5.4 量子 Fourier 变换的一般应用——习题与解答

DanX, Joe Chen*, and Li Fan

练习 5.20（（周期函数的离散 Fourier 变换））. 设 $f\colon \mathbb{Z}\to\mathbb{C}$ 满足周期性

$$f(x+r)=f(x)\quad (0\le x<N),$$

其中 N 是 r 的一个正整数倍。定义 N 点离散 *Fourier* 变换

$$\hat{f}(l)=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-2\pi ilx/N}f(x),\qquad l=0,1,\ldots,N-1.$$

利用周期性和

$$\sum_{k\in\{0,r,2r,\ldots,N-r\}}e^{2\pi ikl/N}=\begin{cases}N/r, & l\ \text{为}N/r\ \text{的整倍数},\\ 0, & \text{否则},\end{cases}$$

计算 $\hat{f}(l)$，并把结果与书中 r 点变换

$$\hat{g}(\lambda)=\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{-2\pi i\lambda x/r}g(x)$$

联系起来，其中 $g(x)=f(x)$ $(0\le x<r)$。

解答. **1. 把求和按一个周期拆分**。

因为 N 是 r 的倍数，可写 $N=(N/r)\,r$。对每个

$$x=jr+d,\qquad j=0,\ldots,N/r-1,\ \ d=0,\ldots,r-1,$$

有 $f(x)=f(jr+d)=f(d)$。于是

$$\begin{aligned}\hat{f}(l)&=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-2\pi ilx/N}f(x)\\&=\frac{1}{\sqrt{N}}\sum_{j=0}^{N/r-1}\sum_{d=0}^{r-1}e^{-2\pi il(jr+d)/N}f(d)\\&=\frac{1}{\sqrt{N}}\sum_{d=0}^{r-1}\Big(\sum_{j=0}^{N/r-1}e^{-2\pi iljr/N}\Big)e^{-2\pi ild/N}f(d).\end{aligned}$$

记

$$S(l):=\sum_{j=0}^{N/r-1}e^{-2\pi iljr/N}.$$

这是首项为 1、公比为 $\omega=e^{-2\pi ilr/N}$ 的等比数列。

2. 利用几何级数求和。

*qhc.statistics@gmail.com

若 $\omega = 1$，即 $e^{-2\pi i l r/N} = 1$，说明

$$\frac{N}{r} \mid l,$$

此时 $S(l) = N/r$。

若 $\omega \neq 1$，

$$S(l) = \frac{1-\omega^{N/r}}{1-\omega} = \frac{1-e^{-2\pi i l}}{1-\omega} = 0.$$

因此

$$S(l) = \begin{cases} N/r, & \dfrac{N}{r} \mid l, \\ 0, & \text{否则.} \end{cases}$$

代回 $\hat{f}(l)$：

$$\hat{f}(l) = \begin{cases} \dfrac{1}{\sqrt{N}} \dfrac{N}{r} \displaystyle\sum_{d=0}^{r-1} e^{-2\pi i l d/N} f(d), & \dfrac{N}{r} \mid l, \\ 0, & \text{否则.} \end{cases}$$

也就是说，$\hat{f}(l)$ 只有在 l 是 N/r 的整数倍时才可能非零。

3. 用 r 点 Fourier 变换重新写。

令

$$l = \lambda \frac{N}{r}, \qquad \lambda = 0, 1, \ldots, r-1.$$

则

$$e^{-2\pi i l d/N} = e^{-2\pi i (\lambda N/r) d/N} = e^{-2\pi i \lambda d/r}.$$

于是

$$\hat{f}\left(\lambda \frac{N}{r}\right) = \frac{\sqrt{N}}{r} \sum_{d=0}^{r-1} e^{-2\pi i \lambda d/r} f(d).$$

把 $f(d)$ 限制在一个周期上看作函数 $g(d) = f(d)$ $(0 \le d < r)$，则

$$\hat{g}(\lambda) = \frac{1}{\sqrt{r}} \sum_{d=0}^{r-1} e^{-2\pi i \lambda d/r} g(d) = \frac{1}{\sqrt{r}} \sum_{d=0}^{r-1} e^{-2\pi i \lambda d/r} f(d).$$

比较两式可得

$$\hat{f}\left(\lambda \frac{N}{r}\right) = \sqrt{\frac{N}{r}}\, \hat{g}(\lambda).$$

总结：

- 若 $N/r \nmid l$，则 $\hat{f}(l) = 0$；- 若 $l = \lambda N/r$，则 $\hat{f}(l) = \sqrt{N/r}\, \hat{g}(\lambda)$。

这说明：对周期为 r 的函数做 N 点 Fourier 变换时，只在频率是 N/r 的整数倍处有非零值，其值与 r 点变换 $\hat{g}(\lambda)$ 只差一个归一化因子。 □

练习 5.21（（求周期与相位估计））. 设 $f : \mathbb{Z} \to \mathcal{H}$ 满足 $f(x+r) = f(x)$，并定义

$$\left|\hat{f}(l)\right\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i l x/r} \left|f(x)\right\rangle, \quad l = 0, \ldots, r-1.$$

给定酉算符

$$U_y \left|f(x)\right\rangle = \left|f(x+y)\right\rangle.$$

1. 证明 $\left|\hat{f}(l)\right\rangle$ 是 U_y 的本征态，并求本征值；

2. 说明若我们只拿到某个固定的 $|f(x_0)\rangle$（而不直接访问 $f(x)$ 的黑箱），则仍可以用 U_y 构造与求周期问题中黑箱 $U:|x\rangle|0\rangle\mapsto|x\rangle|f(x)\rangle$ 同等有用的装置。

解答. **(1) 证明本征态和本征值。**

由定义

$$\left|\hat{f}(l)\right\rangle=\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{-2\pi ilx/r}|f(x)\rangle.$$

作用 U_y：

$$U_y\left|\hat{f}(l)\right\rangle=\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{-2\pi ilx/r}|f(x+y)\rangle.$$

令 $u=x+y$，则 $x=u-y$，求和区间 $u=y,\dots,r-1+y$。利用周期性 $f(u)=f(u-r)$ 可将区间“折回”到 $0,\dots,r-1$：

$$\begin{aligned}
U_y\left|\hat{f}(l)\right\rangle&=\frac{1}{\sqrt{r}}\sum_{u=y}^{r-1+y}e^{-2\pi il(u-y)/r}|f(u)\rangle\\
&=e^{2\pi ily/r}\frac{1}{\sqrt{r}}\sum_{u=y}^{r-1+y}e^{-2\pi ilu/r}|f(u)\rangle\\
&=e^{2\pi ily/r}\frac{1}{\sqrt{r}}\left(\sum_{u=y}^{r-1}e^{-2\pi ilu/r}|f(u)\rangle+\sum_{u=r}^{r-1+y}e^{-2\pi ilu/r}|f(u-r)\rangle\right)\\
&=e^{2\pi ily/r}\frac{1}{\sqrt{r}}\left(\sum_{u=y}^{r-1}e^{-2\pi ilu/r}|f(u)\rangle+\sum_{u'=0}^{y-1}e^{-2\pi il(u'+r)/r}|f(u')\rangle\right)\\
&=e^{2\pi ily/r}\frac{1}{\sqrt{r}}\left(\sum_{u=y}^{r-1}e^{-2\pi ilu/r}|f(u)\rangle+\sum_{u'=0}^{y-1}e^{-2\pi ilu'/r}|f(u')\rangle\right)\\
&=e^{2\pi ily/r}\left|\hat{f}(l)\right\rangle.
\end{aligned}$$

其中用到 $e^{-2\pi il}=1$ 以及周期性。因此 $\left|\hat{f}(l)\right\rangle$ 是 U_y 的本征态，本征值为

$$\lambda_l=e^{2\pi ily/r}.$$

(2) 用 U_y 构造“求周期黑箱”。

对任意固定 x_0，由反 Fourier 展开有

$$|f(x_0)\rangle=\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{2\pi ilx_0/r}\left|\hat{f}(l)\right\rangle.$$

考虑两寄存器状态

$$\frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle$$

（实际线路中先在第一寄存器做均匀叠加，然后用某种方式准备第二寄存器的值 $f(x)$；这里仅讨论形式）。对第二寄存器作用 U_y：

$$\begin{aligned}
\frac{1}{\sqrt{2^t}}\sum_x|x\rangle U_y|f(x)\rangle&=\frac{1}{\sqrt{2^t}}\sum_x|x\rangle\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{2\pi ilx/r}U_y\left|\hat{f}(l)\right\rangle\\
&=\frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}e^{-2\pi ily/r}\sum_x e^{2\pi ilx/r}|x\rangle\left|\hat{f}(l)\right\rangle.
\end{aligned}$$

接下来只对第一寄存器做逆 QFT：

$$\frac{1}{\sqrt{2^t}}\sum_x e^{2\pi i l x/r}\,|x\rangle \longrightarrow \left|\widetilde{l/r}\right\rangle,$$

其中 $\left|\widetilde{l/r}\right\rangle$ 是 l/r 的二进制近似编码。于是总态变为

$$\frac{1}{\sqrt{r}}\sum_{l=0}^{r-1} e^{-2\pi i l y/r}\left|\widetilde{l/r}\right\rangle\left|\hat{f}(l)\right\rangle.$$

对第一寄存器测量得到某个分数 $\widetilde{l/r}$。可以看到，相比书中标准求周期黑箱得到的状态，只多了一个全局的相位因子 $e^{-2\pi i l y/r}$ 作用在第二寄存器上，这不会影响第一寄存器测量的结果及其概率分布。

因此，利用 U_y 和一个初始态 $|f(x_0)\rangle$，通过标准的相位估计算法，我们仍然可以采样到近似的 l/r，进而像求周期问题那样从若干样本中恢复周期 r。也就是说，$|f(x)\rangle \mapsto |f(x+y)\rangle$ 的黑箱与传统的 $|x\rangle \mapsto |x\rangle|f(x)\rangle$ 在信息论意义上是等价的。 □

练习 5.22（（双变量函数的 Fourier 变换））**.** 设

$$f(x_1,x_2) = a^{sx_1+x_2} \pmod N,$$

其周期为 r。定义

$$\left|\hat{f}(l_1,l_2)\right\rangle = \frac{1}{r}\sum_{x_1,x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r}\,|f(x_1,x_2)\rangle.$$

证明

$$\left|\hat{f}(l_1,l_2)\right\rangle = \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\,|f(0,j)\rangle,$$

且只有当 $r \mid (l_1 - l_2 s)$ 时该表达式才非零。

解答. 首先注意到

$$f(x_1,x_2) = a^{sx_1+x_2} = f(0, sx_1+x_2),$$

于是

$$|f(x_1,x_2)\rangle = |f(0,sx_1+x_2)\rangle.$$

代入定义：

$$\left|\hat{f}(l_1,l_2)\right\rangle = \frac{1}{r}\sum_{x_1,x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r}\,|f(0,sx_1+x_2)\rangle.$$

令

$$j = sx_1 + x_2.$$

因为 x_2 从 0 到 $r-1$，相当于 j 从 sx_1 到 sx_1+r-1。利用 j 方向的周期性 $f(0,j+r)=f(0,j)$，我们可以把对 j 的求和区间折回到 $0,\dots,r-1$：

$$\begin{aligned}\left|\hat{f}(l_1,l_2)\right\rangle &= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{j=0}^{r-1} e^{-2\pi i(l_1x_1+l_2j-l_2sx_1)/r}\,|f(0,j)\rangle \\ &= \frac{1}{r}\sum_{x_1=0}^{r-1} e^{-2\pi i x_1(l_1-l_2s)/r}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\,|f(0,j)\rangle.\end{aligned}$$

先看外层和式

$$S := \sum_{x_1=0}^{r-1} e^{-2\pi i x_1(l_1-l_2 s)/r}.$$

这是一个单位根的和：

$$S = \begin{cases} r, & r \mid (l_1 - l_2 s), \\ 0, & r \nmid (l_1 - l_2 s). \end{cases}$$

因此

$$\left|\hat{f}(l_1,l_2)\right\rangle = \begin{cases} \displaystyle\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} \left|f(0,j)\right\rangle, & r \mid (l_1 - l_2 s), \\ 0, & r \nmid (l_1 - l_2 s). \end{cases}$$

这就完成了证明。 □

练习 5.23（（反变换还原原函数））. 利用上一题中的结果，证明

$$\frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{2\pi i(l_1x_1+l_2x_2)/r}\left|\hat{f}(l_1,l_2)\right\rangle = \left|f(x_1,x_2)\right\rangle.$$

解答. 将 5.22 题中的表达式代入左边：

$$\begin{aligned} |\Psi\rangle &:= \frac{1}{r}\sum_{l_1,l_2} e^{2\pi i(l_1x_1+l_2x_2)/r}\left|\hat{f}(l_1,l_2)\right\rangle \\ &= \frac{1}{r}\sum_{l_1,l_2} e^{2\pi i(l_1x_1+l_2x_2)/r} \cdot \begin{cases} \displaystyle\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\left|f(0,j)\right\rangle, & r \mid (l_1 - l_2 s), \\ 0, & \text{否则}. \end{cases} \end{aligned}$$

只有满足 $l_1 \equiv l_2 s \pmod r$ 的项才保留。在这些项中可写 $l_1 = l_2 s + kr$，但模 r 计算时 kr 不影响指数，因此

$$e^{2\pi i l_1 x_1/r} = e^{2\pi i l_2 s x_1/r}.$$

于是

$$|\Psi\rangle = \frac{1}{r}\sum_{l_2=0}^{r-1}\sum_{\substack{l_1 \\ l_1 \equiv l_2 s \pmod r}} e^{2\pi i(l_1x_1+l_2x_2)/r}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\left|f(0,j)\right\rangle.$$

对固定的 l_2，满足同余条件的 l_1 在 $0,\dots,r-1$ 内只有一个，记为 $l_1 = l_2 s \pmod r$。于是

$$|\Psi\rangle = \frac{1}{r}\sum_{l_2=0}^{r-1} e^{2\pi i l_2(sx_1+x_2)/r}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\left|f(0,j)\right\rangle.$$

交换求和次序：

$$|\Psi\rangle = \frac{1}{r}\sum_{j=0}^{r-1}\left[\sum_{l_2=0}^{r-1} e^{2\pi i l_2(sx_1+x_2-j)/r}\right]\left|f(0,j)\right\rangle.$$

内层和是一个标准的单位根和：

$$\sum_{l_2=0}^{r-1} e^{2\pi i l_2(sx_1+x_2-j)/r} = \begin{cases} r, & sx_1 + x_2 \equiv j \pmod r, \\ 0, & \text{否则}. \end{cases}$$

因此唯一非零项在 $j \equiv sx_1 + x_2 \pmod r$ 时出现，于是

$$|\Psi\rangle = \left|f\big(0, sx_1 + x_2\big)\right\rangle = |f(x_1, x_2)\rangle\,,$$

这里最后一步用的是 $f(x_1, x_2) = f(0, sx_1 + x_2)$。因此所给反变换确实恢复了原函数。 □

练习 5.24（（离散对数算法中测量结果的分布））. 在求离散对数的量子算法中，通过对 $|f(x_1, x_2)\rangle$ 做二维 QFT，得到的态可写为

$$\frac{1}{r}\sum_{l_1,l_2=0}^{r-1} |l_1, l_2\rangle \left|\hat{f}(l_1, l_2)\right\rangle.$$

结合练习 *5.22* 的结论，分析测量前两个寄存器得到某一对 (l_1, l_2) 的概率分布，并说明这等价于得到一个随机解满足

$$l_1 \equiv sl_2 \pmod r,$$

从而可以通过经典后处理恢复离散对数 s。

解答. 由 5.22 的结果，

$$\left|\hat{f}(l_1, l_2)\right\rangle = \begin{cases} \displaystyle\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\,|f(0, j)\rangle\,, & r \mid (l_1 - l_2 s), \\ 0, & \text{否则.} \end{cases}$$

因此上述总态实际上只有那些满足

$$l_1 \equiv sl_2 \pmod r$$

的项有振幅，其余项振幅为零。把态写为

$$|\Psi\rangle = \frac{1}{r}\sum_{l_1,l_2} |l_1, l_2\rangle \left|\hat{f}(l_1, l_2)\right\rangle,$$

则测量第一二寄存器得到一对 (l_1, l_2) 的非零概率当且仅当 $r \mid (l_1 - l_2 s)$。

在满足该条件的项中，第三寄存器的态

$$|\phi_{l_2}\rangle := \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r}\,|f(0, j)\rangle$$

与 (l_1, l_2) 的振幅大小无关（仅依赖 l_2），而 $||\phi_{l_2}\rangle|$ 对所有允许的 l_2 是一致的。再加上前因子 $1/r$，可以看出所有满足 $l_1 \equiv sl_2 \pmod r$ 的对 (l_1, l_2) 出现的概率是均匀的。

因此，算法每次运行，在前两个寄存器上给出一组随机方程

$$l_1 \equiv sl_2 \pmod r.$$

若随机到的 l_2 与 r 互素，则可以在 $\mathbb{Z}_r$ 中算出 l_2^{-1}，从而得到

$$s \equiv l_1 l_2^{-1} \pmod r.$$

$\gcd(l_2, r) = 1$ 的概率约为 $\varphi(r)/r$，大致在常数量级上（随 r 缓慢下降）。因此重复若干次即可以高概率获得一个“好”的样本，从而恢复离散对数 s。

这说明测量前两个寄存器等价于得到一组随机的线性同余方程 $l_1 \equiv sl_2 \pmod r$，完全符合离散对数量子算法的设计。 □

练习 5.25（（实现算法中用到的黑箱））. 在离散对数的量子算法中，需要一个酉算符

$$U : |x_1\rangle |x_2\rangle |y\rangle \longmapsto |x_1\rangle |x_2\rangle |y \cdot b^{x_1} a^{x_2} \bmod N\rangle ,$$

其中 N 为 L 位整数，$a, b \in \mathbb{Z}_N^\times$。仅使用模乘、模加等基本算术门，估算实现该 U 所需的基本门数的量级。

解答. 整体上看，U 是一个经典可逆运算的量子提升：输入 (x_1, x_2, y)，输出 $(x_1, x_2, y \cdot b^{x_1} a^{x_2} \bmod N)$。

1. 计算 $b^{x_1} \bmod N$ 与 $a^{x_2} \bmod N$。

采用“重复平方法”计算幂：对一个固定基 g，要计算 $g^x \bmod N$，可以预先准备

$$g^{2^0}, g^{2^1}, g^{2^2}, \ldots, g^{2^{L-1}} \ (\mathrm{mod} N),$$

然后根据 x 的二进制展开 $x = \sum_k x_k 2^k$，依次在对应的位为 1 时乘上 g^{2^k}。

- 每次模乘（L 位数之间）可以在 $O(L^2)$ 个基本门内完成；- 对每个幂计算需进行 $O(L)$ 次模乘，因此单次模指数运算的复杂度为 $O(L^3)$。

同理，可在 $O(L^3)$ 门数内实现量子版本的 $|x_1\rangle |1\rangle \mapsto |x_1\rangle |b^{x_1} \bmod N\rangle$，以及 $|x_2\rangle |1\rangle \mapsto |x_2\rangle |a^{x_2} \bmod N\rangle$。

2. 计算 $y \cdot b^{x_1} a^{x_2} \bmod N$。

设已经在辅助寄存器中得到了 $|b^{x_1}\rangle$ 与 $|a^{x_2}\rangle$。可以先做一次模乘得到

$$c := b^{x_1} a^{x_2} \bmod N,$$

再做一次模乘

$$y \cdot c \bmod N.$$

这两次模乘各需要 $O(L^2)$ 个基本门，因此和指数运算相比可以忽略不计。

3. 汇总复杂度。

- 量子模指数 b^{x_1} 和 a^{x_2} 各需要 $O(L^3)$ 个基本门；- 额外的模乘和一些模加、寄存器交换、清除辅助比特等操作，总量是 $O(L^2)$ 量级。

因此，实现黑箱 U 所需的总门数是

$$O(L^3),$$

与 Shor 算法中的模指数运算同一复杂度量级。 □

练习 5.26（（离散对数问题的复杂度含义））. 综合本节讨论，说明：若存在一个多项式规模的量子算法，可以在给定 N, a, b 的情况下以常数成功概率求出

$$s = \log_a b \pmod r, \qquad a^r \equiv 1 \pmod N,$$

则整数分解问题属于 BQP，即存在多项式规模的量子算法可以分解一般整数 N。并简要说明其思路与 *Shor* 因数分解算法之间的联系。

解答. 关键是：**知道离散对数就能知道阶，而知道阶就能因数分解**。

1. 从离散对数到阶。

对任意选取的 $a \in \mathbb{Z}_N^\times$，设其阶为 r，即 $a^r \equiv 1 \pmod N$。若我们有一个能高效求解离散对数的量子算法，则可以在同一群中构造若干对 (a, b) 使得

$$b = a^k \bmod N$$

的指数 k 与 r 之间有简单关系，从而利用

$$k = \log_a b \pmod r$$

的信息恢复 r。例如选择 $b = a^{2^m}$ 等等，配合若干次调用离散对数子程序和简单的数论运算，可以确定 r 的素因子分解，从而得到 r 本身。

（这里的构造类似于经典“从离散对数求群阶”的标准做法，只是将其中计算密集部分交给量子离散对数子程序完成。）

2. 从阶到因数分解。

一旦求得一个元素 a 的阶 r，就可以像 Shor 算法那样分解 N：

- 随机选择 $a \in \mathbb{Z}_N^\times$；
- 若 r 为奇数或 $a^{r/2} \equiv -1 \pmod N$，则重选；
- 否则计算

$$d_1 = \gcd(a^{r/2} - 1, N), \qquad d_2 = \gcd(a^{r/2} + 1, N),$$

则 d_1, d_2 中至少有一个是 N 的非平凡因子。

求 gcd 可以在经典多项式时间内完成，因此整个过程的时间主要花在“求阶”上。

3. 复杂度与 BQP。

若假设离散对数在给定 (N, a, b) 时可以由某个量子算法在多项式时间内、以常数成功概率求出，那么上一步从离散对数到阶的过程也只需要多项式次调用该子程序和多项式时间的经典运算。于是求阶问题落在 BQP 中。

再加上“从阶到因数分解”的那步完全是经典多项式时间操作，所以整体上，因数分解问题也落在 BQP 中。

这与 Shor 算法的思路是一致的：Shor 直接通过相位估计求周期（阶）；而本题是假设有一个求离散对数的量子子程序，先借它求阶，再按 Shor 的后处理步骤分解 N。两者都体现了“求阶 $\Rightarrow$ 分解”这一核心结构。 □

练习 5.27（（有限阿贝尔群的素幂分解））. 当然，一般的有限阿贝尔群 G 到素幂阶循环群乘积的分解通常是一个困难问题（至少和整数因子分解一样难）。这里可以用量子算法来“补救”：说明如何利用本章的量子算法，有效地把 G 分解成若干素幂阶循环群的直和。

解答. 先回顾一点群论：有限阿贝尔群结构定理告诉我们

$$G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}},$$

其中 p_i 是素数（允许相同），$r_i \geq 1$。题目要我们说明：怎样用本章的量子算法“真的算出”这样的分解。

整体思路分两步：

（A）先把 G 分解成若干循环群 $\quad G \cong \bigoplus_{j=1}^{m} \mathbb{Z}_{r_j}$，

这里 r_j 不一定是素数幂；

（B）再利用量子因子分解算法把每个 r_j 拆成素数幂，并据此细化为素幂阶分解。

下面按这个思路往下拆。

第 1 步：得到 $G \cong \bigoplus_j \mathbb{Z}_{r_j}$ 的分解

在本章前面已经说明：若我们能计算元素阶、做离散对数，就能用完全经典的多项式时间算法把一个有限阿贝尔群分解成若干循环群的直和。关键是这些“计算阶、做离散对数”的子任务可以用量子算法高效完成：

- 元素的阶可以通过“周期寻找”量子算法（本章用来做因式分解的那套）在多项式时间里求出；
- 离散对数也可以化成一个隐含子群问题，用阿贝尔隐含子群的量子算法求解。

于是我们可以（在期望多项式时间内）得到一组元素

$$a_1, \dots, a_m \in G, \qquad \text{阶分别为} r_1, \dots, r_m,$$

满足：

$$\forall g \in G, \quad g = a_1^{x_1} \cdots a_m^{x_m}, \quad 0 \le x_j < r_j,$$

并且表示是唯一的。也就是说已经有了一个同构

$$G \;\cong\; \mathbb{Z}_{r_1} \oplus \cdots \oplus \mathbb{Z}_{r_m},$$

其中第 j 个分量的生成元可以看成是 a_j。

这一步的量子开销是多项式于 $\log |G|$ 的（调用若干次求阶、离散对数的量子子程序）。

第 2 步：用量子因式分解细化成素幂阶分解

现在只剩下纯“整数问题”：对每个 r_j，用 Shor 因式分解算法求出它的素因子分解

$$r_j = \prod_{\ell} p_{j,\ell}^{e_{j,\ell}}.$$

Shor 算法在期望时间 $\mathrm{poly}(\log r_j)$ 内完成，这对每个 r_j 都是多项式时间。

如何把 $\mathbb{Z}_{r_j}$ 拆成若干 $\mathbb{Z}_{p^e}$？

纯群论事实：若 m, n 互素，则

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

因此对 $r_j = \prod_\ell p_{j,\ell}^{e_{j,\ell}}$，有自然同构

$$\mathbb{Z}_{r_j} \cong \bigoplus_{\ell} \mathbb{Z}_{p_{j,\ell}^{e_{j,\ell}}}.$$

在实际算法里，还需要给出这些子群对应的具体生成元。做法也很简单：设 a_j 生成 $\mathbb{Z}_{r_j}$，定义

$$g_{j,\ell} := a_j^{\,r_j / p_{j,\ell}^{e_{j,\ell}}}.$$

那么 $g_{j,\ell}$ 的阶正好是 $p_{j,\ell}^{e_{j,\ell}}$（因为把 a_j 提升这么多次以后，剩下的周期就是这一个素数幂），从而每个 $g_{j,\ell}$ 生成一个阶为 $p_{j,\ell}^{e_{j,\ell}}$ 的循环子群。

更进一步，还可以验证：

$$\langle g_{j,\ell} \;:\; \text{所有} \ell \rangle \quad \cong \quad \bigoplus_{\ell} \mathbb{Z}_{p_{j,\ell}^{e_{j,\ell}}},$$

并且它恰好等于原来 $\langle a_j \rangle$ 这个子群。对所有 j 进行同样的操作，就得到

$$G \cong \bigoplus_{j,\ell} \mathbb{Z}_{p_{j,\ell}^{e_{j,\ell}}},$$

即所需的素幂阶循环群分解。

时间复杂度

- m（循环因子个数）满足 $m = O(\log |G|)$；
- 对每个 r_j 做量子因式分解的开销是 $\mathrm{poly}(\log r_j) \le \mathrm{poly}(\log |G|)$。

所以总的量子时间是 $\mathrm{poly}(\log |G|)$，也就是多项式于输入规模（元素编码长度）的期望时间。失败概率可以像本章前面一样，通过重复运行、取多数表决，把它压低到任意小的 ε。

综上，用本章的求阶、离散对数与因式分解算法，确实可以在期望多项式时间内，把有限阿贝尔群 G 分解成若干素幂阶循环群的直和。 □

练习 5.28（（有限阿贝尔群上隐含子群问题的完整算法））. 详细写出对有限阿贝尔群解决隐含子群问题的量子算法，给出运行时间和成功概率的估计。

解答. **1. 问题设定（Abelian HSP）**

给定有限阿贝尔群 G，并且我们已经知道它的分解

$$G \cong \mathbb{Z}_{r_1} \oplus \cdots \oplus \mathbb{Z}_{r_n},$$

即任意 $g \in G$ 都可以唯一写成

$$g = (g_1, \ldots, g_n), \qquad 0 \le g_j < r_j.$$

给定一个函数 $f : G \to Y$，满足：

- 存在某个子群 $K \le G$，使得 f 在每个陪集 $g + K$ 上都是常数；
- 在不同的陪集上取到的函数值都不同（即 f 在 G/K 上是单射）。

目标：用量子算法找出 K 的一个生成元集合。

我们还假设有一个黑箱酉算符 U_f 可供调用：

$$U_f : |x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle\,,$$

第二个寄存器用来存放函数值。

2. 高层想法：先找 $K^\perp$，再还原 K

对阿贝尔群 G，它的“对偶群” $\widehat{G}$ 同样是一个阿贝尔群，元素是特征（characters）$\chi : G \to \mathbb{C}$。对于前面的分解，有一个自然同构

$$\widehat{G} \cong G, \quad l = (l_1, \ldots, l_n) \mapsto \chi_l,$$

其中

$$\chi_l(g) = \exp\Big(2\pi i \sum_{j=1}^{n} \frac{g_j l_j}{r_j}\Big).$$

对任意子群 $K \le G$，定义

$$K^\perp = \{\, l \in G : \ \chi_l(k) = 1, \ \forall k \in K \,\},$$

这是 $\widehat{G}$ 中的一个正交子群。经典结论：$K^\perp$ 完全确定 K，而且可以从 $K^\perp$ 的生成元集合算法地算出 K 的生成元（本章附录给出了用 Smith 标准形求解的办法）。

量子部分要做的就是：通过 QFT 从 f 中“抽样”出 $K^\perp$ 的随机元素；然后用经典算法从这些样本恢复 K。

3. 量子算法主体（一次采样）

一次运行算法的核心步骤可以简化为：

1. 制备 G 上的均匀叠加。

   用 n 个寄存器分别表示每个坐标 g_j，大小至少 $\lceil \log_2 r_j \rceil$ 比特。通过 Hadamard 与适当的“截断/拒绝采样”等标准技巧，可以在多项式时间内制备近似均匀的态

   $$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|0\rangle\,.$$

   （书中第 5 章已经详细说明怎么处理 r_j 不是 2 的幂的情况，这里不再展开细节。）

2. 调用一次黑箱 U_f：

   $$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|f(g)\rangle\,.$$

3. 丢弃函数值寄存器。

   可以直接忽略第二寄存器，相当于对它做一次测量并忘记结果。第一寄存器于是变成一个混合态：

   $$\rho = \frac{1}{|G/K|} \sum_{\text{陪集}C} |\psi_C\rangle\,\langle\psi_C|\,,$$

   其中

   $$|\psi_C\rangle = \frac{1}{\sqrt{|K|}} \sum_{k\in K} |c+k\rangle$$

   是每个陪集上均匀叠加的量子态。

4. 对第一寄存器做 G 上的量子傅里叶变换 QFT。

   量子傅里叶变换 F_G 把基矢 $|g\rangle$ 映到

   $$F_G\,|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{l\in G} \chi_l(g)\,|l\rangle\,.$$

   对每个 $|\psi_C\rangle$ 应用 F_G，可以得到

   $$F_G\,|\psi_C\rangle = \sqrt{\frac{|K|}{|G|}} \sum_{l\in K^\perp} \chi_l(C)\,|l\rangle\,.$$

   重要的是：只在 $K^\perp$ 上有振幅，且模长相同。

5. 测量第一寄存器。

   因为上一步的振幅在 $K^\perp$ 上是均匀的，测量结果 l 将是 $K^\perp$ 中的一个随机元素，且服从均匀分布。

这样一次运行算法，我们就从 $K^\perp$ 中抽到了一个随机元素 l。

4. 重复采样，直到生成 $K^\perp$

令 n_0 为生成 $K^\perp$ 所需的最少生成元数。群论可以证明，对任何有限阿贝尔群都有

$$n_0 \le \log_2 |K^\perp| \le \log_2 |G| = O(\log |G|).$$

如果我们独立地从 $K^\perp$ 中均匀抽取元素 $l^{(1)}, l^{(2)}, \dots$，则有一个简单的引理（书中附录有证明）：

引理：设 H 是有限阿贝尔群，需要 r 个生成元即可生成。则从 H 中均匀随机地取 mr 个元素，它们生成整个 H 的概率至少为 $1 - r2^{-m}$。

套在 $H = K^\perp$ 上就得到：只要我们取

$$J = O\Big(\log|G|\big(\log\log|G| + \log(1/\varepsilon)\big)\Big)$$

个样本 $l^{(1)}, \dots, l^{(J)}$，它们生成整个 $K^\perp$ 的概率就至少是 $1 - \varepsilon$。

5. 从 $K^\perp$ 的生成元算出 K

现在我们有了一组 $K^\perp$ 的生成元 $\{l^{(j)}\}$。剩下是纯经典的计算：求出所有

$$k = (k_1, \dots, k_n) \in G$$

使得对所有 j 都有

$$\chi_{l^{(j)}}(k) = 1.$$

展开一下 χ 的定义，上式等价于一堆模方程：

$$\sum_{i=1}^{n} \frac{k_i l_i^{(j)}}{r_i} \equiv 0 \pmod 1 \quad \Longleftrightarrow \quad \sum_{i=1}^{n} s_i l_i^{(j)} k_i \equiv 0 \pmod r$$

（适当选 $r = \mathrm{lcm}(r_1, \dots, r_n)$，$s_i = r/r_i$）。这是一组线性方程（在模 r 环里），可以用 Smith 标准形等线性代数工具在多项式时间内求解，从而得到 K 的一个生成元集合。

6. 复杂度小结

- 量子部分：
  每一次采样调用一次 U_f，再做一次 QFT，门数是 $\mathrm{poly}(\log|G|)$。总共采样 $J = O(\log|G|(\log\log|G| + \log(1/\varepsilon)))$ 次，所以

  $$\text{调用} U_f \text{ 的次数和总量子门数都是} \mathrm{poly}(\log|G|, \log(1/\varepsilon)).$$

- 经典部分：
  主要是解一个规模 $O(\log|G|)$ 的线性方程组，同样是多项式时间。

7. 结论（一句话版）

这个算法通过 QFT 把“在 G 上的函数 f 隐含的子群 K”转换成“在对偶群 $\widehat{G}$ 上的正交子群 $K^\perp$ 的随机样本”，再用线性代数恢复 K。整体运行时间是 $\mathrm{poly}(\log|G|)$，成功概率可以放大到任意接近 1。 □

练习 5.29（（用 HSP 框架重写 Deutsch 和 Simon 算法））. 使用隐含子群问题的框架，给出解决在图 *5–5* 列出的 *Deutsch* 问题和 *Simon* 问题的量子算法。

解答. 这一题的意思是：把「Deutsch 问题」和「Simon 问题」重新包装成“在某个阿贝尔群上的隐含子群问题”，然后用上一题的 HSP 思路来写出算法。我们分别处理。

一、Deutsch 问题

问题回顾：群取 $G = \mathbb{Z}_2 = \{0, 1\}$。给定一个黑箱函数

$$f : G \to \mathbb{Z}_2,$$

我们知道只有两种可能：

- 常值： $f(0) = f(1)$；
- 平衡： $f(0) \neq f(1)$。

目标是区分这两种情况。
在 HSP 视角下，我们把“隐藏子群”选成：

- 若 f 常值，则 $K = G$（整群都是“对称”）；
- 若 f 平衡，则 $K = \{0\}$（只有平凡子群）。

于是我们要做的其实是：判断隐藏子群到底是 G 还是 $\{0\}$。

算法（*HSP* 风格，但是专门为 $G = \mathbb{Z}_2$ 简化）：

1. 准备两比特初态 $|0\rangle\,|0\rangle$。
2. 对第一个比特做 Hadamard：
$$|0\rangle\,|0\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\,|0\rangle\,.$$
这就是 G 上的均匀叠加。
3. 调用一次黑箱 U_f：
$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle\,|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle\,|f(x)\rangle\,.$$
4. 再对第一个比特做 Hadamard（这一步起到 QFT 的作用，因为 $\mathbb{Z}_2$ 上的 QFT 就是 H）：
$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle\,|f(x)\rangle \xrightarrow{H\otimes I} \frac{1}{2}\sum_{l=0}^{1}\left(\sum_{x=0}^{1}(-1)^{lx}\,|x\rangle\right)|f(x)\rangle\,.$$
把第二比特当作“附属寄存器”，可以看成
$$\frac{1}{\sqrt{2}}\sum_{l=0}^{1}|l\rangle\,\left|\widehat{f}(l)\right\rangle,$$
其中 $\left|\widehat{f}(l)\right\rangle$ 是某个依赖于 f 的态。
5. 测量第一个比特，得到结果 $l \in \{0,1\}$。
6. 若测到 $l = 0$，输出“f 可能是常值”；若测到 $l = 1$，输出“f 是平衡”的判断。可以重复整个过程多次：如果多次测量中至少出现过一次 1，就几乎可以肯定是平衡；若一直都是 0，就判断为常值。

为什么这样做？
计算一下
$$\left|\widehat{f}(l)\right\rangle = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{lx}\,|f(x)\rangle\,.$$

- 若 f 常值，容易看出只有 $l = 0$ 时这个向量非零，也就是说测量 l 一定得到 0；
- 若 f 平衡，那么 $l = 0$ 和 $l = 1$ 的概率都是 1/2。

于是：常值时算法永远不会错，平衡时有一半概率给出正确答案。重复 n 次，只要有一次测到 1 我们就能确定是平衡；错判的概率变成 2^{-n}，可以做到任意小。

这就是 Deutsch 问题在 HSP 框架下的一种量子算法（不是课本 1 章里那个“完美判别”的版本，但结构更接近一般 HSP 算法）。

二、Simon 问题

问题回顾：现在群是 $G = \mathbb{Z}_2^n$。给定一个黑箱函数

$$f : G \to X,$$

存在一个未知“秘密”向量 $s \in \mathbb{Z}_2^n$，使得

$$f(y) = f(x) \quad \Longleftrightarrow \quad y = x \text{ 或 } y = x \oplus s.$$

也就是说，每个函数值恰好对应两个输入 x、$x \oplus s$。目标是找出 s。

在 HSP 视角下，隐藏子群就是

$$K = \{0, s\} \subseteq \mathbb{Z}_2^n.$$

算法（基本就是 *Simon* 原始算法，只是用 *HSP* 的语言解释）：

1. 准备初态 $|0\rangle^{\otimes n} |0\rangle$。

2. 对前 n 个比特做 $H^{\otimes n}$，得到

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} |x\rangle |0\rangle .$$

这就是 G 上的均匀叠加。

3. 调用一次 U_f：

$$\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle |f(x)\rangle .$$

4. （可选）测量第二寄存器并忘掉结果。

无论是否测量第二寄存器，对第一寄存器的有效状态都可以理解为某个陪集 $x + K$ 上的均匀叠加（即 $|x\rangle$ 和 $|x \oplus s\rangle$ 的均匀和）。

5. 对第一寄存器做 $H^{\otimes n}$（即对 G 做 QFT）：

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{l \in \mathbb{Z}_2^n} (-1)^{l \cdot x} |l\rangle .$$

对 $|x\rangle + |x \oplus s\rangle$ 这样的叠加应用 $H^{\otimes n}$ 得到

$$\frac{1}{\sqrt{2^{n-1}}} \sum_{l : l \cdot s = 0} (-1)^{l \cdot x} |l\rangle ,$$

也就是说：测量时得到的 l 一定满足

$$l \cdot s = 0 \pmod 2.$$

这正是 $K^{\perp}$ 的定义。

6. 测量第一寄存器，得到一个向量 $l^{(1)}$，它是从 $K^{\perp}$ 中均匀随机抽到的。

7. 重复上述步骤 J 次，得到 $l^{(1)}, \dots, l^{(J)}$。这里取

$$J = n\,m, \qquad m = O\big(\log n + \log(1/\varepsilon)\big),$$

可以保证这 J 个向量以至少 $1-\varepsilon$ 的概率生成整个 $K^{\perp}$。

8. 现在我们要从这些 $l^{(j)}$ 中“解出” s：它必须满足

$$s \cdot l^{(j)} = 0 \pmod 2, \qquad j = 1, \dots, J.$$

这是一组线性方程（模 2），未知量是 s 的 n 个比特。用高斯消元等经典线性代数方法可以在 $O(n^3)$ 时间内求出 s，并且上面的选择保证“解”几乎肯定是唯一的真实 s。

复杂度与成功概率：

- 每次运行算法调用一次黑箱 U_f，加上 $O(n^2)$ 个门实现 $H^{\otimes n}$；
- 总共运行 $J = nm = O\big(n(\log n + \log(1/\varepsilon))\big)$ 次；
- 经典部分解线性方程组的时间为 $O(J^3)$，仍是多项式时间；
- 根据前面“随机生成元”引理，选择这样的 J，可以保证最终恢复到 s 的概率至少为 $1-\varepsilon$。

小结

Deutsch 问题和 Simon 问题都可以看成是「在某个 $\mathbb{Z}_2^n$ 上寻找隐藏子群」的特例：

- Deutsch：$G = \mathbb{Z}_2$，隐藏子群要么是 G，要么是 $\{0\}$；
- Simon：$G = \mathbb{Z}_2^n$，隐藏子群是 $\{0, s\}$。

用一般的 Abelian HSP 量子算法思路（均匀叠加 $\to$ 调用 f $\to$ QFT $\to$ 抽样 $K^{\perp}$ $\to$ 经典线性代数）就能自然地得到这两个著名算法的量子版本。 □