5.2 相位估计——习题与详细解答

DanX, Joe Chen*, and Li Fan

练习 5.7. 通过证明图 *5.2* 那样的受控 U 运算会将状态 $|j\rangle|u\rangle$ 变为 $|j\rangle U^j|u\rangle$，从而对图 *5.2* 线路可以有更为深刻的认识。这里 $|j\rangle$ 是第一寄存器的计算基态，可写成

$$|j\rangle = |j_1 j_2 \cdots j_t\rangle, \qquad j_k \in \{0,1\},$$

并且第 k 个比特控制的量子门是 ctrl$-U^{2^{t-k}}$。证明上述结论，并说明这个结论并不依赖 $|u\rangle$ 是 U 的本征态。

解答. **1. 把线路结构说清楚**。

相位估计算法中，假设第一寄存器有 t 个比特，写成 $|j_1 j_2 \cdots j_t\rangle$，第二寄存器上放置某个态 $|u\rangle$。

线路里依次有

$$\text{ctrl}-U^{2^{t-1}},\ \text{ctrl}-U^{2^{t-2}},\ \ldots,\ \text{ctrl}-U^{2^0},$$

第 k 个比特（从左到右）控制 ctrl$-U^{2^{t-k}}$。

也就是说：

- 如果第 k 个比特 $j_k = 0$，对应的受控门「不开」，等价于作用恒等算符 I；- 如果第 k 个比特 $j_k = 1$，对应的受控门「打开」，就在第二寄存器上作用 $U^{2^{t-k}}$。

2. 从一个控制比特看起。

先只看第一个控制比特 j_1。对于总态 $|j_1\rangle|\text{其余比特}\rangle|u\rangle$，

- 若 $j_1 = 0$：该门不起作用，第二寄存器上相当于作用 $U^0 = I$；- 若 $j_1 = 1$：该门起作用，在第二寄存器上作用 $U^{2^{t-1}}$。

这两种情况可以统一写成：

$$|j_1\rangle|\cdots\rangle|u\rangle \longrightarrow |j_1\rangle|\cdots\rangle\, U^{j_1 2^{t-1}}|u\rangle.$$

完全类似地：

- 第 2 个比特控制 ctrl$-U^{2^{t-2}}$，作用结果是再乘上 $U^{j_2 2^{t-2}}$；- ... - 第 t 个比特控制 ctrl$-U^{2^0}$，作用结果是再乘上 $U^{j_t 2^0}$。

3. 把所有受控门的作用乘在一起。

所有门依次作用在第二寄存器上，相当于在 $|u\rangle$ 上依次作用

$$U^{j_1 2^{t-1}},\ U^{j_2 2^{t-2}},\ \ldots,\ U^{j_t 2^0}.$$

因为 U 是酉算符，满足

$$U^a U^b = U^{a+b} \quad \text{(指数相加)}.$$

所以总作用是

$$U^{j_1 2^{t-1}} U^{j_2 2^{t-2}} \cdots U^{j_t 2^0} = U^{j_1 2^{t-1} + j_2 2^{t-2} + \cdots + j_t 2^0}.$$

*qhc.statistics@gmail.com

而

$$j := j_1 2^{t-1} + j_2 2^{t-2} + \cdots + j_t 2^0$$

正是二进制数 $j_1 j_2 \cdots j_t$ 对应的十进制数值。因此

$$U^{j_1 2^{t-1}} \cdots U^{j_t 2^0} = U^j.$$

于是总的变换就是

$$|j_1 \cdots j_t\rangle |u\rangle \longrightarrow |j_1 \cdots j_t\rangle \, U^j |u\rangle ,$$

也就是

$$|j\rangle |u\rangle \longrightarrow |j\rangle \, U^j |u\rangle .$$

注意整个推导过程中，我们只用到了「受控门要么作用 U^{2^k}，要么作用恒等」和「$U^a U^b = U^{a+b}$」这两个事实，完全没有用到 $|u\rangle$ 是否是本征态。所以结论对任意态 $|u\rangle$ 都成立。 □

练习 5.8. 设相位估计算法把状态 $|0\rangle |u\rangle$ 变为 $|\tilde{\varphi}_u\rangle |u\rangle$，其中 $|\tilde{\varphi}_u\rangle$ 是第一寄存器中对本征相位 φ_u 的近似编码。如果给定输入

$$|0\rangle \left(\sum_u c_u |u\rangle \right),$$

则算法输出

$$\sum_u c_u |\tilde{\varphi}_u\rangle |u\rangle .$$

证明：当辅助比特数 t 按照教材式 *(5.35)* 选择时，在相位估计算法后精确到 n 比特测量 φ_u 的概率，至少是 $|c_u|^2(1-\varepsilon)$。

解答. 这题的直觉是：

「对每一个本征态 $|u\rangle$，算法都有至少 $1-\varepsilon$ 的概率给出正确的 n 比特近似；如果起始态里 $|u\rangle$ 的权重是 $|c_u|^2$，那么同时要求“既选中了本征态 $|u\rangle$，又测得相位正确”的概率，自然是两者相乘：$|c_u|^2(1-\varepsilon)$。」

正式证明要把「线性性」和「测量概率如何计算」说清楚。

1. 对单一本征态的相位估计结果。

设 $U |u\rangle = e^{2\pi i \varphi_u} |u\rangle$，相位估计算法作用在 $|0\rangle^{\otimes t} |u\rangle$ 上，得到

$$|0\rangle^{\otimes t} |u\rangle \longrightarrow |\Phi_u\rangle = \sum_{k=0}^{2^t-1} \alpha_{u,k} \, |k\rangle |u\rangle ,$$

其中 $|k\rangle$ 是第一寄存器的计算基态。$|\Phi_u\rangle$ 已规范化：$\sum_k |\alpha_{u,k}|^2 = 1$。

教材中已经证明：若 t 选得足够大（按式 (5.35)），则对于每个本征态 $|u\rangle$，有

$$\sum_{k \text{ 是 } \varphi_u \text{ 的好近似}} |\alpha_{u,k}|^2 \geq 1 - \varepsilon.$$

也就是说，给定 $|u\rangle$ 为输入，测量第一寄存器得到「正确的 n 比特近似」的概率至少是 $1-\varepsilon$。

2. 对线性叠加态的相位估计：线性性。

现在输入量子态是叠加态

$$|\Psi_{\text{in}}\rangle = |0\rangle^{\otimes t} \left(\sum_u c_u |u\rangle \right) = \sum_u c_u |0\rangle^{\otimes t} |u\rangle .$$

相位估计算法整体是一个酉算符 W（包括第一阶段的受控 U^j 和第二阶段的逆 QFT），所以它对叠加态的作用是线性的：

$$W\left|\Psi_{\text{in}}\right\rangle = \sum_u c_u W\left(\left|0\right\rangle^{\otimes t}\left|u\right\rangle\right) = \sum_u c_u \left|\Phi_u\right\rangle = \sum_u c_u \sum_k \alpha_{u,k}\left|k\right\rangle\left|u\right\rangle.$$

因此，在测量之前总态是

$$\left|\Psi_{\text{out}}\right\rangle = \sum_{u,k} c_u \alpha_{u,k}\left|k\right\rangle\left|u\right\rangle.$$

3. 测量两寄存器：概率怎么算？

现在对两个寄存器都在计算基下做测量。所有可能的结果是成对的 (k,u)，测得结果 (k,u) 的概率是

$$p(k,u) = \left|c_u \alpha_{u,k}\right|^2.$$

因为展开后的态在 $\{\left|k\right\rangle\left|u\right\rangle\}$ 这组正交基下的系数就是 $c_u\alpha_{u,k}$。

我们关心的是：

「测得的本征态是某个特定的 $|\rangle$，同时第一寄存器上的结果给出了 φ 的正确 n 比特近似」这一事件的概率是多少?

令 $\mathcal{G}$ 表示所有「对 φ 来说是好近似」的比特串集合。那么所求概率就是

$$\begin{aligned} P(\text{测得好近似并选中}\,|\rangle) &= \sum_{k\in\mathcal{G}} p(k,) \\ &= \sum_{k\in\mathcal{G}} \left|c\alpha_{,k}\right|^2 \\ &= \left|c\right|^2 \sum_{k\in\mathcal{G}} \left|\alpha_{,k}\right|^2. \end{aligned}$$

而对单一本征态 $|\rangle$ 的相位估计已有结论

$$\sum_{k\in\mathcal{G}} \left|\alpha_{,k}\right|^2 \geq 1-\varepsilon.$$

所以

$$P(\text{测得好近似并选中}\,|\rangle) \geq \left|c\right|^2(1-\varepsilon).$$

这正是题目要求证明的结论：对特定本征态 $\left|u\right\rangle$（这里记作 $|\rangle$），相位估计算法在叠加态输入下，测得它对应的本征相位且精度达到 n 比特的概率，至少是 $\left|c_u\right|^2(1-\varepsilon)$。

4. 直观总结。

- $\left|c_u\right|^2$：一开始「抽中本征态 $\left|u\right\rangle$」的权重；- $1-\varepsilon$：在 $\left|u\right\rangle$ 已被抽中的前提下，算法成功给出正确近似的概率；- 所以两者相乘就是「既抽中 $\left|u\right\rangle$ 又估计成功」的总概率。

线性性保证了不同本征态之间不会互相「串门」，测量时每个 (k,u) 的概率就是单独那一项的模平方。 □

练习 5.9. *令 U 是一个特征值为 ±1 的酉变换，作用在单比特（或多比特）状态 $\left|\psi\right\rangle$ 上。利用相位估计算法，构造一个量子线路，使得 $\left|\psi\right\rangle$ 坍缩到 U 的两个本征态之一，并给出最终状态在哪个本征空间的经典指示器。并与练习 4.34 的结果进行比较。*

解答. **1. 观察：特征值 ±1 对应的本征相位。**

如果 $U\left|u_\pm\right\rangle = \pm\left|u_\pm\right\rangle$，可以写成

$$\pm1 = e^{2\pi i\varphi_\pm}$$

的形式。两个相位分别是

$$\varphi_+ = 0, \qquad \varphi_- = \tfrac{1}{2}.$$

也就是说，相位只有两种可能：0 或 1/2，只需要 一位二进制就能区分：

$$0 = (0)_2, \qquad \tfrac{1}{2} = (0.1)_2.$$

这暗示：用相位估计时，第一寄存器只要 1 个辅助比特就够了。

2. 用一位相位估计的线路。

一位相位估计的标准流程：

1. 辅助比特初态为 $|0\rangle$，对它作用 Hadamard，得到 $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$；2. 以辅助比特为控制，对系统比特作用 ctrl$-U$；3. 再对辅助比特作用 Hadamard；4. 最后测量辅助比特。

整个线路就是：

$$|0\rangle|\psi\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|\psi\rangle \xrightarrow{\text{ctrl}-U} \frac{1}{\sqrt{2}}\big(|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle\big) \xrightarrow{H\otimes I} \cdots$$

这和练习 4.34 中的线路一模一样，只是那时把 U 看成一个可观测量，这里把它看成特征值为 ± 1 的酉算符。

3. 把 $|\psi\rangle$ 展开在本征态基下。

把初始态 $|\psi\rangle$ 在 U 的本征基 $\{|u_+\rangle, |u_-\rangle\}$ 下展开：

$$|\psi\rangle = \alpha|u_+\rangle + \beta|u_-\rangle, \qquad |\alpha|^2 + |\beta|^2 = 1.$$

初始总态：

$$|\Psi_0\rangle = |0\rangle|\psi\rangle.$$

第一步 Hadamard：

$$|\Psi_1\rangle = (H\otimes I)|\Psi_0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)(\alpha|u_+\rangle + \beta|u_-\rangle).$$

受控-U：

$$\begin{aligned}
|\Psi_2\rangle &= \frac{1}{\sqrt{2}}\Big(|0\rangle(\alpha|u_+\rangle + \beta|u_-\rangle) + |1\rangle U(\alpha|u_+\rangle + \beta|u_-\rangle)\Big) \\
&= \frac{1}{\sqrt{2}}\Big(|0\rangle(\alpha|u_+\rangle + \beta|u_-\rangle) + |1\rangle(\alpha\cdot(+1)|u_+\rangle + \beta\cdot(-1)|u_-\rangle)\Big) \\
&= \frac{1}{\sqrt{2}}\Big(|0\rangle(\alpha|u_+\rangle + \beta|u_-\rangle) + |1\rangle(\alpha|u_+\rangle - \beta|u_-\rangle)\Big).
\end{aligned}$$

再对辅助比特做 Hadamard：

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

于是

$$\begin{aligned}
|\Psi_3\rangle &= (H\otimes I)|\Psi_2\rangle \\
&= \frac{1}{2}\Big[(|0\rangle + |1\rangle)(\alpha|u_+\rangle + \beta|u_-\rangle) + (|0\rangle - |1\rangle)(\alpha|u_+\rangle - \beta|u_-\rangle)\Big] \\
&= \frac{1}{2}\Big[|0\rangle\big[(\alpha|u_+\rangle + \beta|u_-\rangle) + (\alpha|u_+\rangle - \beta|u_-\rangle)\big] \\
&\qquad + |1\rangle\big[(\alpha|u_+\rangle + \beta|u_-\rangle) - (\alpha|u_+\rangle - \beta|u_-\rangle)\big]\Big] \\
&= \frac{1}{2}\Big[|0\rangle\big(2\alpha|u_+\rangle\big) + |1\rangle\big(2\beta|u_-\rangle\big)\Big] \\
&= \alpha|0\rangle|u_+\rangle + \beta|1\rangle|u_-\rangle.
\end{aligned}$$

这一步非常关键：辅助比特与本征态完美纠缠了。

4. 测量辅助比特：得到本征空间的经典指示。

现在测量辅助比特在 $\{|0\rangle, |1\rangle\}$ 基下：

- 若结果为 0，概率为 $|\alpha|^2$，第二寄存器坍缩为 $|u_+\rangle$（归一化后）；- 若结果为 1，概率为 $|\beta|^2$，第二寄存器坍缩为 $|u_-\rangle$（归一化后）。

因此，这条线路实现了：

1. 把 $|\psi\rangle$ 投影到 U 的两个本征空间之一；2. 用一个经典比特（测量结果 0/1）告诉你「是在 $\lambda = +1$ 本征空间，还是 $\lambda = -1$ 本征空间」。

这正是题目要求的「给出经典指示器」的含义。

5. 与练习 4.34 的比较。

在练习 4.34 中，我们把 U 看成一个可观测量，本征值为 ± 1，构造的线路就是

$$|0\rangle\,|\psi\rangle \xrightarrow{H} \xrightarrow{\text{ctrl-}U} \xrightarrow{H} \text{测量辅助比特.}$$

可以看到：

- 这条线路正是一位相位估计算法；- 对应的本征相位是 0 与 1/2，一位二进制正好能区分；- 所以「测量可观测量 U」和「对 U 做一位相位估计」在这里完全是同一件事。

换句话说：练习 4.34 给出的就是相位估计算法在「特征值只为 ± 1」这一特例下的实现。 □