6.3 量子计数——习题与解答

DanX, and Shan Jin *

练习 6.13 (经典计数算法的标准差与复杂度)**.** 考虑计数问题的一个经典算法。该算法在包含 N 个元素的搜索空间中均匀、独立地进行 k 次采样。

记 *oracle* 第 j 次调用的结果为

$$X_j = \begin{cases} 1, & \text{若第 } j \text{ 次采样是一个解;} \\ 0, & \text{若第 } j \text{ 次采样不是解,} \end{cases} \qquad j = 1, \ldots, k.$$

设搜索空间中一共有 M 个解。算法给出的解的数目的估计量定义为

$$S \equiv \frac{N}{k} \sum_{j=1}^{k} X_j.$$

(1) 证明估计量 S 的标准差为

$$\Delta S = \sqrt{\frac{M(N-M)}{k}}.$$

(2) 进一步证明：若要对所有 M 估计 M，并且以至少 3/4 的概率达到精度 $\sqrt{M}$，则必须有

$$k = \Omega(N),$$

也就是说，采样次数的量级至少与 N 成正比。

解答. (1) 计算 S 的标准差

首先注意：每次采样都是独立同分布的，且第 j 次采样为解的概率

$$p := \Pr(X_j = 1) = \frac{M}{N}, \qquad \Pr(X_j = 0) = 1 - p = \frac{N-M}{N}.$$

因此所有 X_j 都是参数为 p 的独立伯努利随机变量。

记

$$Y := \sum_{j=1}^{k} X_j,$$

即 k 次采样中一共命中了解多少次。那么 Y 服从二项分布

$$Y \sim \text{Binomial}(k, p).$$

先求 Y 的期望与方差。

由二项分布的标准结论：

$$\mathbb{E}[Y] = kp, \qquad \text{Var}(Y) = kp(1-p).$$

*jinshan@tgqs.net

也可以用线性性和独立性直接算一遍：

$$\mathbb{E}[Y] = \sum_{j=1}^{k} \mathbb{E}[X_j] = k\,\mathbb{E}[X_1] = k\,(0 \cdot \Pr(X_1 = 0) + 1 \cdot \Pr(X_1 = 1)) = kp,$$

$$\mathrm{Var}(Y) = \sum_{j=1}^{k} \mathrm{Var}(X_j) = k\,\mathrm{Var}(X_1),$$

而

$$\mathrm{Var}(X_1) = \mathbb{E}[X_1^2] - \mathbb{E}[X_1]^2 = p - p^2 = p(1-p),$$

所以

$$\mathrm{Var}(Y) = kp(1-p).$$

再把 Y 换成 S。

估计量

$$S = \frac{N}{k} Y.$$

利用“线性变换下的方差”：

$$\mathbb{E}[S] = \frac{N}{k}\,\mathbb{E}[Y] = \frac{N}{k} \cdot kp = Np = M,$$

$$\mathrm{Var}(S) = \left(\frac{N}{k}\right)^2 \mathrm{Var}(Y) = \left(\frac{N}{k}\right)^2 kp(1-p).$$

代入 $p = M/N$：

$$\begin{aligned}
\mathrm{Var}(S) &= \frac{N^2}{k^2} \cdot k \cdot \frac{M}{N}\left(1 - \frac{M}{N}\right) \\
&= \frac{N^2}{k^2} \cdot k \cdot \frac{M}{N} \cdot \frac{N-M}{N} \\
&= \frac{M(N-M)}{k}.
\end{aligned}$$

于是标准差

$$\Delta S = \sqrt{\mathrm{Var}(S)} = \sqrt{\frac{M(N-M)}{k}},$$

这就是要证明的第一个结论。

(2) 证明 $k = \Omega(N)$

题意是：希望用这个估计量 S 来估计真实的解的数目 M，并且对于所有可能的 M，都满足

$$\Pr\big(|S - M| \le \sqrt{M}\big) \;\ge\; \frac{3}{4}.$$

我们用切比雪夫不等式（Chebyshev inequality）来建立“精度”与方差之间的关系。切比雪夫不等式说：对任意随机变量 X，

$$\Pr\big(|X - \mathbb{E}[X]| \ge t\big) \;\le\; \frac{\mathrm{Var}(X)}{t^2}.$$

在本题中，$X = S$，$\mathbb{E}[S] = M$，$t = \sqrt{M}$。因此

$$\Pr\big(|S - M| \ge \sqrt{M}\big) \;\le\; \frac{\mathrm{Var}(S)}{M} = \frac{M(N-M)/k}{M} = \frac{N-M}{k}.$$

希望估计足够好，即

$$\Pr\big(|S-M|\ge\sqrt{M}\big)\ \le\ \frac{1}{4},$$

从而

$$\frac{N-M}{k}\le\frac{1}{4}\quad\Longrightarrow\quad k\ge 4(N-M).$$

题目要求“对所有 M”都要成立，因此在最坏情况下（对我们要求 k 最大的那种 M）：

$$k\ge 4(N-M_{\min}).$$

只要存在某些 M 使得 $N-M$ 是 $\Theta(N)$，就会得到 $k=\Omega(N)$。例如，当 M 远小于 N（比如 $M=1$，只有一个解）时，

$$k\ge 4(N-1)=\Omega(N).$$

更简单地说：题目要求算法对所有 M 都有效，包括“解很少”的极端情况，这时采样到解的概率 $p=M/N$ 非常小；要在误差 $\sqrt{M}$ 的尺度内准确估计 M，就必须进行次数量级为 N 的采样。因此

$$k=\Omega(N).$$

这说明纯经典的随机采样计数算法在最坏情况下需要线性于 N 的 oracle 调用次数，无法达到像量子计数那样的平方加速。 □

练习 6.14 (带常数因子的精度界)**.** 在上一题中，我们考虑的是精度为 $\sqrt{M}$ 的情况。现在推广一点：设 $c>0$ 为一个常数。

证明：对任何至少以概率在 $c\sqrt{M}$ 精度内，对所有的 M 估计 M 的算法（仍采用上题的经典随机采样方式），都必须满足

$$k=\Omega(N).$$

也就是说，即便只要求达到“误差 $\le c\sqrt{M}$”这样的较宽松精度，采样次数的量级仍然至少是 N 的常数倍。

解答. 和上一题一样，估计量仍为

$$S=\frac{N}{k}\sum_{j=1}^{k}X_j,\quad \mathbb{E}[S]=M,\quad \mathrm{Var}(S)=\frac{M(N-M)}{k}.$$

题设的要求是：对于所有 M，都希望

$$\Pr\big(|S-M|\le c\sqrt{M}\big)\ \ge\ \frac{3}{4}.$$

(1) 用切比雪夫不等式给出必要条件

同样使用切比雪夫不等式，对任意 M：

$$\Pr\big(|S-M|\ge c\sqrt{M}\big)\ \le\ \frac{\mathrm{Var}(S)}{c^2M}=\frac{M(N-M)/k}{c^2M}=\frac{N-M}{c^2k}.$$

为了使得

$$\Pr\big(|S-M|\le c\sqrt{M}\big)\ge\frac{3}{4},$$

必然要有

$$\Pr\big(|S-M|\ge c\sqrt{M}\big)\le\frac{1}{4},$$

从而

$$\frac{N-M}{c^2k} \le \frac{1}{4} \quad \Longrightarrow \quad k \ge \frac{4(N-M)}{c^2}.$$

(2) 对“所有 M”的含义

上式对每一个 M 都必须成立。题目要求算法对所有 M 都给出如此精度的估计，所以我们要看在这些不等式中，对 k 的约束最强的是哪一个 M。

当 M 较小（比如 $M = O(1)$，只有常数个解）时，

$$N - M \approx N,$$

于是

$$k \gtrsim \frac{4N}{c^2}.$$

这表明：为了保证在“解非常稀少”的情况下仍然可以以误差 $c\sqrt{M}$ 估计 M，采样次数 k 必须与 N 同阶，满足

$$k = \Omega(N).$$

(3) 直观理解

- 当 M 很小（例如 $M = 1$）时，单次采样命中解的概率 $p = M/N$ 非常低；- 要在误差 $\sim c\sqrt{M}$（也就是常数量级）的精度下可靠地估计 M，就必须累积足够多的命中次数；- 这意味着总采样次数 k 至少要与 $1/p \sim N$ 同数量级。

因此，无论常数 c 取多少，只要要求“对所有 M 均有效且成功概率至少 $3/4$”，就必须有

$$k = \Omega(N).$$

这与量子计数可以在 $O(\sqrt{N})$ 次 oracle 调用内完成高精度估计形成鲜明对比，也从另一个角度说明了量子计数算法的加速本质。 □