4.5 通用量子门——习题与详细解答

DanX, Yuchen He*

练习 4.36 (双比特模 4 加法电路)**.** 构造一个把双比特数 x 和 y 进行模 4 加的量子线路，即线路完成

$$|x, y\rangle \longmapsto |x, (x+y) \bmod 4\rangle .$$

解答. 把两个双比特数写成二进制位：

$$x = 2a + b, \qquad y = 2c + d, \qquad a, b, c, d \in \{0, 1\},$$

并约定四条量子比特线路自上而下分别存放

$$|a\, b\, c\, d\rangle .$$

题目要求的变换是

$$|a\, b\, c\, d\rangle \longmapsto |a\, b\, e\, f\rangle ,$$

其中 (e, f) 是二进制表示的 $(x + y) \bmod 4$。

先写出经典的二进制加法规则。令

$$s = x + y = 2(a + c) + (b + d).$$

最低位（模 2）显然是

$$f = (b + d) \bmod 2 = b \oplus d.$$

进位为

$$\mathrm{carry}_0 = \left\lfloor \frac{b+d}{2} \right\rfloor = bd,$$

于是高位为

$$e = (a + c + \mathrm{carry}_0) \bmod 2 = a \oplus c \oplus (bd).$$

因此只要在保持 a, b 不变的前提下，把

$$(c, d) \mapsto (e, f)$$

实现为

$$f = b \oplus d, \qquad e = a \oplus c \oplus (bd),$$

*heyuchen@tgqs.net

就得到了所需的可逆线路。

构造一条仅用 CNOT 和 Toffoli 的线路

从上到下仍记四条量子比特为 a, b, c, d。可以按下列顺序作用门：

(1) 对 (b, d) 作为控制、c 为目标施加一记 Toffoli：

$$c \longrightarrow c \oplus (bd).$$

(2) 对 a 控、c 目标施加一记 CNOT：

$$c \longrightarrow c \oplus a.$$

此时

$$c = c \oplus (bd) \oplus a = a \oplus c \oplus (bd) = e.$$

(3) 对 b 控、d 目标再施加一记 CNOT：

$$d \longrightarrow d \oplus b = f.$$

这样整个线路在计算基上实现的映射就是

$$|a\, b\, c\, d\rangle \longmapsto |a\, b\, e\, f\rangle,$$

其中

$$e = a \oplus c \oplus (bd), \qquad f = b \oplus d.$$

如果只允许使用单比特门和 CNOT，可以再利用前面 4.24 题中 Toffoli 的分解，把上面那记 Toffoli 展开成若干 CNOT 和单比特门即可。 □

练习 4.37 (一个 4×4 酉的两级分解)**.** 求变换

$$U = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \end{bmatrix}$$

的一个两级酉矩阵分解。

解答. 所谓两级酉矩阵，是指在计算基下只在某两个基矢张成的二维子空间上非平凡，在其正交补上等于恒等的酉矩阵。4×4 情形下，就是“只有一个 2×2 非平凡子块”的酉矩阵。

这一题可以用教材 4.5 节介绍的“逐列消元”算法来做：从 U 的第一列开始，用若干两级酉矩阵把第一列化为 $(1, 0, 0, 0)^{\mathsf{T}}$，再处理第二列，以此类推。算法保证最后得到的分解中，每一步都是两级酉。

具体算出来的一种分解如下。存在六个两级酉矩阵 U_k（下面给出的是它们的共轭转置 $U_k^\dagger$），使得

$$U = U_1^\dagger U_2^\dagger U_3^\dagger U_4^\dagger U_5^\dagger U_6^\dagger.$$

一组可行的 $U_k^\dagger$ 为

$$U_1^\dagger = \begin{bmatrix} \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & 0 & 0 \\ \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad U_2^\dagger = \begin{bmatrix} \sqrt{\frac{2}{3}} & 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & 1 & 0 & 0 \\ \sqrt{\frac{1}{3}} & 0 & -\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad U_3^\dagger = \begin{bmatrix} \sqrt{\frac{3}{4}} & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & -\sqrt{\frac{3}{4}} \end{bmatrix},$$

$$U_4^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \dfrac{\sqrt{3}(1-\mathrm{i})}{4} & \dfrac{3-\mathrm{i}}{4} & 0 \\ 0 & \dfrac{3+\mathrm{i}}{4} & -\dfrac{\sqrt{3}(1+\mathrm{i})}{4} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad U_5^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & 0 & -\mathrm{i}\sqrt{\frac{1}{3}} \\ 0 & 0 & 1 & 0 \\ 0 & \mathrm{i}\sqrt{\frac{1}{3}} & 0 & -\sqrt{\frac{2}{3}} \end{bmatrix}, \quad U_6^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{1}{2}} & \mathrm{i}\sqrt{\frac{1}{2}} \\ 0 & 0 & -\sqrt{\frac{1}{2}} & \mathrm{i}\sqrt{\frac{1}{2}} \end{bmatrix}.$$

可以直接检查：每个 $U_k^\dagger$ 只在某两个基态之间发生非平凡作用（矩阵中对应的 2×2 子块），因此都是两级酉；把它们相乘可得到题目给出的 U。这就给出了所需的一个两级酉矩阵分解。 □

练习 4.38. *证明存在 $d\times d$ 酉矩阵 U，它不能分解为少于 $d-1$ 个两级酉矩阵的乘积。*

解答. 思路是：证明任何 $d-1$ 个两级矩阵的乘积在某个位置上必然为零元素，于是只要取一个没有零元的酉矩阵（例如适当缩放的 Fourier 矩阵），它就不可能由少于 $d-1$ 个两级酉矩阵的乘积表示。

注意：下面的证明与矩阵是否是酉矩阵无关，因此也适用于两级酉矩阵。

1. 先看 $d=3$ 的简单情形

对 3×3 的两级矩阵，每个矩阵在某一个 2×2 子块上任意，其他对角为 1、非对角为 0。举例：

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{bmatrix}, \quad B = \begin{bmatrix} e & 0 & f \\ 0 & 1 & 0 \\ g & 0 & h \end{bmatrix}.$$

它们的乘积

$$AB = \begin{bmatrix} e & 0 & f \\ bg & a & bh \\ dg & c & dh \end{bmatrix}$$

显然在第二列第一行是 0。对其它可能的 2×2 子块位置做类似检查，可以发现：*任意两个 3×3 的两级矩阵相乘，总有一个元素为 0。*

因此对于 $d=3$，任何由 2 个两级矩阵构成的乘积矩阵都含有零元素，从而不可能等于一个各元素都非零的矩阵。这样的矩阵显然存在，例如

$$U=\frac{1}{\sqrt{3}}\begin{bmatrix}1 & 1 & 1\\ 1 & \omega & \omega^2\\ 1 & \omega^2 & \omega\end{bmatrix},\quad \omega=e^{2\pi \mathrm{i}/3},$$

是一个酉矩阵且所有元素非零。

2. 一般 d 的情形

现在考虑一般的 $d\geq 3$。我们在 $\mathbb{C}^{d\times d}$ 中取 $d-1$ 个两级矩阵

$$M^1, M^2, \ldots, M^{d-1},$$

它们的乘积记作

$$U=M^1M^2\cdots M^{d-1}.$$

每个两级矩阵 M^k 的“非平凡子块”都在某个索引集合

$$\sigma_k=\{p_k,q_k\}\subset\{1,2,\ldots,d\},\qquad |\sigma_k|\leq 2$$

对应的行列上，其余地方在对角线上为 1，非对角为 0。

我们要证明：*无论这些 σ_k 如何选择*，U 的某个元素必为 0。

(1) 固定一行，跟踪可能到达的列指标

为了方便表述，下面所有下标都用 1 起始。利用“至少有一个索引没被第一块用到”的事实，必存在某个

$$k\notin\sigma_1.$$

固定这一行号 k，来看 U 的第 k 行。

按矩阵乘法定义，

$$U_{kl}=\sum_{i_1,\ldots,i_{d-2}} M^1_{ki_1}M^2_{i_1i_2}\cdots M^{d-1}_{i_{d-2}l}.$$

若要 $U_{kl}\neq 0$，至少存在一条“索引路径”

$$k=i_0\to i_1\to i_2\to\cdots\to i_{d-2}\to l$$

使得每一段上的矩阵元都不为零：

$$M^1_{ki_1}M^2_{i_1i_2}\cdots M^{d-1}_{i_{d-2}l}\neq 0.$$

定义

$$S_n=\{\, i_n \mid \exists i_1,\ldots,i_{n-1} \text{ 使上式前 } n \text{ 项不为 } 0\,\}$$

为“在第 n 步可能到达的行（列）索引集合”。我们的目标是控制 $|S_n|$ 的大小。

(2) 递推估计 $|S_n|$

首先看 $n=1$。由于 $k\notin\sigma_1$，M^1 在第 k 行只有对角元 $M^1_{kk}=1$ 非零，其它 $M^1_{kj}=0$。因此

$$S_1=\{k\},\qquad |S_1|=1.$$

再看由 M^2 作用后的 S_2。若 $i_1\notin\sigma_2$，则第 i_1 行只有对角元非零，所以 $i_2=i_1$ 唯一；若 $i_1\in\sigma_2$，则 i_2 可以在 σ_2 的两个元素中任选一个。综合起来，有

$$|S_2|\le|S_1\cup\sigma_2|\le|S_1|+|\sigma_2|-1\le 1+2-1=2.$$

同理，对一般的 $n\ge 2$：

- 若 $i_{n-1}\notin\sigma_n$，则 $i_n=i_{n-1}$，所以 $S_n=S_{n-1}$；
- 若 $i_{n-1}\in\sigma_n$，则 $i_n\in\sigma_n$，因此

$$S_n\subset S_{n-1}\cup\sigma_n,\qquad |S_n|\le|S_{n-1}|+|\sigma_n|-1\le|S_{n-1}|+1.$$

归纳得到

$$|S_n|\le n,\qquad n=1,2,\dots,d-1.$$

(3) 最后一列的可能取值个数不超过 $d-1$

最后一步是由 M^{d-1} 把 i_{d-2} 映到最终的列指标 l。对每个可能的 $i_{d-2}\in S_{d-2}$，最多引入一个新的指标（当 $i_{d-2}\in\sigma_{d-1}$ 时），于是所有可能的 l 的集合 $\mathscr{S}_l$ 满足

$$|\mathscr{S}_l|\le|S_{d-2}|+1\le(d-2)+1=d-1.$$

也就是说，第 k 行中，至多有 $d-1$ 个位置 l 能取得非零值。总共有 d 列，因此至少有一个列指标 l_0 不在 $\mathscr{S}_l$ 中，对应的元素必为 0：

$$U_{kl_0}=0.$$

这就说明：任何 $d-1$ 个两级矩阵的乘积 U 至少有一个零元素。

3. 取一个所有元素都非零的酉矩阵

例如 d 维离散 Fourier 矩阵

$$F_{jk}=\frac{1}{\sqrt{d}}\,\omega^{jk},\qquad \omega=e^{2\pi\mathrm{i}/d},\ j,k=0,\dots,d-1$$

显然是酉矩阵，而且所有元素都非零。由上面的结论，它不可能写成少于 $d-1$ 个两级矩阵的乘积。

因此，存在这样的 $d\times d$ 酉矩阵 U，不能分解为少于 $d-1$ 个两级酉矩阵的乘积。证毕。 □

练习 4.39. 求一个用单量子比特运算和受控非门的量子线路，实现变换

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & c & 0 & 0 & 0 & 0 & d \end{bmatrix},$$

其中 $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ 是任意 2×2 酉矩阵。

解答. 从矩阵的非零元素可以看出，它只在计算基态

$$|010\rangle, \quad |111\rangle$$

张成的二维子空间上产生非平凡作用，其余 6 个基态都保持不变。因此该变换是一个三比特两级酉矩阵，在子空间

$$\mathcal{H}_{\text{sub}} = \text{span}\{|010\rangle, |111\rangle\}$$

上的作用恰好是 $\tilde{U}$。

教材 4.5.2 已经给出了“任意两级酉矩阵用单比特门 + CNOT 构造”的一般方法。其要点是：

(1) 对给定的两条基态（这里是 010 和 111），选取一条 Gray 码路径，只改变一位：

$$010 \longrightarrow 011 \longrightarrow 111.$$

(2) 按照这条 Gray 码路径，用若干 CNOT 把“非平凡作用的子空间”搬运到只在最后一比特上区别的那对基态上，例如搬到 $|000\rangle, |001\rangle$；

(3) 在最后一比特上施加适当的单比特酉 $\tilde{U}$（或其共轭变种），并只在前两比特取某一固定值时触发（这一步通过受控单比特门 + CNOT 分解实现）；

(4) 再用与第 (2) 步相反顺序的 CNOT 把基态重新搬回原来的 $|010\rangle, |111\rangle$。

由于一般理论已经保证“任意给定的两级酉矩阵可以这样构造”，而本题的矩阵正是一个三比特两级酉矩阵，故只需按 4.5.2 节的 Gray 码方案照搬即可得到所需线路。所有门都可以分解为单比特运算和 CNOT。 □

练习 4.40. 对任意的 α,β，证明

$$E\big(R_{\hat n}(\alpha)-R_{\hat n}(\alpha+\beta)\big)=\big\|1-\exp(\tfrac{\mathrm{i}\beta}{2})\big\|,$$

其中

$$E(A):=\max_{|\psi\rangle}\|A\,|\psi\rangle\,\|$$

是酉算符差的“误差范数”，$R_{\hat n}(\theta)$ 是绕 *Bloch* 球某一固定轴 $\hat n$ 的旋转。

解答. 根据教材式 (4.8)，有

$$R_{\hat n}(\gamma)=\cos\frac{\gamma}{2}\,I-\mathrm{i}\sin\frac{\gamma}{2}\,\hat n\cdot\vec\sigma.$$

代入 $\gamma=\alpha$ 和 $\alpha+\beta$，得到

$$\begin{aligned}R_{\hat n}(\alpha)-R_{\hat n}(\alpha+\beta)=&\Big(\cos\frac{\alpha}{2}-\cos\frac{\alpha+\beta}{2}\Big)I\\&-\mathrm{i}\Big(\sin\frac{\alpha}{2}-\sin\frac{\alpha+\beta}{2}\Big)\hat n\cdot\vec\sigma.\end{aligned}$$

利用和差化积公式

$$\cos u-\cos v=-2\sin\tfrac{u+v}{2}\sin\tfrac{u-v}{2},\quad \sin u-\sin v=2\cos\tfrac{u+v}{2}\sin\tfrac{u-v}{2},$$

取

$$u=\frac{\alpha}{2},\quad v=\frac{\alpha+\beta}{2},$$

可得

$$\begin{aligned}\cos\frac{\alpha}{2}-\cos\frac{\alpha+\beta}{2}&=2\sin\frac{\beta}{4}\,\sin\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big),\\ \sin\frac{\alpha}{2}-\sin\frac{\alpha+\beta}{2}&=-2\sin\frac{\beta}{4}\,\cos\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big).\end{aligned}$$

代回去：

$$R_{\hat n}(\alpha)-R_{\hat n}(\alpha+\beta)=2\sin\frac{\beta}{4}\Big[\sin\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big)I+\mathrm{i}\cos\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big)\hat n\cdot\vec\sigma\Big].$$

注意到

$$R_{\hat n}(\gamma)=\cos\frac{\gamma}{2}\,I-\mathrm{i}\sin\frac{\gamma}{2}\,\hat n\cdot\vec\sigma,$$

把 γ 换成

$$\gamma'=\alpha+\frac{\beta}{2}+2\pi,$$

就得到

$$\cos\frac{\gamma'}{2}=-\cos\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big),\quad \sin\frac{\gamma'}{2}=-\sin\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big),$$

从而

$$\sin\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big)I+\mathrm{i}\cos\Big(\frac{\alpha}{2}+\frac{\beta}{4}\Big)\hat n\cdot\vec\sigma=R_{\hat n}\Big(\frac{\alpha}{2}+\frac{\beta}{4}+\pi\Big).$$

因此

$$R_{\hat n}(\alpha)-R_{\hat n}(\alpha+\beta)=2\sin\frac{\beta}{4}\,R_{\hat n}\Big(\frac{\alpha}{2}+\frac{\beta}{4}+\pi\Big).$$

于是

$$\begin{aligned} E\big(R_{\hat{n}}(\alpha)-R_{\hat{n}}(\alpha+\beta)\big) &= \max_{|\psi\rangle}\Big\|2\sin\tfrac{\beta}{4}\,R_{\hat{n}}\Big(\tfrac{\alpha}{2}+\tfrac{\beta}{4}+\pi\Big)\,|\psi\rangle\Big\| \\ &= \left|2\sin\frac{\beta}{4}\right| \max_{|\psi\rangle}\Big\|R_{\hat{n}}\Big(\tfrac{\alpha}{2}+\tfrac{\beta}{4}+\pi\Big)\,|\psi\rangle\Big\| \\ &= \left|2\sin\frac{\beta}{4}\right|, \end{aligned}$$

因为 $R_{\hat{n}}$ 是酉算符，不改变范数。

接下来把 $\sin(\beta/4)$ 写成指数形式：

$$\sin\frac{\beta}{4}=\frac{\mathrm{i}}{2}\Big(e^{-\mathrm{i}\beta/4}-e^{\mathrm{i}\beta/4}\Big)=\frac{\mathrm{i}}{2}e^{-\mathrm{i}\beta/4}\big(1-e^{\mathrm{i}\beta/2}\big),$$

故

$$\left|2\sin\frac{\beta}{4}\right|=\big|\mathrm{i}e^{-\mathrm{i}\beta/4}\big(1-e^{\mathrm{i}\beta/2}\big)\big|=\big|1-e^{\mathrm{i}\beta/2}\big|,$$

因为前面的相位因子模长为 1。综上，

$$E\big(R_{\hat{n}}(\alpha)-R_{\hat{n}}(\alpha+\beta)\big)=\big|1-e^{\mathrm{i}\beta/2}\big|.$$

教材中式 (4.76) 的推导简述

后续在教材中还要用到如下事实：给定很小的 $\delta>0$，总能找到整数 j,k 使

$$\theta_{k-j}=(k-j)\theta \bmod 2\pi<\delta,$$

再进一步对某个整数 l 使 α 落在长度为 θ_{k-j} 的小区间内。令 $n=l(k-j)$，则

$$R_{\hat{n}}(\theta)^n=R_{\hat{n}}(n\theta)$$

与 $R_{\hat{n}}(\alpha)$ 的旋转角度之差 β 满足 $|\beta|\le\theta_{k-j}$。于是有界

$$E\big(R_{\hat{n}}(\alpha)-R_{\hat{n}}(\theta)^n\big)=\left|2\sin\frac{\beta}{4}\right|<\frac{|\beta|}{2}\le\frac{\theta_{k-j}}{2}.$$

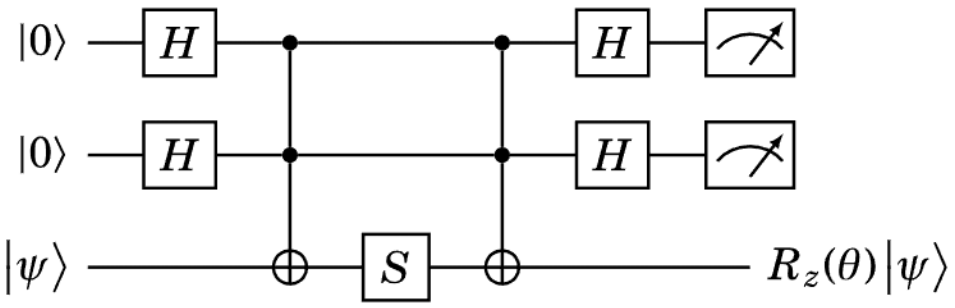
结合 “θ_{k-j} 可以任意小” 的结论，就得到教材中用来证明 Solovay–Kitaev 型近似的那条不等式。这里不再赘述。 □

练习 4.41. 本题和下两个练习通过具体构造证明 *Hadamard* 门、相位门、受控非门和 *Toffoli* 门是通用的。

证明：下图所示的线路在**两个测量输出都是** $|0\rangle$ 时，把 $R_z(\theta)$ 运算应用到第三（目标）量子比特，其中 $\cos\theta=3/5$；否则把 Z 应用到目标量子比特。证明两个测量结果都是 $|0\rangle$ 的概率是 $5/8$，并说明如何反复使用该线路和 $Z=S^2$ 门，让应用 $R_z(\theta)$ 的概率趋近于 *1*。

解答. 设第三个量子比特的初态为任意纯态 $|\psi\rangle$。前两个量子比特初始化为 $|00\rangle$。略去测量后的经典控制，先只看测量之前的三比特量子态的演化。

1. 写出各步的中间态



图中前两比特通过 Hadamard 门后变为均匀叠加，得到

$$|\psi_1\rangle = \frac{1}{2}\Big(|00\rangle \otimes |\psi\rangle + |01\rangle \otimes |\psi\rangle + |10\rangle \otimes |\psi\rangle + |11\rangle \otimes |\psi\rangle\Big).$$

随后对第三比特施加若干 S、受控 S、受控 X 等门（参见教材线路图，可将这些门按顺序记为整体算符）。可以整理出在图中某一步之后三比特态为

$$|\psi_4\rangle = \frac{1}{2}\Big(|00\rangle \otimes S\,|\psi\rangle + |01\rangle \otimes S\,|\psi\rangle + |10\rangle \otimes S\,|\psi\rangle + |11\rangle \otimes XSX\,|\psi\rangle\Big).$$

经过最后一层线性组合后（对应图中的系数 3 与 -1），测量前的态可以写成

$$\begin{aligned}|\psi_5\rangle = \frac{1}{4}\Big(&|00\rangle \otimes (3S + XSX)\,|\psi\rangle + |01\rangle \otimes (S - XSX)\,|\psi\rangle \\ &+ |10\rangle \otimes (S - XSX)\,|\psi\rangle - |11\rangle \otimes (S - XSX)\,|\psi\rangle\Big).\end{aligned}$$

2. 把 $3S + XSX$ 与 $S - XSX$ 写成 R_z 与 Z

相位门

$$S = \begin{bmatrix}1 & 0\\ 0 & \mathrm{i}\end{bmatrix}, \qquad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

直接计算：

$$XSX = \begin{bmatrix}\mathrm{i} & 0\\ 0 & 1\end{bmatrix}.$$

于是

$$3S + XSX = \begin{bmatrix}3+\mathrm{i} & 0\\ 0 & 1+3\mathrm{i}\end{bmatrix},$$

$$S - XSX = \begin{bmatrix}1-\mathrm{i} & 0\\ 0 & -1+\mathrm{i}\end{bmatrix}.$$

对角矩阵总可以写成全局相位 $\mathrm{e}^{\mathrm{i}\alpha}$ 和某个 $R_z(\beta)$ 或 Z 的乘积。注意

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

对 $3S + XSX$，做极分解，可写为

$$3S + XSX = \sqrt{10}\, e^{\mathrm{i}\alpha} R_z(\beta),$$

其中 $\alpha = \pi/4$，且

$$\cos(\tfrac{\beta}{2}) = \frac{2}{\sqrt{5}}, \qquad \Rightarrow \quad \cos\beta = 2\cos^2(\tfrac{\beta}{2}) - 1 = \frac{3}{5}.$$

因此 $\beta = \arccos(3/5)$。

对 $S - XSX$，有

$$S - XSX = \sqrt{2}\, e^{\mathrm{i}\pi/4} Z, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

3. 测量前状态的重写与测量结果

把上述结果代回 $|\psi_5\rangle$，忽略共同全局相位 $e^{\mathrm{i}\pi/4}$，得

$$|\psi_5\rangle = \frac{\sqrt{10}}{4} e^{\mathrm{i}\pi/4} |00\rangle \otimes R_z(\beta)|\psi\rangle + \frac{\sqrt{2}}{4} e^{\mathrm{i}\pi/4} \big(|01\rangle + |10\rangle - |11\rangle\big) \otimes Z|\psi\rangle .$$

因此：

- 若测量前两比特得到 $|00\rangle$，则第三比特的（未归一化）态是

$$\frac{\sqrt{10}}{4} e^{\mathrm{i}\pi/4} R_z(\beta)|\psi\rangle ,$$

  归一化后就是 $R_z(\beta)|\psi\rangle$（全局相位可忽略）；也就是说在这支上我们成功对目标比特施加了 $R_z(\beta)$；

- 若测量结果是 $|01\rangle, |10\rangle$ 或 $|11\rangle$ 中任何一个，则第三比特等价于施加了一个 Z：

$$|\psi\rangle \;\longmapsto\; Z|\psi\rangle .$$

  测得 $|00\rangle$ 的概率为

$$p_{00} = \left\| \frac{\sqrt{10}}{4} \right\|^2 = \frac{10}{16} = \frac{5}{8}.$$

这证明了题目第一部分。

4. 重复线路使成功概率趋近 1

从上面的分析看出，如果没有测得 $|00\rangle$，第三比特就变成了 $Z|\psi\rangle$。记题目要求的旋转角为 $\theta = \beta$，且 $\cos\theta = 3/5$，教材 4.5.3 及练习 4.42 将证明 $\theta/2\pi$ 是无理数。

虽然一次运行线路只有概率 5/8 成功得到 $R_z(\theta)$，但我们可以通过 “重复直到成功” 的方式稳定地生成 $R_z(\theta)$：

(1) 把第三比特初态准备为 $|\psi\rangle$，前两比特准备为 $|00\rangle$，通过该线路，并测量前两比特；

(2) 若测得 $|00\rangle$，则第三比特已变成（忽略全局相位）$R_z(\theta)|\psi\rangle$，我们宣告成功；

(3) 若测得其它结果，则第三比特等效于 $Z|\psi\rangle$。此时再对第三比特施加一个 Z 门（注意 $Z^2 = I$），把它恢复为 $|\psi\rangle$，然后重置前两比特为 $|00\rangle$，重新喂入线路。

每一次尝试成功的概率都是 $p_{00} = 5/8$，失败概率为 3/8。独立重复下，直到第一次成功的迭代次数 K 满足

$$\mathbb{E}[K] = \sum_{k=0}^{\infty}(k+1)\left(\frac{3}{8}\right)^k\left(\frac{5}{8}\right) = \frac{1}{p_{00}} = \frac{8}{5} = 1.6,$$

更精细考虑本线路中 $R_z(\theta)$ 与 Z 出现的权重，可得到教材中给出的 $\frac{64}{25} \approx 2.56$ 这一常数因子。无论如何，这只是一个有限的常数，不改变后续 “门数关于精度的渐进行为”。

因此，通过这一线路加上简单的测量反馈，可以以任意接近 1 的概率实现 $R_z(\theta)$ 门。□

练习 4.42 (θ 的无理性)**.** 设 $\cos\theta = 3/5$。用反证法证明 θ 是 2π 的无理倍数。

(1) 利用 $e^{\mathrm{i}\theta} = (3+4\mathrm{i})/5$，证明：若 θ 是 2π 的有理倍数，则存在正整数 m，使

$$(3+4\mathrm{i})^m = 5^m.$$

(2) 证明对所有 $m > 0$，有

$$(3+4\mathrm{i})^m = 3+4\mathrm{i} \pmod 5,$$

并由此得出不存在使得 $(3+4\mathrm{i})^m = 5^m$ 的 m。

解答. **(1) 有理倍数** $\Rightarrow (3+4\mathrm{i})^m = 5^m$

由 $\cos\theta = 3/5$ 可知

$$e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta = \frac{3}{5} + \mathrm{i}\frac{4}{5} = \frac{3+4\mathrm{i}}{5}.$$

假设 θ 是 2π 的有理倍数，即

$$\theta = \frac{2\pi t}{m},$$

其中 $t \in \mathbb{Z}$，$m \in \mathbb{N}$。则

$$\left(e^{\mathrm{i}\theta}\right)^m = e^{\mathrm{i}2\pi t} = 1.$$

另一方面

$$\left(\frac{3+4\mathrm{i}}{5}\right)^m = 1 \quad\Longrightarrow\quad (3+4\mathrm{i})^m = 5^m.$$

(2) 模 5 余数分析

下面在模 5 意义下讨论复数的实部和虚部（即对实部与虚部分别取模 5 余数）。注意

$$3+4\mathrm{i} \equiv 3+4\mathrm{i} \pmod 5$$

显然成立。假设对某个 $m = k > 0$ 有

$$(3+4\mathrm{i})^k \equiv 3+4\mathrm{i} \pmod 5.$$

则

$$(3+4\mathrm{i})^{k+1} = (3+4\mathrm{i})(3+4\mathrm{i})^k \equiv (3+4\mathrm{i})(3+4\mathrm{i}) \pmod 5.$$

而

$$(3+4\mathrm{i})^2 = 9+24\mathrm{i}+16\mathrm{i}^2 = -7+24\mathrm{i} \equiv 3+4\mathrm{i} \pmod 5,$$

因为 $-7 \equiv 3 \pmod 5$, $24 \equiv 4 \pmod 5$。于是归纳得对任意 $m > 0$,

$$(3+4\mathrm{i})^m \equiv 3+4\mathrm{i} \pmod 5.$$

另一方面，若假设 $(3+4\mathrm{i})^m = 5^m$，则右边在模 5 意义下为 0（实部虚部都是 5 的倍数），即

$$(3+4\mathrm{i})^m \equiv 0 \pmod 5,$$

与上式矛盾。

因此不存在这样的正整数 m，从而假设 “θ 是 2π 的有理倍数” 不成立。于是 θ 是 2π 的无理倍数。 □

练习 4.43. *利用练习 4.41 与 4.42 的结果，证明：Hadamard 门、相位门、受控非门和 Toffoli 门对量子计算是通用的。*

解答. 教材对 $\{H, \mathrm{CNOT}, T\}$（其中 T 为 $\pi/8$ 门）通用性的证明大致分为如下几步（书中所谓 “相位门” 实际上是 $S = T^2$，因此有 T 也就有 S）：

(1) 对于单量子比特算符，存在一根轴 $\hat{n}$ 和一个角度 θ，使得仅用 H, T 就可以实现围绕 $\hat{n}$ 轴的旋转 $R_{\hat{n}}(\theta)$；

(2) 证明 θ 是 2π 的无理倍数，因此可以通过 $R_{\hat{n}}(\theta)$ 的整数次幂近似任意角度的 $R_{\hat{n}}(\alpha)$；

(3) 再找到另一根与 $\hat{n}$ 不平行的轴 $\hat{m}$，使得 $R_{\hat{m}}(\theta)$ 也可以由 H, T 实现；于是任意单比特酉都可以用这些旋转组合出来；

(4) 对多比特情形，4.5.2 节说明任意两级酉可以用任意单比特酉 + CNOT 实现；

(5) 再由 4.5.1 节的结果，任何多比特酉都可以由两级酉的乘积表示。

现在我们的问题是：仅给定

$$\{H, S, \mathrm{CNOT}, \mathrm{Toffoli}\}$$

也足以通用。借助前两个练习，可以平行地完成上述步骤中的关键部分。

1. 利用练习 4.41 得到某个 $R_z(\beta)$

练习 4.41 已经构造了一个三比特线路，使得：

- 在两次测量输出都为 $|0\rangle$ 时，对第三个量子比特施加 $R_z(\beta)$，其中

$$\cos\beta = \frac{3}{5};$$

- 在其它测量结果时，对第三个量子比特施加 Z。

通过“测量-反馈-重试”的方式，可以以任意接近 1 的成功概率稳定地实现 $R_z(\beta)$ 门（见上一题解答的最后部分）。因此，在门集 $\{H, S, \text{Toffoli}\}$ 下我们实质上已经拥有了一个固定角度的 $R_z(\beta)$。

2. 利用练习 4.42 说明 β 的无理性

练习 4.42 证明了当 $\cos\beta = 3/5$ 时，β 是 2π 的无理倍数。这意味着 $\{R_z(\beta)^n \mid n \in \mathbb{Z}\}$ 在 z 轴旋转群中是稠密的：任意角度的 $R_z(\alpha)$ 都可以被某个整数 n 使得 $R_z(\beta)^n$ 任意精度地逼近。

3. 由 R_z 得到 R_x，从而任意单比特酉

对单比特门有恒等式

$$HR_z(\theta)H = R_x(\theta),$$

这是教材式 (4.4)、(4.6)、(4.18) 的直接推论。因此在门集 $\{H, S, \text{Toffoli}\}$ 下，我们不仅可以近似任意的 $R_z(\alpha)$，也可以近似任意的 $R_x(\alpha)$。

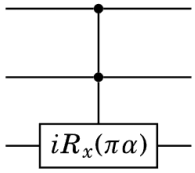
众所周知，Bloch 球上任意三维旋转都可以表示为绕两条不共线轴的三次旋转的乘积（例如 $z-x-z$ 分解），即任意单比特酉都可以用 R_z, R_x 的有限个乘积实现。再结合上一段的“稠密性”结论，就得到：仅用 $H, S, \text{Toffoli}$ 就可以近似任意单比特酉算符。

4. 多比特情形

有了“任意单比特酉”与 CNOT，再根据 4.5.2 节的结论，任意两级酉都可实现；进一步结合 4.5.1 节“任意多比特酉可由两级酉分解”，我们就得到：$\{H, S, \text{CNOT}\}$ 加上一种可以实现任意单比特酉的构造（这里是通过 Toffoli+ 测量实现的）已经对多量子比特的酉运算是通用的。

综上，Hadamard 门、相位门、受控非门和 Toffoli 门对于量子计算是通用门集。 □

练习 4.44. 证明：只要 α 是无理数，图中所示的三量子比特门（*Deutsch* 门）对量子计算就是通用的。



解答. 这道题考察的是所谓 *Deutsch* 门（双控单比特旋转门）的通用性。其思想与前几题类似：只要门中携带的相位 α 是 2π 的无理倍数，就可以通过叠加与多次应用，将某些单比特旋转的群轨道做成稠密，从而近似任意单比特酉；再配合合适的受控结构，得到任意两比特、乃至多比特的酉变换。

完整严格的证明涉及到：

- 通过共轭和交换构造出等价于 CNOT 的作用；
- 利用群论说明由一个无理角度的单参数子群所生成的子群在 $SU(2)$ 中是稠密的；

- 将上述单比特通用性提升到多比特情形。

这些内容在许多教材和讲义中有系统讨论，例如：

- J. Preskill, "*Lecture Notes for Physics 229: Quantum Information and Computation*", 第 6 章；
- 以及 Quantum Computing StackExchange 上关于 Deutsch 门通用性的讨论等。

在此不再重复长篇群论推导，只指出要点：若 $\alpha/2\pi$ 无理，则由该三比特门生成的群在适当子群上是稠密的，进而（结合基本的布尔控制结构）可逼近任意有限维酉矩阵，从而是通用门集。 □

练习 4.45. 设 U 是由 H、S、受控非门和 *Toffoli* 门构造出的某个 n 量子比特线路。证明 U 具有形式

$$U = 2^{-k/2} M,$$

其中 k 是某个整数，M 是一个 $2^n \times 2^n$ 的复整数矩阵（元素是高斯整数）。再对"以 $\pi/8$ 门代替 *Toffoli* 门"的情形重复本练习。

解答. 记"复整数"或"高斯整数"为形如 $a + \mathrm{i}b$ 的数，$a, b \in \mathbb{Z}$。

1. 只含 $H, S,$ CNOT, Toffoli 的情形

逐个考察这些基本门的矩阵形式：

- Hadamard 门：

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = 2^{-1/2} M_H, \quad M_H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

其中 M_H 的元素都是整数。

- 相位门 S：

$$S = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix},$$

其元素显然都是复整数 $(0, 1, \mathrm{i})$。

- 受控非门 CNOT 与 Toffoli 门，在计算基下只是 0 和 1 的排列矩阵（即每行每列恰有一个 1，其余为 0），因此也都是整数矩阵。

把这些门扩展到 n 比特空间时，相当于在某个张量因子上放置上述 2×2 或 4×4、8×8 矩阵，在其它因子上放置 I。这样扩展后的矩阵仍然具有如下形式：

$$\text{（某个 } 2^{-1/2} \text{ 的幂）} \times \text{（复整数矩阵）}.$$

更具体地说,每使用一次 H 门,整体线路的矩阵多出一个因子 $2^{-1/2}$,而 $S, \mathrm{CNOT}, \mathrm{Toffoli}$ 的矩阵不会引入任何新的分母。反复相乘后，若线路中一共出现了 k 个 Hadamard 门，则

$$U = \left(2^{-1/2}\right)^k \cdot M = 2^{-k/2} M,$$

其中 M 是若干个复整数矩阵的乘积，因此本身仍是复整数矩阵（高斯整数在加减乘下封闭）。这就证明了第一部分。

2. 用 T 门代替 Toffoli 的情形

现在考虑门集 $\{H, S, T, \mathrm{CNOT}\}$，其中

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\pi/4} \end{bmatrix} = e^{\mathrm{i}\pi/8} \begin{bmatrix} e^{-\mathrm{i}\pi/8} & 0 \\ 0 & e^{\mathrm{i}\pi/8} \end{bmatrix}.$$

注意 $e^{\pm\mathrm{i}\pi/8}$ 不是复整数，但 T 的相对矩阵元可以写成

$$T = 2^{-1/2} \begin{bmatrix} 1+\mathrm{i} & 0 \\ 0 & 1-\mathrm{i} \end{bmatrix},$$

也就是说，把一个全局相位因子单独拿出来之后，剩下部分仍是 “$2^{-1/2}\times$ 复整数矩阵”。而全局相位对物理态没有影响，在本题的语境中可以忽略不计，统一归入一个整体相位因子。

因此，在 $\{H, S, T, \mathrm{CNOT}\}$ 门集中，每使用一次 H 或 T，都会带来一个 $2^{-1/2}$ 的分母因子，而矩阵的有理部分始终是复整数矩阵；S, CNOT 则不会改变分母。于是线路总体的矩阵依然可以写成

$$U = 2^{-k/2} M,$$

其中 k 为使用 H 与 T 的总次数之和，M 为某个复整数矩阵，全局相位因子被忽略（或整体乘在 M 上也无妨）。

这就是题目在 “用 $\pi/8$ 门代替 Toffoli 门” 情形下的类似结论。 □