量子搜索算法探索历程

姜忠伟　赵临风

西北大学物理学院

2024 年 10 月 8 日

目录

1. 量子计算基础
2. 量子搜索算法
3. 量子搜索算法的下界
4. 龙算法
5. Abdulrahman 的工作

布洛赫变换

由模长为一且忽略全局相位，Bloch 球面表示为我们提供了一种更直观的方式来观察量子比特，即从量子比特到三维实球体的同构:

$$\mathbb{CP}^1 \to S^2$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \mapsto \vec{n}_\psi = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)^T.$$

这里 $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$.

SU2

From Lie group elements, any single-qubit unitary can be written as a product of exponentials of Pauli matrices by a global phase:

$$U = e^{i\alpha} \exp\left(-i\frac{\omega}{2}\vec{n}\cdot\vec{\sigma}\right), \tag{1}$$

which $\vec{n}$ is the coordinates of the rotation axis on the Bloch sphere. From the isomorphism **??**, we can also induce an isomorphism of operations on two spaces:

$$\begin{aligned} SU(2)/\{\pm 1\} &\to SO(3) \\ \exp\left(-i\frac{\omega}{2}\vec{n}\cdot\vec{\sigma}\right) &\mapsto \exp\left(\omega\vec{n}\cdot\vec{J}\right) \end{aligned} \tag{2}$$

which $\omega \in [0, \pi]$ and J_j are the three generators of Lie group $SO(3)$, the former refers to single-qubit gates and the latter to transformations on the Bloch sphere. For visualization and convenience, we let $R_{\vec{n}}(\omega) := \exp\left(-i\frac{\omega}{2}\vec{n}\cdot\vec{\sigma}\right)$.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{4}$$

背景

我们需要在包含 $N = 2^n$ 个元素的搜索空间 $S = \{0,1\}^n$ 中搜索目标元素 $T \subseteq S$，T 包含 M 个元素。将输出的目标元素和非目标元素分别表示为两个态

$$|\beta\rangle := \frac{1}{\sqrt{M}} \sum_{x \in T} |x\rangle \quad \text{and} \quad |\alpha\rangle := \frac{1}{\sqrt{N-M}} \sum_{x \notin T} |x\rangle . \tag{5}$$

考虑平凡的输入态

$$|\psi\rangle := H^{\otimes n} |0\rangle \tag{6}$$

这里将 $|0\rangle^{\otimes n}$ 简写为 $|0\rangle$。有性质

$$\langle \alpha | \beta \rangle = 0 \quad \text{and} \quad |\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle . \tag{7}$$

主要思路

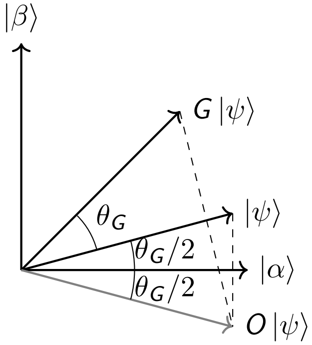


图 1: Grover's 算法可视化

为了让初态通过不断迭代逼近目标态，我们引入两个反射操作：

- O 是关于 $|\alpha\rangle$ 的反射；
- D 是关于 $|\psi\rangle$ 的反射。

Grover 迭代 $G = DO$ 给了我们一个 θ_G 的旋转，这里 $\sin(\theta_G/2) = \sqrt{M/N}$.

主要思路

初始态 $|\psi\rangle$ 通过

$$R := \left\lfloor \frac{\pi - \theta_G}{2\theta_G} \right\rceil \tag{8}$$

次迭代可以近似得到目标态 $|\beta\rangle$。

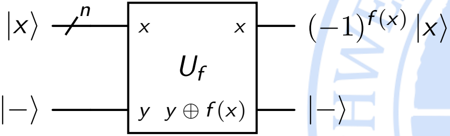
当 $M \ll N$，有

$$G^R |\psi\rangle = \cos(\frac{2R+1}{2}\theta_G) |\alpha\rangle + \sin(\frac{2R+1}{2}\theta_G) |\beta\rangle \approx |\beta\rangle\,. \tag{9}$$

具体实现

Oracle

由于 $|\alpha\rangle$ 和 $|\beta\rangle$ 是未确定的，我们需要构造一个操作对每个元素分别识别并反转



(10)

这一操作对态的影响是 $|x\rangle \xrightarrow{U_f} (-1)^{f(x)}\,|x\rangle$，据此可以构造映射

$$S(x) = \begin{cases} 1 & x \in T \\ 0 & x \notin T \end{cases} \tag{11}$$

$$\begin{aligned} U_S\,|\beta\rangle &= -\,|\beta\rangle \\ U_S\,|\alpha\rangle &= |\alpha\rangle\,. \end{aligned} \tag{12}$$

具体实现

Grover 迭代

Then, let's construct the reflection about $|\psi\rangle$. Same as the oracle, we decompose states into

$$|x\rangle = |\psi\rangle\langle\psi|x\rangle + |\psi_\perp\rangle\langle\psi_\perp|x\rangle \tag{13}$$

which $|\psi_\perp\rangle = \sqrt{\frac{M}{N}}|\alpha\rangle - \sqrt{\frac{N-M}{N}}|\beta\rangle$, and we wish

$$D|x\rangle = |\psi\rangle\langle\psi|x\rangle - |\psi_\perp\rangle\langle\psi_\perp|x\rangle. \tag{14}$$

But this time, we know $|\psi\rangle$ specifically, operation $2|\psi\rangle\langle\psi| - I$ is what we need. So we get the construction of the Grover iteration:

$$G = DO = (2|\psi\rangle\langle\psi| - I)U_S. \tag{15}$$

电路实现

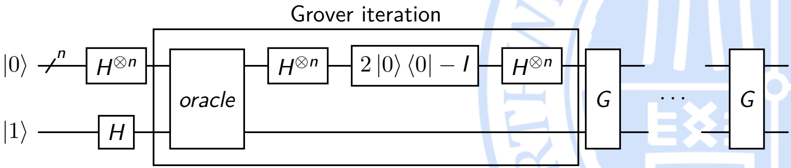


图 2: 量子搜索算法电路实现

主要思路

在 Grover 算法中，Oracle 是一个很特殊的操作，考虑将一部分 Oracle 替换成单位操作来观察 Oracle 带来的影响。

$$|\Psi_x^R\rangle = \prod_{j=1}^{R} U_j O_x |\psi\rangle \tag{16}$$

$$|\Psi_x^{i,R}\rangle = \prod_{j=i+1}^{R} U_j O_x \prod_{j=1}^{i} U_j I |\psi\rangle \tag{17}$$

$$|\Psi^R\rangle = \prod_{j=1}^{R} U_j I |\psi\rangle \tag{18}$$

考虑角度度量 $A(|\alpha\rangle, |\beta\rangle) = \arccos \frac{|\langle\alpha|\beta\rangle|}{\||\alpha\rangle\|\||\beta\rangle\|}$。对我们需要的目标元素的概率有距离

$$
\begin{aligned}
& A(|\Psi_x^R\rangle, |\Psi^R\rangle) \\
&= \arccos\left(\left|\langle\Psi_x^R|\Psi^R\rangle\right|\right) \\
&= \arccos\left(\langle\Psi_x^R| (\Pi_x + \Pi_x^\perp)^\dagger(\Pi_x + \Pi_x^\perp) |\Psi^R\rangle\right) \\
&= \arccos\left(\left\|\Pi_x |\Psi_x^R\rangle\right\| \cdot \left\|\Pi_x |\Psi^R\rangle\right\| + \left\|\Pi_x^\perp |\Psi_x^R\rangle\right\| \cdot \left\|\Pi_x^\perp |\Psi^R\rangle\right\|\right) \\
&= \arccos\left(\sin\phi_x^R \sin\theta_x^R + \cos\phi_x^R \cos\theta_x^R\right) \\
&= \phi_x^R - \theta_x^R \geq \arcsin\sqrt{p} - \theta_x^R
\end{aligned}
$$

可以计算

$$
\frac{1}{N}\sum_{x=1}^{N} A(|\Psi_x^R\rangle, |\Psi^R\rangle) \geq \arcsin\sqrt{p} - \frac{1}{N}\sum_{x=1}^{N}\theta_x^R \geq \arcsin\sqrt{p} - \arcsin\frac{1}{\sqrt{N}}
$$

考虑 R 次迭代有距离

$$
\begin{aligned}
&\frac{1}{N}\sum_{x=1}^{N} A(|\Psi_x^R\rangle, |\Psi^R\rangle) \\
&= \frac{1}{N}\sum_{x=1}^{N} A(|\Psi_x^{0,R}\rangle, |\Psi_x^{R,R}\rangle) \leq \frac{1}{N}\sum_{x=1}^{N}\sum_{i=1}^{R} A(|\Psi_x^{i-1,R}\rangle, |\Psi_x^{i,R}\rangle) \\
&= \frac{1}{N}\sum_{i=1}^{R}\sum_{x=1}^{N} A(O_x|\Psi^i\rangle, |\Psi^i\rangle) = \frac{1}{N}\sum_{i=1}^{R}\sum_{x=1}^{N} \arccos(\left|\cos(2\theta_x^i)\right|) \\
&\leq 2\sum_{i=1}^{R} \arcsin(\frac{1}{\sqrt{N}}) = 2R\arcsin(\frac{1}{\sqrt{N}}),
\end{aligned}
$$

可以看到 Oracle 带来的距离至多是线性增加的

$$\frac{1}{N}\sum_{x=1}^{N} A(|\Psi_x^R\rangle, |\Psi^R\rangle) \geq \arcsin\sqrt{p} - \arcsin\frac{1}{\sqrt{N}}. \tag{19}$$

$$\frac{1}{N}\sum_{x=1}^{N} A(|\Psi_x^R\rangle, |\Psi^R\rangle) \leq 2R\arcsin(\frac{1}{\sqrt{N}}). \tag{20}$$

$$R \geq \frac{\arcsin\sqrt{p} - \arcsin\frac{1}{\sqrt{N}}}{2\arcsin\frac{1}{\sqrt{N}}}. \tag{21}$$

主要思路

有时我们需要更精确的达到目标态。考虑经典 Grover 算法中没利用的相对相位，拓展 Grover 迭代

$$G = DO = (I - 2\left|\psi_\perp\right\rangle\left\langle\psi_\perp\right|)(I - 2\left|\beta\right\rangle\left\langle\beta\right|) \tag{22}$$

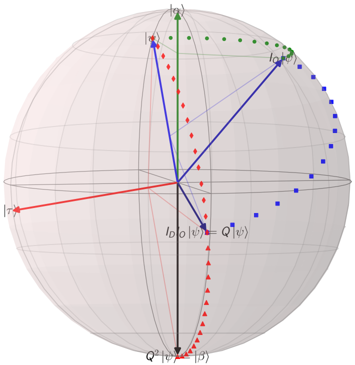
至

$$I_D = I + (e^{-i\phi} - 1)\left|\psi_\perp\right\rangle\left\langle\psi_\perp\right| = e^{-i\phi}(I + (e^{i\phi} - 1)\left|\psi\right\rangle\left\langle\psi\right|)$$

$$I_O = I + (e^{i\phi} - 1)\left|\beta\right\rangle\left\langle\beta\right|$$

$$Q = I_D I_O = e^{-i\phi}H^{\otimes n}(I + (e^{i\phi} - 1)\left|0\right\rangle\left\langle0\right|)H^{\otimes n}(I + (e^{i\phi} - 1)\left|\beta\right\rangle\left\langle\beta\right|).$$

主要思路



$$\omega = 4\arcsin(\sin\frac{\phi}{2}\sin\frac{\theta_G}{2})$$

$$\vec{r}_\tau = k(\cos\frac{\phi}{2}, \sin\frac{\phi}{2}, \cos\frac{\phi}{2}\tan\frac{\theta_G}{2})^T$$

$$\Delta\varphi = 2\arccos(\sin\frac{\phi}{2}\sin\frac{\theta_G}{2})$$

引入

从式4，可以看到当 N 足够大时有

$$R \propto 1/\theta_G \tag{23}$$

我们可以尝试找到更大的角度来减少迭代次数。

我们需要一个更大的状态空间。对比 $|\psi\rangle$，引入独立于目标态的态

$$|\overline{\psi}\rangle := H^{\otimes n}(|0\rangle^{\otimes n-1} \otimes |1\rangle) \tag{24}$$

来扩充空间。

主要思路

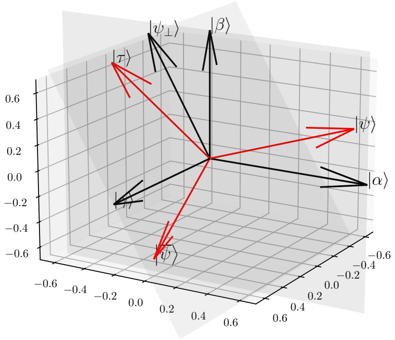


图 3: 正交基 $(|\overline{\psi}\rangle, |\psi\rangle, |\tau\rangle)$

可以计算的是

$$\langle\psi_\perp|\overline{\psi}\rangle = \pm\sqrt{\frac{1}{N-1}} \tag{25}$$

当且仅当目标元素的最后一位是 0 时取正，我们不妨先讨论取正这种情况。

主要思路

在对扩张的空间有基本了解之后，考虑一个独立于目标元素的在 $|\psi\rangle$ 和 $|\overline{\psi}\rangle$ 张成的平面内的旋转，在子空间 $(|\overline{\psi}\rangle, |\psi\rangle, |\tau\rangle)$ 中可以写成

$$A(\phi) := H^{\otimes n} X^{\otimes n} c^{n-1}\left(R_y(\phi)\right) X^{\otimes n} H^{\otimes n} = \begin{pmatrix} \cos\frac{\phi}{2} & -\sin\frac{\phi}{2} & 0 \\ \sin\frac{\phi}{2} & \cos\frac{\phi}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

主要思路

我们的期望是使目标元素的概率最大。容易看出的是在旋转 $A(\phi)$ 的作用下，态们仅在转到 $|\gamma\rangle$ 和 $|\beta\rangle$ 张成的平面中时目标态的概率最大。

所以我们拓展 Grover 迭代 $G = DO$ 为

$$Q = A(\phi)G = A(\phi)DO, \tag{26}$$

来保证每次 Grover 迭代后，态都回到这个平面。

具体实现

为了方便我们用基 $(|\overline{\psi}\rangle, |\psi\rangle, |\tau\rangle)$ 和球坐标 $(x, y, z)^T \to (\sin\frac{\theta}{2}\sin\varphi, \sin\frac{\theta}{2}\cos\varphi, \cos\frac{\theta}{2})^T$ 来描述这个空间。

可以计算的是

$$|\beta\rangle = (\sin\frac{\theta_Q}{2}\sin\frac{\pi}{4}, \sin\frac{\theta_Q}{2}\cos\frac{\pi}{4}, \cos\frac{\theta_Q}{2})^T, \tag{27}$$

这里 $\sin(\theta_Q/2) = \sqrt{2/N}$，所以 $|\gamma\rangle$ 和 $|\beta\rangle$ 张成的平面可以写成 $\varphi = \pi/4$。

具体实现

我们先将输入态转进平面 $\varphi = \pi/4$，我们对 $|\psi\rangle$ 做操作

$$A_0 := A(-2(\varphi_\beta - \varphi_\psi)) = A(-\pi/2) \tag{28}$$

于是有

$$A_0 |\psi\rangle = (\sin\frac{\pi}{4}, \cos\frac{\pi}{4}, 0)^T. \tag{29}$$

具体实现

接下来让我们考虑 Grover 迭代对 φ 的影响，对平面中的态操作 Oracle 给出映射

$$O: \frac{\theta}{2} \to \pi - \frac{\theta}{2} + \theta_Q \qquad \varphi \to \varphi \tag{30}$$

扩散操作 D 给出映射

$$D: \frac{\theta}{2} \to \pi - \frac{\theta}{2} \qquad \varphi \to -\varphi. \tag{31}$$

与 A_0 类似，我们用 $A := A(-2(\varphi - (-\varphi))) = A(-\pi)$ 来将角度拉回。

具体实现

所以操作 $Q = AG$ 给出映射

$$Q = AG\colon \frac{\theta}{2} \to \frac{\theta}{2} - \theta_Q \qquad (32)$$
$$\varphi \to \varphi.$$

可以看到 Q 保持 φ 不变，我们不妨取出平面 $\varphi = \pi/4$ 来观察 Q 对 θ 的影响。

具体实现

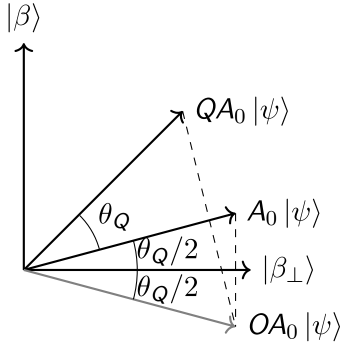


图 4:

和经典 Grover 类似，对 $A_0|\psi\rangle$ 应用

$$R_Q = \left\lfloor \frac{\pi - \theta_Q/2}{\theta_Q} \right\rceil \tag{33}$$

次操作 Q，有

$$Q^{R_Q} A_0 |\psi\rangle = \cos(\frac{2R_Q+1}{2}\theta_Q)|\beta_\perp\rangle + \sin(\frac{2R_Q+1}{2}\theta_Q)|\beta\rangle \approx |\beta\rangle.$$

性能

可以看到与经典的迭代次数的比

$$R_Q/R \approx \theta_G/\theta_Q \approx 1/\sqrt{2} \tag{34}$$

这似乎违反了我们曾算过的下界。

可以计算的是，如果目标元素的最后一位是 1，有 $A_0 = A(\pi/2)$ 和 $A = A(\pi)$，所以必须要先辨别结果的最后一位，我们才能有效的迭代，这就是加速的来源。

结果

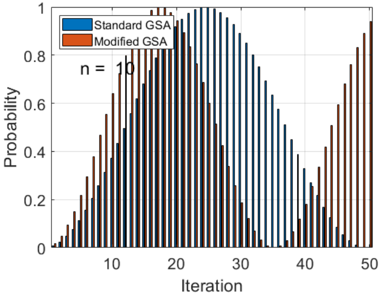


图 5: 目标态 0 结尾

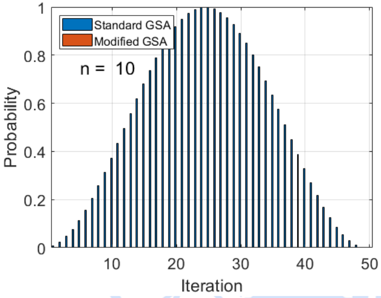


图 6: 目标态 1 结尾

Best Wishes!