# 6.6 搜索算法的最优性——习题与解答

DanX, and Shan Jin *

**练习 6.15** (Cauchy–Schwarz 不等式的应用)**.** *利用 Cauchy–Schwarz 不等式，证明：对任何归一化状态向量 $|\psi\rangle$ 和一组含有 $N$ 个向量的正交归一基 $\{|x\rangle\}_{x=1}^{N}$，都有*

$$\sum_{x}\big\| \,|\psi\rangle - |x\rangle\,\big\|^{2} \geq 2N - 2\sqrt{N}.$$

**解答.** **(1) 逐项展开范数平方。**

对固定的基向量 $|x\rangle$，有

$$\begin{aligned}\big\||\psi\rangle - |x\rangle\big\|^{2} &= \big(\langle\psi| - \langle x|\big)\big(|\psi\rangle - |x\rangle\big)\\ &= \langle\psi|\psi\rangle - \langle\psi|x\rangle - \langle x|\psi\rangle + \langle x|x\rangle\,.\end{aligned}$$

因为 $|\psi\rangle$ 归一化、$|x\rangle$ 也归一化，故

$$\langle\psi|\psi\rangle = 1, \qquad \langle x|x\rangle = 1.$$

于是

$$\big\||\psi\rangle - |x\rangle\big\|^{2} = 2 - \langle\psi|x\rangle - \langle x|\psi\rangle = 2 - 2\ \mathrm{Re}\big(\langle\psi|x\rangle\big),$$

其中 $\mathrm{Re}(z)$ 表示复数 $z$ 的实部。

**(2) 对全部基向量求和。**

对 $x$ 求和，注意一共有 $N$ 个基向量：

$$\sum_{x}\big\||\psi\rangle - |x\rangle\big\|^{2} = \sum_{x}\Big(2 - 2\ \mathrm{Re}\big(\langle\psi|x\rangle\big)\Big) = 2N - 2\ \mathrm{Re}\Big(\sum_{x}\langle\psi|x\rangle\Big).$$

现在把求和改写成与某个平均态的内积。定义

$$|\chi\rangle := \frac{1}{\sqrt{N}}\sum_{x}|x\rangle\,,$$

显然 $|\chi\rangle$ 也是归一化态，因为

$$\langle\chi|\chi\rangle = \frac{1}{N}\sum_{x,x'}\langle x|x'\rangle = \frac{1}{N}\sum_{x}1 = 1.$$

于是

$$\sum_{x}\langle\psi|x\rangle = \sqrt{N}\ \langle\psi|\chi\rangle\,,$$

从而

$$\sum_{x}\big\||\psi\rangle - |x\rangle\big\|^{2} = 2N - 2\sqrt{N}\ \mathrm{Re}\big(\langle\psi|\chi\rangle\big).$$

*jinshan@tgqs.net

**(3) 用 Cauchy–Schwarz 不等式给出下界。**

对归一化态 $|\psi\rangle, |\chi\rangle$，Cauchy–Schwarz 不等式给出

$$\big|\langle\psi|\chi\rangle\big| \le \|\psi\|\,\|\chi\| = 1.$$

实部不超过模长，因此

$$\mathrm{Re}\big(\langle\psi|\chi\rangle\big) \le \big|\langle\psi|\chi\rangle\big| \le 1.$$

将这一点代入刚才的表达式：

$$\sum_x \big\||\psi\rangle - |x\rangle\big\|^2 = 2N - 2\sqrt{N}\,\mathrm{Re}\big(\langle\psi|\chi\rangle\big) \ge 2N - 2\sqrt{N}\cdot 1 = 2N - 2\sqrt{N}.$$

**(4) 等号何时成立？**

要使等号成立，必须同时满足

$$\big|\langle\psi|\chi\rangle\big| = 1, \qquad \mathrm{Re}\big(\langle\psi|\chi\rangle\big) = 1.$$

第一条说明 $|\psi\rangle$ 与 $|\chi\rangle$ 只差一个全局相位；第二条说明这个相位必须是 1（否则实部小于 1）。

因此只有当

$$|\psi\rangle = |\chi\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$$

时等号取到。证明完毕。 □

**练习 6.16** (平均意义下的成功概率)**.** 设搜索问题的条件稍作修改：不再要求对所有可能的解 $x$，算法的错误概率都小于 $1/2$，而是只要求在对 $x$ 的均匀平均下，错误概率小于 $1/2$。即若 $k$ 次 *oracle* 调用后、在 $x$ 为解时系统处于 $|\psi_k^x\rangle$，则新的条件是

$$\frac{1}{N}\sum_x \big|\langle x|\psi_k^x\rangle\big|^2 \ge \frac{1}{2}.$$

证明：在这种较弱的条件下，$O(\sqrt{N})$ 次 *oracle* 调用仍然是必需的。

**解答.** 思路是：沿用书中对 Grover 算法最优性的证明，只是把“对所有 $x$ 成功”的条件换成“对 $x$ 的平均成功”的条件，重新估计量

$$E_k := \sum_x \big\||\psi_k^x\rangle - |x\rangle\big\|^2$$

的上界，然后代回书中给出的关键不等式即可。

**(1) 重新估计 $E_k$ 的上界。**

与上一题类似，对每个 $x$ 有

$$\big\||\psi_k^x\rangle - |x\rangle\big\|^2 = 2 - 2\,\mathrm{Re}\big(\langle\psi_k^x|x\rangle\big),$$

因此

$$\begin{aligned} E_k &= \sum_x \big\||\psi_k^x\rangle - |x\rangle\big\|^2 \\ &= \sum_x \Big(2 - 2\,\mathrm{Re}\big(\langle\psi_k^x|x\rangle\big)\Big) \\ &= 2N - 2\sum_x \mathrm{Re}\big(\langle\psi_k^x|x\rangle\big). \end{aligned}$$

利用 $\mathrm{Re}(z) \geq -|z|$ 或者更直接地，注意到对任意复数 $z$，

$$\mathrm{Re}(z) \leq |z|,$$

故

$$E_k \leq 2N - 2\sum_x \left|\langle\psi_k^x|x\rangle\right|.$$

另一方面，由于振幅的模不超过 1，有

$$|z| \geq |z|^2, \qquad (|z| \leq 1),$$

于是对每个 $x$，

$$\left|\langle\psi_k^x|x\rangle\right| \geq \left|\langle x|\psi_k^x\rangle\right|^2.$$

（这里用到 $\left|\langle\psi_k^x|x\rangle\right| = \left|\langle x|\psi_k^x\rangle\right|$。）

对 $x$ 求和，结合题设的平均成功条件：

$$\sum_x \left|\langle\psi_k^x|x\rangle\right| \geq \sum_x \left|\langle x|\psi_k^x\rangle\right|^2 \geq \frac{N}{2}.$$

代回 $E_k$ 的上界：

$$E_k \leq 2N - 2\cdot\frac{N}{2} = N.$$

**(2) 利用书中的关键不等式。**

书中对搜索最优性的证明中，引入了三个量（这里直接引用其结构）：

- $F_k$：只依赖于“无解”情况下得到的那一族状态，与 $|\psi_k^x\rangle$ 无关；
- $E_k := \sum_x \||\psi_k^x\rangle - |x\rangle\|^2$（我们刚刚估计了上界）；
- $D_k$：衡量带 oracle 与不带 oracle 两种演化之间“总体差异”的量。

书中证明得到两个重要不等式（这里直接使用）：

$$D_k \leq 4k^2, \qquad D_k \geq \left(\sqrt{F_k} - \sqrt{E_k}\right)^2.$$

另一方面，由练习 6.15 的结果可知，对任意态族 $\{|\phi_k^x\rangle\}$ 与正交归一基 $\{|x\rangle\}$，总有

$$F_k := \sum_x \left\||\phi_k^x\rangle - |x\rangle\right\|^2 \geq 2N - 2\sqrt{N}.$$

在 Grover 搜索最优性证明中，$|\phi_k^x\rangle$ 的选择方式使得这个下界同样适用，因此我们可以认为

$$F_k \geq 2N - 2\sqrt{N} \quad \text{（这一点与成功概率条件无关）}.$$

而上一小节得到

$$E_k \leq N.$$

于是

$$\begin{aligned} D_k &\geq \left(\sqrt{F_k} - \sqrt{E_k}\right)^2 \\ &\geq \left(\sqrt{2N - 2\sqrt{N}} - \sqrt{N}\right)^2. \end{aligned}$$

对大 $N$，我们可以把 $2N - 2\sqrt{N}$ 看作略小于 $2N$，所以

$$\sqrt{2N - 2\sqrt{N}} > \sqrt{2N} - 1.$$

粗略估计即可看出

$$\left(\sqrt{2N-2\sqrt{N}}-\sqrt{N}\right)^2 > (\sqrt{2}-1)^2\,N,$$

其中 $(\sqrt{2}-1)^2 \approx 0.17$ 是一个正的常数。

于是得到

$$4k^2 \geq D_k > (\sqrt{2}-1)^2\,N.$$

**(3) 得到对 $k$ 的下界。**

令 $c$ 为任何小于 $(\sqrt{2}-1)^2$ 的常数，则上式蕴含

$$4k^2 \geq cN \quad \Rightarrow \quad k \geq \sqrt{\frac{c}{4}}\sqrt{N} = \Omega(\sqrt{N}).$$

因此，即使只要求平均意义下的错误概率小于 $1/2$，Grover 型搜索仍然必须使用 $\Omega(\sqrt{N})$ 量级的 oracle 调用。结合 Grover 算法的 $O(\sqrt{N})$ 上界，说明 $O(\sqrt{N})$ 仍然是最优阶。 □

**练习 6.17** (对多重解的最优性)**.** 假设搜索问题在 $N$ 个备选项中有 $M$ 个解（记为“标记元素”），即 *oracle* 对这些解的输出为 1，对其他输入输出为 0。证明：为了找到任意一个解，仍然需要 $\Omega\left(\sqrt{N/M}\right)$ 次 *oracle* 调用。

**解答.** 这里给出一个比较简洁的归约证明思路：我们已知“单解搜索”必须使用 $\Omega(\sqrt{N})$ 次 oracle 调用；我们将证明若存在比 $O\left(\sqrt{N/M}\right)$ 更快的“多解搜索”算法，就可以构造出更快的“单解搜索”算法，从而与已知下界矛盾。

为方便叙述，先假设 $N$ 是 $M$ 的整数倍，即

$$N = N'M,$$

其中 $N'$ 为正整数。非整除情形可以通过填充若干“永远不是解”的虚拟元素处理，不影响渐近阶。

**(1) 单解搜索问题与多解搜索问题。**

- **单解搜索问题（规模 $N'$）：** 给定一个未知标记位置 $y \in \{1,\dots,N'\}$，oracle $O_y$ 作用为

$$O_y\,|j\rangle = \begin{cases} -\,|j\rangle, & j = y, \\ |j\rangle, & j \neq y. \end{cases}$$

  其它辅助寄存器略去不写。已知：任何找到 $y$ 的量子算法都需要 $\Omega(\sqrt{N'})$ 次对 $O_y$ 的调用。

- **多解搜索问题（规模 $N$，有 $M$ 个解）：** 现在有 $N = N'M$ 个备选元素，某个未知子集 $S \subseteq \{1,\dots,N\}$，$|S| = M$，为“解集”。oracle $O_S$ 对 $i \in S$ 给出相位标记（或翻转一个辅助比特），目标是找到任意一个 $i \in S$。

我们要证明：若存在一个只用 $o(\sqrt{N/M})$ 次 oracle 调用的算法就能完成后者，则可以构造出一个只用 $o(\sqrt{N'})$ 次 oracle 调用的算法来解决前者，从而与 $\Omega(\sqrt{N'})$ 下界矛盾。

**(2) 用单解 oracle 构造多解 oracle。**

将集合 $\{1,\dots,N\}$ 看成一个笛卡尔积

$$\{1,\dots,N\} \cong \{1,\dots,N'\} \times \{1,\dots,M\},$$

把索引 $i$ 写成一对

$$i \leftrightarrow (j,t), \qquad j \in \{1,\dots,N'\},\ t \in \{1,\dots,M\}.$$

给定单解标记位置 $y \in \{1,\dots,N'\}$，我们在大的 $N$ 元素空间中构造一个“多解”标记集合

$$S_y := \{(y,t) : t = 1,\dots,M\},$$

也就是说：所有“第一坐标为 $y$”的 $M$ 个元素都是解，其余都不是解。

定义目标多解 oracle $O_{S_y}$ 作用在 $|j,t\rangle$ 上为

$$O_{S_y}|j,t\rangle = \begin{cases} -|j,t\rangle, & j = y, \\ |j,t\rangle, & j \neq y. \end{cases}$$

注意到，判断“$(j,t)$ 是否在 $S_y$”本质只依赖于“$j$ 是否等于 $y$”，因此我们可以用一次对单解 oracle $O_y$ 的调用来实现一次 $O_{S_y}$ 的调用：

- 把算法给出的查询输入 $i$ 解释成 $(j,t)$；
- 用 $O_y$ 作用在 $j$（连同必要的辅助寄存器）上；
- 若 $j = y$，就为整个 $|j,t\rangle$ 加上相位 $-1$，否则不变。

这样，每调用一次“多解 oracle” $O_{S_y}$，只需要调用一次原始的单解 oracle $O_y$。

**(3) 用假想的“快速多解算法”构造“快速单解算法”。**

假设存在一个量子算法 $\mathcal{A}$，在 $N$ 维空间、面对 $M$ 个解的情形下，只用

$$k = o\big(\sqrt{N/M}\big)$$

次对 $O_S$ 的调用，就能以常数成功概率（例如 $\geq 2/3$）找到一个解 $i \in S$。

现在我们要解决单解搜索问题（规模为 $N'$，有唯一标记 $y$）：

- 给定 oracle $O_y$，在更大的 Hilbert 空间 $\{|j,t\rangle\}$ 上，把它包装成一个“多解 oracle” $O_{S_y}$，如上一小节所述；
- 在该空间中运行算法 $\mathcal{A}$，把 $O_{S_y}$ 作为 oracle，调用次数仍为 $k$；
- $\mathcal{A}$ 输出某个 $(j,t)$，我们丢弃第二坐标 $t$，仅取第一坐标 $j$；
- 显然，当 $\mathcal{A}$ 成功找到一个 $(y,t)$ 时，我们就找到了原问题的唯一解 $y$。

整个过程中，每次 $\mathcal{A}$ 访问“多解 oracle” $O_{S_y}$，我们都只调用一次 $O_y$。因此，总的 $O_y$ 调用次数也是 $k$。

由于 $N = N'M$，我们有

$$k = o\big(\sqrt{N/M}\big) = o\big(\sqrt{N'}\big),$$

这意味着我们构造了一个单解搜索算法，只用 $o(\sqrt{N'})$ 次 oracle 调用就能找到解，这与已经证明的 $\Omega(\sqrt{N'})$ 下界矛盾。

**(4) 得出多解情形的下界。**

矛盾说明我们的假设不成立，也就是说：任何能在多解情形下找到一个解的量子算法，其 oracle 调用次数 $k$ 必须满足

$$k = \Omega\big(\sqrt{N'}\big) = \Omega\big(\sqrt{N/M}\big).$$

结合 Grover 算法在有 $M$ 个解时可以在 $O\big(\sqrt{N/M}\big)$ 次调用内找到解，便知这是紧的下界：多重解搜索问题的最优查询复杂度为

$$\Theta\big(\sqrt{N/M}\big).$$

□