{good}} &= I - 2\,|\psi_{\text{good}}\rangle\langle\psi_{\text{good}}|\,, \\ R_\psi &= -(I - 2\,|\psi\rangle\langle\psi|) = U_\psi(2\,|0\rangle\langle 0| - I)\,U_\psi^\dagger \end{aligned}$$

$$\Longrightarrow \quad (R_\psi R_{\text{good}})^k\,|\psi\rangle = c\,|\psi_{\text{good}}\rangle + \sqrt{1-c^2}\,|\psi_{\text{bad}}\rangle\,,$$

其中 $c = \Omega(1), k = \mathcal{O}(1/\sqrt{p})$

注意：需要知道如何关于 $|\psi_{\text{good}}\rangle$ 做对称

振幅放大

$$U_\psi |0^a\rangle |0^n\rangle = \sqrt{p} |0^a\rangle |\psi\rangle + |\perp\rangle , \quad (|0^a\rangle \langle 0^a| \otimes I_n) |\perp\rangle = 0$$

直接测量：概率 p 得到 $|0^a\rangle |\psi\rangle$，需要重复 $\mathcal{O}(1/p)$ 次

$$\begin{aligned} R_{\text{good}} &= (I_a - 2 |0^a\rangle \langle 0^a|) \otimes I_n, \\ R_\psi &= U_\psi (2 |0^{a+n}\rangle \langle 0^{a+n}| - I_{a+n}) U_\psi^\dagger \end{aligned}$$

考虑

$$(R_\psi R_{\text{good}})^k U_\psi |0^a\rangle |0^n\rangle , \quad k = \mathcal{O}(1/\sqrt{p})$$

振幅放大

$$U_\psi \left|0^a\right\rangle \left|0^n\right\rangle = \sqrt{p}\left|0^a\right\rangle \left|\psi\right\rangle + \sqrt{1-p}\left|u\right\rangle, \quad \left(\left|0^a\right\rangle \left\langle 0^a\right| \otimes I_n\right)\left|u\right\rangle = 0$$

考虑 $V = \mathrm{span}\{\left|0^a\right\rangle \left|\psi\right\rangle, \left|u\right\rangle\}$,

$$R_{\mathrm{good}} \left|0^a\right\rangle \left|\psi\right\rangle = -\left|0^a\right\rangle \left|\psi\right\rangle, \quad R_{\mathrm{good}} \left|u\right\rangle = \left|u\right\rangle$$

$$\begin{aligned} R_\psi \left|0^a\right\rangle \left|\psi\right\rangle &= (2p-1)\left|0^a\right\rangle \left|\psi\right\rangle + 2\sqrt{p(1-p)}\left|u\right\rangle, \\ R_\psi \left|u\right\rangle &= 2\sqrt{p(1-p)}\left|0^a\right\rangle \left|\psi\right\rangle + (1-2p)\left|u\right\rangle \end{aligned}$$

振幅放大

R_{good} 和 R_ψ 在不变子空间 $V = \text{span}\{|0^a\rangle\,|\psi\rangle\,,|u\rangle\}$ 内的矩阵表示：

$$R_{\text{good}} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}_V, \quad R_\psi = \begin{pmatrix} -\cos(\theta) & \sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}_V, \quad \theta = 2\arcsin\sqrt{p}$$

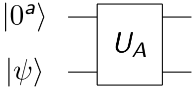
和 Grover 算法等价

算法： 先计算 $(R_\psi R_{\text{good}})^k U_\psi\,|0^a\rangle\,|0^n\rangle$, $k = \mathcal{O}(1/\sqrt{p})$, 再测量

- 访问复杂度 $\mathcal{O}(1/\sqrt{p})$，平方加速
- 无需对 $|\psi\rangle$ 进行对称
- 需要知道 p 的一个下界

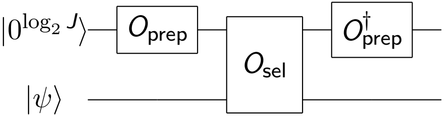
振幅放大：应用

矩阵向量乘：A 的 $(\alpha, a, 0)$-block-encoding U_A，



- 输出 $\frac{1}{\alpha}|0^a\rangle A|\psi\rangle + |\perp\rangle$
- 访问复杂度：$\mathcal{O}(\alpha/\|A|\psi\rangle\|)$

LCU：$\sum c_j U_j$



- 输出 $\frac{1}{\|\vec{c}\|_1}|0^{\log_2 J}\rangle \sum c_j U_j|\psi\rangle + |\perp\rangle$
- 访问复杂度：$\mathcal{O}(\|\vec{c}\|_1/\|\sum c_j U_j|\psi\rangle\|)$

振幅放大：小结

$$|\psi\rangle = \sqrt{p}\,|\psi_{\text{good}}\rangle + \sqrt{1-p}\,|\psi_{\text{bad}}\rangle\,, \quad \langle\psi_{\text{good}}|\psi_{\text{bad}}\rangle = 0$$
$$U_\psi\,|0^a\rangle\,|0^n\rangle = \sqrt{p}\,|0^a\rangle\,|\psi\rangle + |\perp\rangle\,, \quad (|0^a\rangle\,\langle 0^a| \otimes I_n)\,|\perp\rangle = 0$$

访问复杂度：$\mathcal{O}(1/\sqrt{p})$，**平方加速**

- 增加了线路深度
- 需要知道 p 的一个下界（否则会有 overcook 的问题，**解决方法**：fixed-point search/amplitude amplification）
- 连续多次应用会有嵌套问题（某些情况下的解决方法：oblivious amplitude amplification，uniform singular value amplification）

振幅估计

$$|\psi\rangle = \sqrt{p}\,|\psi_{\text{good}}\rangle + \sqrt{1-p}\,|\psi_{\text{bad}}\rangle\,, \quad \langle\psi_{\text{good}}|\psi_{\text{bad}}\rangle = 0$$
$$U_\psi\,|0^a\rangle\,|0^n\rangle = \sqrt{p}\,|0^a\rangle\,|\psi\rangle + |\perp\rangle\,, \quad (|0^a\rangle\,\langle 0^a| \otimes I_n)\,|\perp\rangle = 0$$

目标： 以误差不超过 ϵ 的精度估计 p 的值

算法： Grover + QPE

振幅估计

$$G = R_\psi R_{\mathrm{good}} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}_V, \quad p = \sin^2(\theta/2)$$

G 的特征值和特征向量：$(e^{\pm i\theta}, |\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|\psi_{\mathrm{good}}\rangle \pm i|\psi_{\mathrm{bad}}\rangle))$. 注意到

$$|\langle\psi|\psi_{\mathrm{good}}\rangle|^2 = |\psi|\psi_{\mathrm{bad}}|^2 = \frac{1}{2},$$

可以用 $|\psi\rangle$ 为输入量子态做 QPE，输出会以各 0.5 的概率给出 $\pm\theta$ 的估计

振幅估计：复杂度

$$
\begin{aligned}
|\widetilde{p} - p| &= |\sin^2(\widetilde{\theta}/2) - \sin^2(\theta/2)| = |\sin(\widetilde{\theta}/2) - \sin(\theta/2)| \times |\sin(\widetilde{\theta}/2) + \sin(\theta/2)| \\
&= 2|\sin(\widetilde{\theta}/4 - \theta/4)| \times |\cos(\widetilde{\theta}/4 + \theta/4)| \times |\sin(\widetilde{\theta}/2) + \sin(\theta/2)| \\
&\le |\widetilde{\theta} - \theta|
\end{aligned}
$$

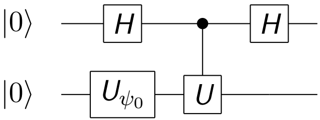
为了使 p 的误差小于 ϵ，只需 θ 的误差小于 ϵ

访问复杂度/线路深度：$\mathcal{O}(1/\epsilon)$

- 相比直接采样的访问复杂度 ($\mathcal{O}(1/\epsilon^2)$) 有平方加速，但增加了线路深度

振幅估计：应用

Hadamard 测试：计算 $\mathrm{Re}\langle\psi_0|U|\psi_0\rangle$，其中 U 是一个酉矩阵



$$|0\rangle|0\rangle \to \frac{1}{2}|0\rangle(I+U)|\psi_0\rangle + \frac{1}{2}|1\rangle(I-U)|\psi_0\rangle := \sqrt{p}|0\rangle|\psi_{\mathrm{good}}\rangle + \sqrt{1-p}|\psi_{\mathrm{bad}}\rangle$$

$$p = \frac{1}{2}(1+\mathrm{Re}\langle\psi_0|U|\psi_0\rangle)$$

结合振幅估计，总的访问复杂度/线路深度为 $\mathcal{O}(1/\epsilon)$

阅读

阅读：

- LL: Chapter 2.2, 2.3, 2.4*, 4.2