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

25-26 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}：

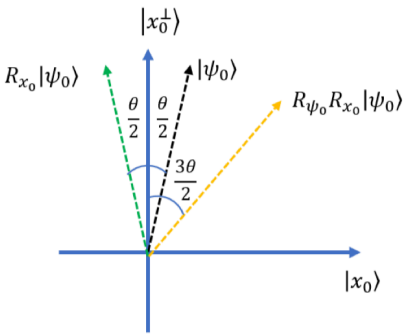
$$R_{x_0}|x\rangle = \begin{cases} |x\rangle, & x \in [N], x \neq x_0, \\ -|x\rangle, & x = x_0, \end{cases} \qquad R_{x_0} = I - 2|x_0\rangle\langle x_0|$$

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**

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

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

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

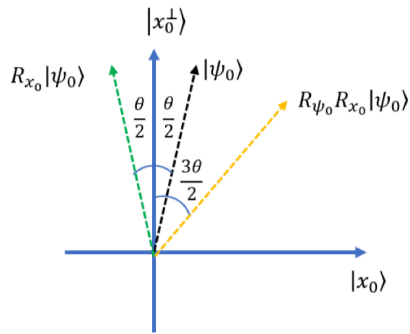
量子搜索：Grover 算法

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：

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

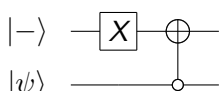
$$R_{\psi_0} = \begin{pmatrix} -\cos(\theta) & \sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}_V$$

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

量子复杂度$\mathcal{O}(\sqrt{N})$ vs 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，$|\psi_{\text{good}}\rangle = |x_0\rangle$, $p = 1/N$

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

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

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

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

振幅放大

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

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

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

考虑

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

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

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

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

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：

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

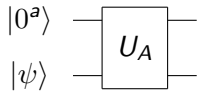
和 Grover 算法等价

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

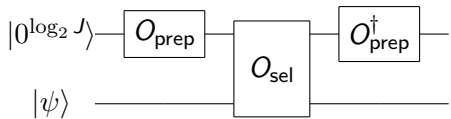
振幅放大：应用

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
- 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）
- 需要知道 p 的一个下界（否则会有 overcook 的问题，解决方法：Quantum Phase Estimation 振幅估计，fixed-point search/amplitude amplification）

Oblivious amplitude amplification

动机：W 是一个酉矩阵，但我们只知道它的一个 $(2, *, 0)$-block-encoding（记为 V）

$$V|0\rangle|\psi\rangle = \frac{1}{2}|0\rangle W|\psi\rangle + |\perp\rangle$$

目标：实现 $W^m|0\rangle$

Oblivious amplitude amplification

一般形式：

$$V|0\rangle|\psi\rangle = \sin\theta\,|0\rangle W|\psi\rangle + |\perp\rangle$$

目标：放大 $|0\rangle W|\psi\rangle$ 的振幅，但过程与 $|\psi\rangle$ 的信息无关

算法：用 QSVT 实现一个 $(2k+1)$ 次 Chebyshev 多项式

$(\sin\theta\ W)$ 的 block-encoding $\quad\mapsto\quad$ $((-1)^k\sin((2k+1)\theta)W)$ 的 block-encoding

$$\widetilde{V}|0\rangle|\psi\rangle = (-1)^k\sin((2k+1)\theta)\,|0\rangle W|\psi\rangle + |\perp\rangle$$

特例：

$$V|0\rangle|\psi\rangle = \frac{1}{2}|0\rangle W|\psi\rangle + |\perp\rangle \quad\to\quad \widetilde{V}|0\rangle|\psi\rangle = -|0\rangle W|\psi\rangle$$

局限：W 必须是酉矩阵

Uniform singular value amplification

设 A 是一个方阵，$\|A\| \leq 1$，U_A 是 A 的一个 $(1/a, *, 0)$-block-encoding **（$a \in (0,1)$）：**

$$U_A |0\rangle |\psi\rangle = a |0\rangle A |\psi\rangle + |\perp\rangle$$

目标：构造 A 的一个 $(c, *, \epsilon)$-block-encoding**，使得 c 尽可能接近于 1**

方法：通过 QSVT 实现 $f(aA)$（通过奇异值变换定义），其中 f 是一个奇函数，且满足

$$f(x) = x/a, \quad x \in [0, a].$$

- **不能直接用线性函数 x/a，因为它在 $[-1,1]$ 上绝对值并不总小于等于 1**

Uniform singular value amplification

Lemma (局部线性函数的多项式近似)

对于任意的 $a \in (0,1), \delta \in (0,1]$，$\epsilon \in (0, a/2)$，存在一个次数为 $d = \mathcal{O}(\frac{1}{a\delta}\log(\frac{1}{a\epsilon}))$ 的奇实多项式 $p(x)$，满足

$$\sup_{x\in[0,a]} |(1+\delta)p(x) - x/a| \leq \epsilon.$$

根据 QSVT，可以实现 $p(aA) \approx \frac{1}{1+\delta}A$

- A 的 $(\frac{1}{1+\delta}, *, \epsilon)$-block-encoding
- 访问复杂度：$\mathcal{O}(\frac{1}{a\delta}\log(\frac{1}{a\epsilon}))$

振幅放大：总结

- Grover：$U|0\rangle = \sqrt{p}\,|\psi_{\text{good}}\rangle + \sqrt{1-p}\,|\psi_{\text{bad}}\rangle$，对“好”和输入态做对称
- 子空间版 AA：$U|0\rangle\,|0\rangle = \sqrt{p}\,|0^a\rangle\,|\psi\rangle + |\perp\rangle$，对“好”的子空间和输入态做对称
- OAA：$U|0\rangle\,|\psi\rangle = \sqrt{p}\,|0\rangle\,V|\psi\rangle + |\perp\rangle$，$U, V$ 是酉变换，对“好”的子空间和整体酉变换做对称（与输入态无关）
- SVA/USVA：可放松 OAA 中 V 是酉变换的要求，但无法将振幅完全放大到 1
- ……

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

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

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

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

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

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

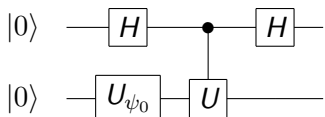
为了使 p 的误差小于 ϵ，只需 θ 的误差小于 ϵ

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



$$|0\rangle\,|0\rangle \to \frac{1}{2}\,|0\rangle\,(I+U)\,|\psi_0\rangle + \frac{1}{2}\,|1\rangle\,(I-U)\,|\psi_0\rangle \coloneqq \sqrt{p}\,|0\rangle\,|\psi_{\mathsf{good}}\rangle + \sqrt{1-p}\,|\psi_{\mathsf{bad}}\rangle$$

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

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