5.1 量子 Fourier 变换——习题与解答

DanX, Joe Chen*, and Li Fan

练习 5.1. 给出式 *(5.2)* 定义的线性变换是酉变换的一个直接证明：

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle . \tag{5.2}$$

解答. 把该线性变换记为矩阵 F。从式 (5.2) 可知，它在计算基 $\{|0\rangle, \ldots, |N-1\rangle\}$ 下的矩阵元为

$$F_{jk} = \frac{1}{\sqrt{N}} e^{2\pi ijk/N}, \qquad j,k = 0, \ldots, N-1.$$

要证明 F 酉，只需证明

$$F^\dagger F = I.$$

考虑 $F^\dagger F$ 的矩阵元：

$$\begin{aligned}(F^\dagger F)_{j\ell} &= \sum_{k=0}^{N-1} (F^\dagger)_{jk} F_{k\ell} = \sum_{k=0}^{N-1} F_{kj}^* F_{k\ell} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi ikj/N} \, e^{2\pi ik\ell/N} = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i(\ell-j)k/N}.\end{aligned}$$

令

$$\omega = e^{2\pi i(\ell-j)/N}.$$

于是

$$(F^\dagger F)_{j\ell} = \frac{1}{N} \sum_{k=0}^{N-1} \omega^k.$$

分两种情况讨论：

1. 若 $\ell = j$，则 $\omega = e^0 = 1$，故

$$(F^\dagger F)_{jj} = \frac{1}{N} \sum_{k=0}^{N-1} 1 = 1.$$

2. 若 $\ell \neq j$，由于 $0 \leq j, \ell \leq N-1$，故 $0 < |\ell - j| < N$，于是

$$\omega = e^{2\pi i(\ell-j)/N} \neq 1.$$

此时 $\{\omega^k\}$ 构成一个比值为 ω，长度为 N 的等比数列，可以使用求和公式：

$$\sum_{k=0}^{N-1} \omega^k = \frac{1-\omega^N}{1-\omega}.$$

*qhc.statistics@gmail.com

又因为 $\ell - j$ 是整数，所以

$$\omega^N = e^{2\pi i(\ell-j)} = 1,$$

从而

$$\sum_{k=0}^{N-1} \omega^k = 0, \qquad (F^\dagger F)_{j\ell} = 0.$$

综上，

$$(F^\dagger F)_{j\ell} = \delta_{j\ell},$$

于是 $F^\dagger F = I$，F 为酉矩阵，式 (5.2) 给出的正是一个酉变换。 □

练习 5.2. 具体计算 n 量子比特状态 $|00\cdots0\rangle$ 的 *Fourier* 变换。

解答. 对 n 个量子比特, Hilbert 空间维数为 $N = 2^n$。计算基态 $|00\cdots0\rangle$ 对应的整数标号是 $j = 0$。把 $j = 0$ 代入式 (5.2)：

$$|00\cdots0\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i\cdot 0\cdot k/N} |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle .$$

因为 $N = 2^n$，可以写成

$$|00\cdots0\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle .$$

也就是说，n 比特全零态经过量子 Fourier 变换后，变成所有 2^n 个计算基态的等幅叠加态。

为了更直观，举一个两比特的例子。设 $n = 2$、$j = 1$，对应量子态为 $|01\rangle$。则

$$|01\rangle \longrightarrow \frac{1}{\sqrt{4}} \sum_{k=0}^{3} e^{2\pi i\cdot 1\cdot k/4} |k\rangle = \frac{1}{2}\Big(|00\rangle + e^{\frac{1}{4}2\pi i} |01\rangle + e^{\frac{2}{4}2\pi i} |10\rangle + e^{\frac{3}{4}2\pi i} |11\rangle\Big),$$

这与一般情形是一致的。 □

练习 5.3（（经典快速 Fourier 变换））**.** 在一个经典计算机上对 2^n 维复向量做离散 *Fourier* 变换。验证：

1. 直接使用式

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}, \tag{5.1}$$

所需的基本算术运算数为 $\Theta(2^{2n})$；

2. 若利用书中式 *(5.4)*（即把变换分解成类似量子 *Fourier* 变换电路那样的结构），算术运算数量可以降低为 $\Theta(n2^n)$。

解答. **(1) 直接使用式 (5.1) 的复杂度**。

设 $N = 2^n$。要计算所有输出 y_k，$k = 0, \ldots, N-1$。

- 对于某个固定的 k，式中求和 $\sum_{j=0}^{N-1}$ 含有 N 项。若假设一次复数乘法 $x_j e^{2\pi ijk/N}$ 和一次复数加法都算作 $O(1)$ 运算，则计算单个 y_k 需要 $O(N)$ 步。
- 一共要计算 N 个不同的 y_k。

因此总运算数为

$$N \times O(N) = O(N^2) = O(2^{2n}).$$

另一方面，显然不可能少于常数倍的 N^2 次操作，故复杂度为 $\Theta(2^{2n})$。

若更加细致地把整数乘法 jk 的代价算成 $O(n)$，则可以得到 $O(n2^{2n})$ 的复杂度，但不影响其指数级的本质。

(2) 利用式 (5.4) 的“快速”算法。

书中的式 (5.4) 给出了 n 比特基态 $|j_1 j_2 \cdots j_n\rangle$ 在 Fourier 变换后的分解形式：

$$|j_1 \cdots j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \prod_{m=1}^{n} \Big(|0\rangle + e^{2\pi i\, 0.j_m j_{m+1} \cdots j_n} |1\rangle \Big), \tag{5.4}$$

其中 $0.j_m j_{m+1} \cdots j_n$ 表示二进制小数。

把这看成是一个经典计算公式：

- 对于每个比特位置 m，需要构造因子

  $$|0\rangle + e^{2\pi i\, 0.j_m j_{m+1} \cdots j_n} |1\rangle .$$

  这里相位指数中含有最多 n 位二进制数，因此计算该相位只需 $O(n)$ 次基本运算，甚至更少；与下面的总复杂度相比可以忽略。

- 整个变换结果可以看成 2^n 个基态的线性组合。每个系数由上述这些因子相乘得到。对于每个输出分量，最多涉及 n 次相位因子的乘法，因此生成一个输出分量需要 $\Theta(n)$ 次运算。

- 一共有 $2^n = N$ 个输出分量。

  于是总运算数为

  $$2^n \times \Theta(n) = \Theta(n2^n).$$

  这与快速 Fourier 变换（FFT）通常的复杂度 $O(N \log N)$（此处 $N = 2^n$，$\log N = n$）相一致。

□

练习 5.4. 给出受控 R_k 门到单量子比特门和受控非门（$CNOT$）的一个分解。

解答. 单比特相位旋转门 R_k 定义为

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}.$$

(1) 先把 R_k 写成 $e^{-i\alpha} AXBXC$ 的形式。

注意到

$$R_k = e^{\pi i/2^k} \begin{bmatrix} e^{-\pi i/2^k} & 0 \\ 0 & e^{\pi i/2^k} \end{bmatrix} = e^{\pi i/2^k} R_z\Big(\frac{\pi}{2^{k-1}}\Big),$$

其中

$$R_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

利用 $R_z(\theta_1) R_z(\theta_2) = R_z(\theta_1 + \theta_2)$，可得

$$R_z\Big(\frac{\pi}{2^{k-1}}\Big) = R_z\Big(\frac{\pi}{2^k}\Big) R_z\Big(\frac{\pi}{2^k}\Big).$$

另一方面，有恒等式

$$XR_z(\theta)X = R_z(-\theta),$$

因此

$$R_z\left(\frac{\pi}{2^k}\right) = XR_z\left(-\frac{\pi}{2^k}\right)X.$$

把它代回上式：

$$\begin{aligned} R_k &= e^{\pi i/2^k} R_z\left(\frac{\pi}{2^k}\right) R_z\left(\frac{\pi}{2^k}\right) \\ &= e^{\pi i/2^k} XR_z\left(-\frac{\pi}{2^k}\right) XR_z\left(\frac{\pi}{2^k}\right). \end{aligned}$$

因此可以取

$$\alpha = -\frac{\pi}{2^k}, \qquad A = I, \qquad B = R_z\left(-\frac{\pi}{2^k}\right), \qquad C = R_z\left(\frac{\pi}{2^k}\right),$$

则

$$R_k = e^{-i\alpha} AXBXC,$$

并且

$$ABC = R_z\left(-\frac{\pi}{2^k}\right) R_z\left(\frac{\pi}{2^k}\right) = I.$$

(2) 利用一般结论构造受控 R_k。

在第 4 章已经证明过：若单比特酉算符 U 可以写成

$$U = e^{-i\alpha} AXBXC, \qquad ABC = I,$$

则受控-U 门可以只用两次 CNOT 和三个单比特门 A, B, C （全部作用在目标比特上）来实现。其结构是：

- 先对目标比特作用 C；
- 施加一次 CNOT（控制比特为控制，目标比特为目标）；
- 对目标比特作用 B；
- 再施加一次 CNOT；
- 最后对目标比特作用 A。

可以直接检验：当控制比特为 $|0\rangle$ 时，两次 CNOT 都不起作用，目标比特经历的总算符是 $CBA = I$；当控制比特为 $|1\rangle$ 时，目标比特经历的总算符为 $AXBXC = e^{i\alpha}U$，只差一个整体相位，对物理无影响。

把这里求出的 (α, A, B, C) 换进去，就得到受控 R_k 门的一个分解，只用单比特 R_z 门和两次 CNOT 即可实现。 □

练习 5.5. 给出进行逆量子 *Fourier* 变换的一个量子线路。

解答. 在经典离散 Fourier 变换中，有

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}, \qquad x_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k e^{-2\pi ijk/N},$$

后一式正是前一式的逆变换。

量子情形类似。量子 Fourier 变换 F 是一个酉算符，其矩阵元与上式中的 $e^{2\pi ijk/N}$ 相对应；因此逆变换就是 $F^\dagger$，把所有相位取复共轭（即指数符号取负号）。

如何从 QFT 电路得到逆 QFT 电路？

设图 5.1 中给出的电路实现的是 F，它由若干 Hadamard 门 H、受控 R_k 门和若干 swap 门组成。由于

$$H^\dagger = H, \qquad R_k^\dagger = R_k^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^k} \end{bmatrix}, \qquad \mathrm{swap}^\dagger = \mathrm{swap},$$

所以 $F^\dagger$ 的电路可以按下述步骤得到：

1. 将原 QFT 电路中所有门的顺序倒过来；
2. 把每个门都替换为它的共轭转置：
   - Hadamard 还是用 H；
   - 每个 R_k 换成 $R_k^\dagger$（相位取负）；
   - swap 门保持不变。

这样得到的新电路就实现了逆量子 Fourier 变换。如果原电路在末尾用了 swap 门来交换量子比特顺序，逆电路只要在电路最前面做相同的 swap 即可。 □

练习 5.6（（量子 Fourier 变换的近似））**.** 设 U 是 n 量子比特上的理想 *Fourier* 变换，V 是将所有受控 R_k 门用精度

$$\Delta = \frac{1}{p(n)}$$

的近似门（$p(n)$ 为某个多项式）替换后得到的量子线路。证明误差

$$E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\| = \Theta\left(\frac{n^2}{p(n)}\right).$$

说明：每个门只需多项式精度，就能保证整个 *Fourier* 变换的误差也是多项式级别的。

解答. (1) 误差可以分解为各门的误差之和。

盒子 4.1 中曾给出一个结论（式 (4.69)）：设

$$U = U_m U_{m-1} \cdots U_1, \qquad V = V_m V_{m-1} \cdots V_1,$$

且各 U_j, V_j 都是酉算符。若对每个 j 有

$$\|U_j - V_j\| \le \epsilon_j,$$

其中范数取算符范数（谱范数），则总体误差满足

$$\|U - V\| \le \sum_{j=1}^{m} \epsilon_j.$$

这一不等式实质上来自三角不等式以及酉算符保持范数不变的性质。

在本题中，我们假设 Hadamard 门和 swap 门都精确实现，只有受控 R_k 门近似实现。于是所有 ϵ_j 中只有对应受控 R_k 的那一部分非零，都等于 $\Delta = 1/p(n)$。

(2) 数一数有多少个受控 R_k 门。

n 比特 QFT 的标准电路中，第 1 个比特与后面的 $n-1$ 个比特之间有 $n-1$ 个受控相位门；第 2 个比特与后面的 $n-2$ 个比特之间有 $n-2$ 个；以此类推。因此受控 R_k 总数为

$$m = (n-1) + (n-2) + \cdots + 1 = \frac{n(n-1)}{2}.$$

(3) 估计总体误差。

每个受控 R_k 门的误差不超过 Δ，于是由上面的不等式有

$$E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\| \le m\Delta = \frac{n(n-1)}{2}\,\Delta = \Theta\left(\frac{n^2}{p(n)}\right).$$

另一方面，可以理解为：如果每个门的近似都“向着同一方向”偏离，则总误差大致会叠加到这个数量级；因此 $E(U,V)$ 的增长阶也不会比 $n^2\Delta$ 更小。在渐近意义下，我们可以写成

$$E(U,V) = \Theta\left(\frac{n^2}{p(n)}\right).$$

这说明：只要每个基本门的精度是多项式级别 $1/p(n)$，整个 n 比特量子 Fourier 变换的总误差仍然是多项式量级，无需对每个门追求指数级的超高精度。 □