6.1 量子搜索算法——习题与解答

DanX, and Shan Jin *

练习 6.1 (Grover 相移的酉算符)**.** 证明对应于 *Grover* 迭代中“把 $|0\rangle$ 保持不变、对所有 $|x>0\rangle$ 加上相位 -1”的相移酉算符是

$$S = 2\,|0\rangle\langle 0| - I.$$

解答. 相移算符 S 的定义效果是:

$$S\,|0\rangle = |0\rangle\,, \qquad S\,|x\rangle = -\,|x\rangle \quad (x>0).$$

1. 用对基矢的作用来验证。

对 $|0\rangle$:

$$S\,|0\rangle = (2\,|0\rangle\langle 0| - I)\,|0\rangle = 2\,|0\rangle\langle 0|0\rangle - |0\rangle = 2\,|0\rangle - |0\rangle = |0\rangle\,.$$

对任意 $|x\rangle$ 且 $x>0$:

$$S\,|x\rangle = (2\,|0\rangle\langle 0| - I)\,|x\rangle = 2\,|0\rangle\langle 0|x\rangle - |x\rangle\,.$$

由于 $\langle 0|x\rangle = 0$（计算基正交），所以

$$S\,|x\rangle = -\,|x\rangle\,, \qquad x>0.$$

这恰好就是题目描述的相移作用：$|0\rangle$ 不变，其余所有基态都乘以 -1。

2. 从矩阵角度看。

在计算基 $\{|0\rangle, |1\rangle, \dots\}$ 下，$|0\rangle\langle 0|$ 是对角线上只有第一个元为 1 的投影，所以

$$2\,|0\rangle\langle 0| - I = \mathrm{diag}(1,-1,-1,\dots),$$

也就是对第一分量给相位 $+1$，其他分量给相位 -1。这和 Grover 迭代中要求的相移完全一致。 □

练习 6.2 (“关于均值的反演”)**.** 设均匀叠加态

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,,$$

对一般态

$$|\phi\rangle = \sum_{k=0}^{N-1}\alpha_k\,|k\rangle$$

作用算符

$$D := 2\,|\psi\rangle\langle\psi| - I,$$

证明

$$D\,|\phi\rangle = \sum_{k=0}^{N-1}\big(-\alpha_k + 2\langle\alpha\rangle\big)\,|k\rangle\,,$$

*jinshan@tgqs.net

其中

$$\langle\alpha\rangle := \frac{1}{N}\sum_{k=0}^{N-1}\alpha_k$$

是振幅的算术平均值。说明为什么 D 可以称为“关于均值的反演”算符。

解答. **1. 先写出 $|\psi\rangle\langle\psi|$ 的形式。**

由定义

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle,$$

故

$$|\psi\rangle\langle\psi| = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}|x\rangle\langle y|.$$

2. 计算 $|\psi\rangle\langle\psi|\phi\rangle$。

将 $|\phi\rangle = \sum_{k=0}^{N-1}\alpha_k|k\rangle$ 代入：

$$\begin{aligned}
|\psi\rangle\langle\psi|\phi\rangle &= \frac{1}{N}\sum_{x,y}|x\rangle\langle y|\sum_k \alpha_k|k\rangle \\
&= \frac{1}{N}\sum_{x,y,k}\alpha_k|x\rangle\langle y|k\rangle \\
&= \frac{1}{N}\sum_{x,k}\alpha_k|x\rangle \quad (\text{因为}\langle y|k\rangle = \delta_{yk}) \\
&= \frac{\sum_k \alpha_k}{N}\sum_x|x\rangle.
\end{aligned}$$

记振幅均值

$$\langle\alpha\rangle = \frac{1}{N}\sum_{k=0}^{N-1}\alpha_k,$$

则

$$|\psi\rangle\langle\psi|\phi\rangle = \langle\alpha\rangle\sum_{x=0}^{N-1}|x\rangle = \sum_{k=0}^{N-1}\langle\alpha\rangle|k\rangle.$$

也就是说，$|\psi\rangle\langle\psi|$ 把原来各个分量 α_k 全都“抹掉”，统一变成均值 $\langle\alpha\rangle$。

3. 再作用 $D = 2|\psi\rangle\langle\psi| - I$。

有

$$D|\phi\rangle = 2|\psi\rangle\langle\psi|\phi\rangle - |\phi\rangle.$$

利用上面的结果：

$$2|\psi\rangle\langle\psi|\phi\rangle = 2\sum_{k=0}^{N-1}\langle\alpha\rangle|k\rangle,$$

而

$$|\phi\rangle = \sum_{k=0}^{N-1}\alpha_k|k\rangle.$$

于是

$$\begin{aligned}
D|\phi\rangle &= \sum_{k=0}^{N-1}\big(2\langle\alpha\rangle - \alpha_k\big)|k\rangle \\
&= \sum_{k=0}^{N-1}\big(-\alpha_k + 2\langle\alpha\rangle\big)|k\rangle.
\end{aligned}$$

4. “关于均值的反演”的含义。

对每个分量 α_k，新振幅为

$$\alpha_k' = -\alpha_k + 2\langle\alpha\rangle = 2\langle\alpha\rangle - \alpha_k.$$

这正好是以 $\langle\alpha\rangle$ 为中心，把 α_k 反射到另一侧的结果（在复平面上沿通过 $\langle\alpha\rangle$ 的直线镜像）。所以 D 可以形象地理解为“绕均值振幅做反射”，即“关于均值的反演”。 □

练习 6.3 (在 $|\alpha\rangle, |\beta\rangle$ 基中的 Grover 迭代)**.** 设

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle,$$

其中 $|\alpha\rangle$ 是所有“非解”均匀叠加，$|\beta\rangle$ 是所有“解”均匀叠加，且 $1 \le M \le N/2$。

证明：在基 $\{|\alpha\rangle, |\beta\rangle\}$ 下，*Grover* 迭代

$$G = (2\,|\psi\rangle\langle\psi| - I)\,O$$

可以写成

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

其中

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}.$$

解答. **1. 先验证 $\sin\theta$ 的表达式。**

由

$$|\psi\rangle = \sqrt{\tfrac{N-M}{N}}\,|\alpha\rangle + \sqrt{\tfrac{M}{N}}\,|\beta\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle,$$

可得

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}, \qquad \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

因此

$$\sin\theta = 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = 2\sqrt{\frac{M}{N}}\sqrt{\frac{N-M}{N}} = \frac{2\sqrt{M(N-M)}}{N},$$

与题目给出的表达式一致。

2. 写出 $|\psi\rangle\langle\psi|$ 的矩阵。

在基 $\{|\alpha\rangle, |\beta\rangle\}$ 下有

$$|\psi\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix},$$

故

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix}.$$

利用

$$\cos^2\tfrac{\theta}{2} = \frac{1+\cos\theta}{2}, \quad \sin^2\tfrac{\theta}{2} = \frac{1-\cos\theta}{2}, \quad \sin\tfrac{\theta}{2}\cos\tfrac{\theta}{2} = \frac{\sin\theta}{2},$$

得到

$$|\psi\rangle\langle\psi| = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \sin\theta \\ \sin\theta & 1-\cos\theta \end{pmatrix}.$$

于是

$$2\left|\psi\right\rangle\left\langle\psi\right|-I=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}.$$

3. 写出 oracle O 的矩阵。

oracle O 的定义是：对“非解”保持不变，对“解”加相位 -1。在 $\{|\alpha\rangle,|\beta\rangle\}$ 基下，

$$O\left|\alpha\right\rangle=\left|\alpha\right\rangle,\qquad O\left|\beta\right\rangle=-\left|\beta\right\rangle,$$

因此

$$O=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

4. 计算 Grover 迭代 G 的矩阵。

$$\begin{aligned}G&=\left(2\left|\psi\right\rangle\left\langle\psi\right|-I\right)O\\&=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\\&=\begin{pmatrix}\cos\theta\cdot1+\sin\theta\cdot0 & \cos\theta\cdot0+\sin\theta\cdot(-1)\\ \sin\theta\cdot1+(-\cos\theta)\cdot0 & \sin\theta\cdot0+(-\cos\theta)\cdot(-1)\end{pmatrix}\\&=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.\end{aligned}$$

这是标准的二维旋转矩阵：在 $\{|\alpha\rangle,|\beta\rangle\}$ 平面内，将向量逆时针旋转角度 θ。 □

练习 6.4 (多解情形下的 Grover 算法步骤)**.** 在存在多个解的情形下，设满足条件的输入个数为 M，且 $1<M<N/2$。仿照书中单解情形的描述，写出量子搜索算法的具体步骤。

解答. 多解情形下，Grover 算法的结构与单解时完全相同，只是迭代次数不同。给出典型步骤如下（假设 M 已知）：

1. **初始化**。令有 n 个输入比特，$N=2^n$。从全零态

   $$\left|0\right\rangle^{\otimes n}\left|0\right\rangle$$

   出发，其中前 n 个比特为“地址寄存器”，最后一个比特为 oracle 工作比特。

2. **制备均匀叠加态**。对前 n 个比特各作用 Hadamard 门，对工作比特作用 H 后再作用 Z（或直接制备 $|-\rangle$ 态）。得到

   $$\left|\psi\right\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\left|x\right\rangle\left|-\right\rangle.$$

3. **定义 Grover 迭代算符**。

   - oracle O：对满足 $f(x)=1$ 的 $|x\rangle$ 加相位 -1，其余不变；
   - “扩散”算符（反演关于均值）

     $$D=2\left|\psi\right\rangle\left\langle\psi\right|-I$$

     作用在地址寄存器上；

- Grover 迭代

$$G = D\,O.$$

4. **选择迭代次数**。对多解情形，最佳迭代次数满足

$$R \approx \frac{\pi}{4}\sqrt{\frac{N}{M}},$$

通常取

$$R = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor \quad \text{或} \quad R = \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil .$$

5. **重复 Grover 迭代**。对地址寄存器施加 R 次迭代：

$$|\psi_{\text{out}}\rangle = G^R\,|\psi\rangle\,.$$

在 $\{|\alpha\rangle, |\beta\rangle\}$ 平面中，这相当于把初始向量旋转到尽量靠近“解子空间”方向。

6. **测量并输出**。在计算基下测量地址寄存器，得到的结果落在解集合中的概率约为常数（接近 1）。如有需要，可以重复整个算法若干次，以进一步提高成功率。

与单解情形相比，唯一的本质区别就是 R 的取值由 $\sqrt{N}$ 换成了 $\sqrt{N/M}$。 □

练习 6.5 (构造增广 oracle O')**.** 设有 *Grover* 算法中的标准 *oracle* O，它作用在 $|x\rangle\,|y\rangle$ 上为

$$O\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle\,,$$

其中 $f(x) \in \{0,1\}$。通过“相位踢回”，对工作比特取 $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ 可得到

$$O\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

证明：只用一次 O 调用、基本单比特门与一个附加的控制比特 $|q\rangle$，可以构造增广 *oracle* O'，其效果是：

$$O'\,|q\rangle\,|x\rangle\,|-\rangle = \begin{cases} (-1)^{f(x)}\,|0\rangle\,|x\rangle\,|-\rangle\,, & q = 0, \\ |1\rangle\,|x\rangle\,|-\rangle\,, & q = 1, \end{cases}$$

也就是：当 $q = 0$ 时按原 *oracle* 标记解；当 $q = 1$ 时“关闭”标记。

解答. 构造思路：对“希望标记”的分支（$q = 0$）让 oracle 像平常那样工作；对“关闭标记”的分支（$q = 1$），利用额外的 Z 门把相位踢回效果抵消掉。

1. 电路结构（文字描述）。

考虑 3 个量子比特：$|q\rangle$（控制）、$|x\rangle$（输入寄存器）、以及工作比特 $|w\rangle$ 初态取 $|-\rangle$。

构造如下线路：

1. 对工作比特施加一个受控-Z 门，以 q 为控制（记作 $\mathrm{CZ}_{q\to w}$）；
2. 作用一次未增广的 oracle O 于 $|x\rangle\,|w\rangle$；
3. 再对工作比特施加同一个受控-Z 门 $\mathrm{CZ}_{q\to w}$。

整个算符可写成

$$O' = (\mathrm{CZ}_{q\to w})\, O\, (\mathrm{CZ}_{q\to w}).$$

2. 分情况分析：$q = 0$ 分支。

初态取

$$|\Psi_{\mathrm{in}}\rangle = |0\rangle\,|x\rangle\,|-\rangle\,, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

第一步： 受控-Z 以 q 为控制。控制比特为 $|0\rangle$ 时，门不起作用，因此工作比特仍为 $|-\rangle$。

第二步： 作用 oracle O 在 $|x\rangle\,|-\rangle$ 上，根据相位踢回性质：

$$O\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|x\rangle\,|-\rangle\,.$$

所以

$$|\Psi_2\rangle = (-1)^{f(x)}\,|0\rangle\,|x\rangle\,|-\rangle\,.$$

第三步： 再次受控-Z 仍然不起作用（控制比特是 $|0\rangle$），因此最终得到

$$O'\,|0\rangle\,|x\rangle\,|-\rangle = (-1)^{f(x)}\,|0\rangle\,|x\rangle\,|-\rangle\,,$$

如题目所需。

3. 分情况分析：$q = 1$ 分支。

初态

$$|\Psi_{\mathrm{in}}\rangle = |1\rangle\,|x\rangle\,|-\rangle\,.$$

第一步： 受控-Z。现在控制比特为 $|1\rangle$，因此对工作比特作用 Z：

$$Z\,|-\rangle = Z\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} =: |+\rangle\,.$$

故

$$|\Psi_1\rangle = |1\rangle\,|x\rangle\,|+\rangle\,.$$

第二步： 作用 oracle O 于 $|x\rangle\,|+\rangle$。利用定义

$$O\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle\,,$$

对 $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 有

$$\begin{aligned} O\,|x\rangle\,|+\rangle &= \frac{1}{\sqrt{2}}\Big(|x\rangle\,|0 \oplus f(x)\rangle + |x\rangle\,|1 \oplus f(x)\rangle\Big) \\ &= \frac{1}{\sqrt{2}}\big(|x\rangle\,|0\rangle + |x\rangle\,|1\rangle\big) = |x\rangle\,|+\rangle\,, \end{aligned}$$

也就是说，$|+\rangle$ 是 O 的本征态，本征值为 $+1$，不产生相位。

所以

$$|\Psi_2\rangle = |1\rangle\,|x\rangle\,|+\rangle\,.$$

第三步： 再次受控-Z：

$$Z\,|+\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle\,.$$

于是

$$|\Psi_{\mathrm{out}}\rangle = |1\rangle\,|x\rangle\,|-\rangle\,.$$

4. 总结。

两种分支的最终效果：

$$O'|q\rangle|x\rangle|-\rangle = \begin{cases} (-1)^{f(x)}|0\rangle|x\rangle|-\rangle, & q=0, \\ |1\rangle|x\rangle|-\rangle, & q=1. \end{cases}$$

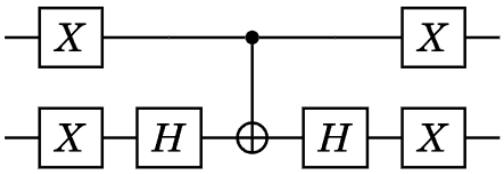
因此，用一次 O 调用，加上前后两个受控-Z 门，就实现了所需的增广 oracle O'：当 $q=0$ 时按原 oracle 标记解，$q=1$ 时完全不标记。 □

练习 6.6 (两比特相移门的实现). 书中盒子 *6.1* 第二个图给出了一个由若干基本门组成的两比特门，作用结果应当与相移算符

$$S_{00} = 2|00\rangle\langle 00| - I$$

只差一个无关紧要的全局相位因子 α。

验证：



$$= e^{i\alpha}(2|00\rangle\langle 00| - I)$$

解答. 根据题干提示，盒子中的门路可以这样等价化简（只描述关键恒等式）。

1. 把控制从“以 $|1\rangle$ 为控”变成“以 $|0\rangle$ 为控”。

对于第一个量子比特，控制点两侧各有一个 X 门。众所周知

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle,$$

所以

$$X\,(\text{以}\,|1\rangle\ \text{为控})\,X = (\text{以}\,|0\rangle\ \text{为控}).$$

因此，在电路整体上，相当于实现了一个“以 $|0\rangle$ 为控制”的受控门。

2. 化简第二个量子比特上的门序列。

盒子里的第二条线上有一串 X, H, X, H, X 之类的门。利用以下恒等式：

- $HXH = Z$；
- $XZX = -Z$（可由 Pauli 矩阵反对易性 $XZ = -ZX$ 得出）；
- $H^2 = I$。

可以得到

$$XHXHX = X(HXH)X = XZX = -Z,$$

而另一条支路上的

$$XHHX = XIX = I.$$

因此，整个带点的框等价于：当第一个量子比特处于 $|0\rangle$ 时，在第二个量子比特上施加 $-Z$；否则不作用。这就是一个“以 $|0\rangle$ 为控制的受控 $-Z$ 门”。

3. 写出这个门的矩阵表示。

在基 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 下：

- 当第一比特为 $|0\rangle$ 时，对第二比特施加 $-Z$：

$$-Z\,|0\rangle = -\,|0\rangle\,, \qquad -Z\,|1\rangle = +\,|1\rangle\,.$$

所以

$$|00\rangle \mapsto -\,|00\rangle\,, \qquad |01\rangle \mapsto |01\rangle\,.$$

- 当第一比特为 $|1\rangle$ 时，不作用第二比特，所以

$$|10\rangle \mapsto |10\rangle\,, \qquad |11\rangle \mapsto |11\rangle\,.$$

总的作用为：

$$|00\rangle \mapsto -\,|00\rangle\,, \quad |01\rangle \mapsto |01\rangle\,, \quad |10\rangle \mapsto |10\rangle\,, \quad |11\rangle \mapsto |11\rangle\,.$$

这对应的算符为

$$U = -\,|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|\,.$$

注意到

$$I = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|\,,$$

因此

$$U = -2\,|00\rangle\langle 00| + I.$$

4. 与 $2\,|00\rangle\langle 00| - I$ 的关系。

比较

$$-2\,|00\rangle\langle 00| + I \quad \text{和} \quad 2\,|00\rangle\langle 00| - I,$$

容易看出

$$-2\,|00\rangle\langle 00| + I = -\big(2\,|00\rangle\langle 00| - I\big) = e^{i\pi}\big(2\,|00\rangle\langle 00| - I\big).$$

即该门与相移算符 $2\,|00\rangle\langle 00| - I$ 只差一个全局相位 $e^{i\pi}$，从物理上来说是完全等价的。 □