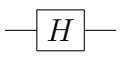
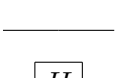
4.3 受控运算——习题与详细解答

DanX, Yuchen He*

练习 4.16 (多量子比特门的矩阵表示). 在计算基下，给出两条线路的 4×4 酉矩阵：一是对第 *1* 比特施加 H；二是对第 *2* 比特施加 H。

解答.　线路图示：

(1) $H\otimes I$:　 

(2) $I\otimes H$:　 

先固定**计算基**的顺序为

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle.$$

单比特 Hadamard 门矩阵是

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\qquad I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

(1) 对第 1 比特施加 H：

这相当于算符 $H\otimes I$。我们可以用“**看它对基态的作用**”的方法来得到矩阵的每一列。记

$$|00\rangle=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\ |01\rangle=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\ |10\rangle=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\ |11\rangle=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

因为 H 只作用在第 1 比特上，我们有：

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

逐个作用：

- 对 $|00\rangle=|0\rangle\otimes|0\rangle$：

$$(H\otimes I)|00\rangle=(H|0\rangle)\otimes|0\rangle=\frac{1}{\sqrt{2}}\big(|0\rangle\otimes|0\rangle+|1\rangle\otimes|0\rangle\big)=\frac{1}{\sqrt{2}}\big(|00\rangle+|10\rangle\big).$$

*heyuchen@tgqs.net

所以矩阵的第 1 列是

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix}.$$

- 对 $|01\rangle = |0\rangle \otimes |1\rangle$：

$$(H \otimes I)\,|01\rangle = (H\,|0\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle\big) = \frac{1}{\sqrt{2}}\big(|01\rangle + |11\rangle\big),$$

所以第 2 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}.$$

- 对 $|10\rangle = |1\rangle \otimes |0\rangle$：

$$(H \otimes I)\,|10\rangle = (H\,|1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |0\rangle - |1\rangle \otimes |0\rangle\big) = \frac{1}{\sqrt{2}}\big(|00\rangle - |10\rangle\big),$$

所以第 3 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\-1\\0\end{pmatrix}.$$

- 对 $|11\rangle = |1\rangle \otimes |1\rangle$：

$$(H \otimes I)\,|11\rangle = (H\,|1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |1\rangle - |1\rangle \otimes |1\rangle\big) = \frac{1}{\sqrt{2}}\big(|01\rangle - |11\rangle\big),$$

所以第 4 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\-1\end{pmatrix}.$$

按列拼到一起，得到

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{pmatrix}.$$

(2) 对第 2 比特施加 H：

现在算符是 $I \otimes H$。同样逐个基态来算：

- 对 $|00\rangle = |0\rangle \otimes |0\rangle$：

$$(I \otimes H)\,|00\rangle = |0\rangle \otimes (H\,|0\rangle) = \frac{1}{\sqrt{2}}\big(|00\rangle + |01\rangle\big),$$

所以第 1 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}.$$

- 对 $|01\rangle = |0\rangle \otimes |1\rangle$：

$$(I \otimes H)\,|01\rangle = |0\rangle \otimes (H\,|1\rangle) = \frac{1}{\sqrt{2}}\big(|00\rangle - |01\rangle\big),$$

第 2 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\\0\\0\end{pmatrix}.$$

- 对 $|10\rangle = |1\rangle \otimes |0\rangle$：

$$(I \otimes H)\,|10\rangle = |1\rangle \otimes (H\,|0\rangle) = \frac{1}{\sqrt{2}}\big(|10\rangle + |11\rangle\big),$$

第 3 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\1\end{pmatrix}.$$

- 对 $|11\rangle = |1\rangle \otimes |1\rangle$：

$$(I \otimes H)\,|11\rangle = |1\rangle \otimes (H\,|1\rangle) = \frac{1}{\sqrt{2}}\big(|10\rangle - |11\rangle\big),$$

第 4 列为

$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}.$$

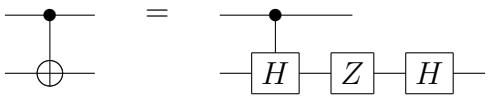
拼成矩阵：

$$I \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\1 & -1 & 0 & 0\\0 & 0 & 1 & 1\\0 & 0 & 1 & -1\end{pmatrix}.$$

这就是题目要求的两个 4×4 酉矩阵。 □

练习 4.17 (由受控 Z 门构造 CNOT)**.** 已知受控 Z 的矩阵 ctrl-$Z = \mathrm{diag}(1,1,1,-1)$。用两个 *Hadamard* 门构造 *CNOT*，并说明控制与目标。

解答.　线路等价性：



我们记受控 Z 为 CZ。在基

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

下，

$$\mathrm{CZ} = \mathrm{diag}(1,1,1,-1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

1. 把 CZ 写成投影形式

记

$$P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

计算

$$P_0 \otimes I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad P_1 \otimes Z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

相加得到

$$P_0 \otimes I + P_1 \otimes Z = \mathrm{diag}(1,1,1,-1) = \mathrm{CZ}.$$

所以

$$\mathrm{CZ} = P_0 \otimes I + P_1 \otimes Z.$$

2. 在第二个比特上夹 Hadamard 门

我们要计算

$$U := (I \otimes H)\,\mathrm{CZ}\,(I \otimes H).$$

先注意两个恒等式（可直接由矩阵相乘验证）：

$$HIH = I, \qquad HZH = X.$$

利用线性展开：

$$\begin{aligned} U &= (I \otimes H)\big[P_0 \otimes I + P_1 \otimes Z\big](I \otimes H) \\ &= P_0 \otimes (HIH) + P_1 \otimes (HZH) \\ &= P_0 \otimes I + P_1 \otimes X. \end{aligned}$$

3. 识别这是 CNOT（第 1 控，第 2 目标）

算符

$$\mathrm{CNOT}_{1\to 2} := P_0 \otimes I + P_1 \otimes X$$

的含义是：

- 当第 1 比特处于 $|0\rangle$（被 P_0 投影）时，对第 2 比特不做任何事；- 当第 1 比特处于 $|1\rangle$（被 P_1 投影）时，对第 2 比特施加 X（翻转）。

也就是说，这是“第 1 比特为控制、第 2 比特为目标”的 CNOT 门。

因此我们得出

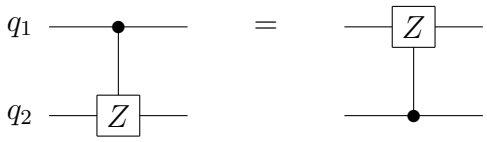
$$(I \otimes H)\,\mathrm{CZ}\,(I \otimes H) = \mathrm{CNOT}_{1\to 2}.$$

这就是所求构造，并且控制比特是第 1 比特，目标比特是第 2 比特。 □

练习 4.18. 证明 $P_0 \otimes I + P_1 \otimes Z = I \otimes P_0 + Z \otimes P_1$。

解答. **量子线路图示：**

此恒等式的物理本质是受控 Z 门（CZ）的对称性。左边对应“第 1 控第 2”，右边对应“第 2 控第 1”。它们的线路效果完全相同：



代数推导：

这里我们用显式矩阵来算一遍，让等式非常直观。

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

先算左边：

$$P_0 \otimes I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad P_1 \otimes Z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

相加：

$$P_0 \otimes I + P_1 \otimes Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \mathrm{diag}(1,1,1,-1).$$

再算右边：

$$I \otimes P_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z \otimes P_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

(注：$Z \otimes P_1$ 的矩阵由 $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ 算出。)

相加显然也得到同样的对角矩阵 $\mathrm{diag}(1,1,1,-1)$。

物理意义： 左边的算符表示 “当第 1 比特为 $|1\rangle$ 时，对第 2 比特施加 Z”；右边的算符表示 “当第 2 比特为 $|1\rangle$ 时，对第 1 比特施加 Z”。由于 Z 门本质上只是给 $|1\rangle$ 态施加 -1 相位，因此两种操作的效果都是：当且仅当两个比特都为 $|1\rangle$ 时（即态为 $|11\rangle$），系统获得 -1 的全局相位。这说明 CZ 门对控制和目标是对称的。 □

练习 4.19 (CNOT 在密度矩阵上的作用)**.** *说明 CNOT_{x_1,x_2} 对任意 4×4 矩阵 A 的共轭作用 $\mathrm{CNOT}\, A\, \mathrm{CNOT}$ 只是对第 3、4 行与第 3、4 列的同时置换。*

解答. 我们把

$$C := \mathrm{CNOT}_{1\to 2}$$

写成显式矩阵。在基

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

下，CNOT 的作用是：

$$|00\rangle \mapsto |00\rangle,\ |01\rangle \mapsto |01\rangle,\ |10\rangle \mapsto |11\rangle,\ |11\rangle \mapsto |10\rangle.$$

因此 C 是一个**置换矩阵**：

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

1. 左乘 C：行置换

设

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}.$$

计算

$$CA = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} A = \begin{pmatrix} \text{第 1 行} \\ \text{第 2 行} \\ \text{第 4 行} \\ \text{第 3 行} \end{pmatrix}.$$

矩阵乘法规则是 “行乘列”，C 的前两行是单位矩阵的前两行，保持 A 的前两行不变；C 的第三行是 $(0,0,0,1)$，挑出 A 的第四行；C 的第四行是 $(0,0,1,0)$，挑出 A 的第三行。

也就是说，**左乘 C 把第 3、4 行交换了**。

2. 右乘 C：列置换

再算

$$A'C = (CA)C.$$

我们已经知道 CA 只是第 3、4 行和原来的对调而已。

现在计算 $(CA)C$，右乘置换矩阵 C 的效果是对列进行同样的置换：

- 第一列和第二列保持不变；- 第三列和第四列交换。

因此

$$(CA)C = \Big(\text{第 1 列} \quad \text{第 2 列} \quad \text{第 4 列} \quad \text{第 3 列}\Big)$$

（这里的 “第几列” 是指 CA 的列）。

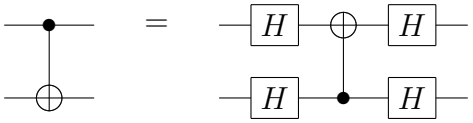
总结起来，对任意 4×4 矩阵 A，

$$CAC$$

的效果就是：**交换第 3、4 行，然后交换第 3、4 列**，其他行列都保持不变。也就是题目中说的：共轭作用只是把第 3、4 行与第 3、4 列做了同一个置换。 □

练习 4.20 (CNOT 的基变换). 在 $\{|\pm\rangle\}$ 基下证明 $(H\otimes H)\,\mathrm{CNOT}_{x_1,x_2}\,(H\otimes H) = \mathrm{CNOT}_{x_2,x_1}$，并由此得到 $|\pm\rangle\,|\pm\rangle$ 的四种映射关系（目标不变、控制在目标为 $|-\rangle$ 时翻转）。

解答. **线路等价性：**



先回顾

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Hadamard 门满足

$$H\,|0\rangle = |+\rangle\,, \quad H\,|1\rangle = |-\rangle\,, \quad H\,|+\rangle = |0\rangle\,, \quad H\,|-\rangle = |1\rangle\,, \quad H^2 = I.$$

1. 在 $|\pm\rangle$ 基下逐个计算 $(H\otimes H)\,\mathrm{CNOT}\,(H\otimes H)$ 的作用

记

$$U := (H\otimes H)\,\mathrm{CNOT}_{1\to 2}\,(H\otimes H).$$

我们对四个输入态 $\{|+\rangle|+\rangle, |+\rangle|-\rangle, |-\rangle|+\rangle, |-\rangle|-\rangle\}$ 分别计算 U 的输出。

(1) 输入 $|+\rangle|+\rangle$：

$$(H\otimes H)|+\rangle|+\rangle = H|+\rangle\otimes H|+\rangle = |0\rangle\otimes|0\rangle = |00\rangle.$$

CNOT 的作用：

$$\mathrm{CNOT}_{1\to 2}|00\rangle = |00\rangle.$$

再乘上 $H\otimes H$：

$$(H\otimes H)|00\rangle = H|0\rangle\otimes H|0\rangle = |+\rangle|+\rangle.$$

所以

$$U|+\rangle|+\rangle = |+\rangle|+\rangle.$$

(2) 输入 $|+\rangle|-\rangle$：

$$(H\otimes H)|+\rangle|-\rangle = H|+\rangle\otimes H|-\rangle = |0\rangle\otimes|1\rangle = |01\rangle.$$

CNOT：

$$\mathrm{CNOT}_{1\to 2}|01\rangle = |01\rangle.$$

再乘 $H\otimes H$：

$$(H\otimes H)|01\rangle = H|0\rangle\otimes H|1\rangle = |+\rangle|-\rangle.$$

所以

$$U|+\rangle|-\rangle = |+\rangle|-\rangle.$$

(3) 输入 $|-\rangle|+\rangle$：

$$(H\otimes H)|-\rangle|+\rangle = H|-\rangle\otimes H|+\rangle = |1\rangle\otimes|0\rangle = |10\rangle.$$

CNOT：

$$\mathrm{CNOT}_{1\to 2}|10\rangle = |11\rangle.$$

再乘 $H\otimes H$：

$$(H\otimes H)|11\rangle = H|1\rangle\otimes H|1\rangle = |-\rangle|-\rangle.$$

所以

$$U|-\rangle|+\rangle = |-\rangle|-\rangle.$$

(4) 输入 $|-\rangle|-\rangle$：

$$(H\otimes H)|-\rangle|-\rangle = H|-\rangle\otimes H|-\rangle = |1\rangle\otimes|1\rangle = |11\rangle.$$

CNOT：

$$\mathrm{CNOT}_{1\to 2}|11\rangle = |10\rangle.$$

再乘 $H \otimes H$：

$$(H \otimes H)\,|10\rangle = H\,|1\rangle \otimes H\,|0\rangle = |-\rangle\,|+\rangle\,.$$

所以

$$U\,|-\rangle\,|-\rangle = |-\rangle\,|+\rangle\,.$$

2. 总结四种映射关系

把结果整理一下：

$$\begin{aligned}
|+\rangle\,|+\rangle &\xrightarrow{U} |+\rangle\,|+\rangle\,,\\
|+\rangle\,|-\rangle &\xrightarrow{U} |+\rangle\,|-\rangle\,,\\
|-\rangle\,|+\rangle &\xrightarrow{U} |-\rangle\,|-\rangle\,,\\
|-\rangle\,|-\rangle &\xrightarrow{U} |-\rangle\,|+\rangle\,.
\end{aligned}$$

从这四条可以看出：

- 第一比特 ($|+\rangle$ 或 $|-\rangle$) 始终不变；- 第二比特在第一比特为 $|-\rangle$ 时发生 $|+\rangle \leftrightarrow |-\rangle$ 的翻转，在第一比特为 $|+\rangle$ 时保持不变。

换句话说：在 $\{|+\rangle, |-\rangle\}$ 基下，U 正好是“第 1 比特为控制、第 2 比特为目标”的 CNOT，只不过“控制条件”从 $|1\rangle$ 变成了「处于 $|-\rangle$ 态时」。

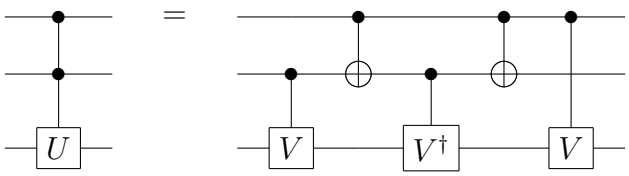
3. 与 CNOT_{x_2,x_1} 的关系

在计算基的矩阵形式上，可以证明

$$(H \otimes H)\,\mathrm{CNOT}_{1\to 2}\,(H \otimes H) = \mathrm{CNOT}_{2\to 1},$$

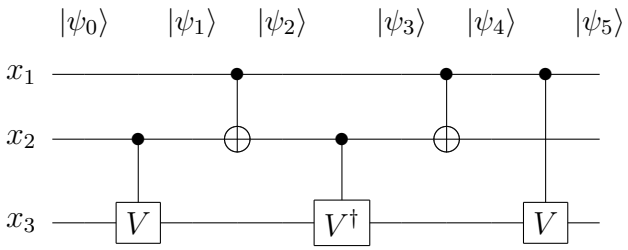
即在 $|0/1\rangle$ 基下，这是一个“控制与目标对调”的 CNOT。我们这里通过对 $|\pm\rangle\,|\pm\rangle$ 的显式作用，给出了同一个算符在 $|\pm\rangle$ 基下的直观表现。 □

练习 4.21 ($C^2(U)$ 的分解验证)**.** 验证下图的 $C^2(U)$ 的分解运算：



其中，$V^2 = U$，且 U, V 均为酉算符。

解答. 该练习尽管可以使用数学方法作证明（矩阵乘法），但过程非常繁琐。分类讨论是最快的处理方法。我们考察分解后的线路图，并在每一步操作后标记系统状态：



上图的过程是指，对于初始三粒子态 $|\psi_0\rangle = |x_1x_2\rangle \otimes |x_3\rangle$，经过该门电路后得到 $|\psi_5\rangle$。我们对 $|x_1x_2\rangle = |00\rangle, |01\rangle, |10\rangle, |11\rangle$ 分别进行讨论。下面需要利用到酉矩阵的性质 $VV^\dagger = V^\dagger V = I$。

$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$	$\|\psi_5\rangle$	
init	ctrl-V_{x_2,x_3}	CNOT_{x_1,x_2}	ctrl-$V^\dagger_{x_2,x_3}$	CNOT_{x_1,x_2}	ctrl-V_{x_1,x_3}	eq
$\|00\rangle \otimes \|x_3\rangle$	$\|00\rangle \otimes \|x_3\rangle$	$\|00\rangle \otimes \|x_3\rangle$	$\|00\rangle \otimes \|x_3\rangle$	$\|00\rangle \otimes \|x_3\rangle$	$\|00\rangle \otimes \|x_3\rangle$	I
$\|01\rangle \otimes \|x_3\rangle$	$\|01\rangle \otimes V\|x_3\rangle$	$\|01\rangle \otimes V\|x_3\rangle$	$\|01\rangle \otimes V^\dagger V\|x_3\rangle$	$\|01\rangle \otimes I\|x_3\rangle$	$\|01\rangle \otimes I\|x_3\rangle$	I
$\|10\rangle \otimes \|x_3\rangle$	$\|10\rangle \otimes \|x_3\rangle$	$\|11\rangle \otimes \|x_3\rangle$	$\|11\rangle \otimes V^\dagger\|x_3\rangle$	$\|10\rangle \otimes V^\dagger\|x_3\rangle$	$\|10\rangle \otimes VV^\dagger\|x_3\rangle$	I
$\|11\rangle \otimes \|x_3\rangle$	$\|11\rangle \otimes V\|x_3\rangle$	$\|10\rangle \otimes V\|x_3\rangle$	$\|10\rangle \otimes V\|x_3\rangle$	$\|11\rangle \otimes V\|x_3\rangle$	$\|11\rangle \otimes V^2\|x_3\rangle$	U

这其中，只有 $|11\rangle\otimes|x_3\rangle$ 给出了 $|11\rangle\otimes U|x_3\rangle$（因为 $V^2 = U$），其它情况（$|00\rangle, |01\rangle, |10\rangle$）都保持初态不变（因为 $V^\dagger V = I$ 且 $VV^\dagger = I$）。

因此，该门路从定义上确实符合 x_1, x_2 为控制量子比特、x_3 为目标量子比特的受控 U 门路（即 $C^2(U)$）。 □

练习 4.22 ($\mathrm{C}^2(U)$ 的分解大纲，文中作引理与步骤)**.** 证明一个 $C^2(U)$*(*对任意单量子比特酉算符 U*)* 可至多用 *8* 个单量子比特门和 *6* 个受控非门构造出来。(本节为 *4.22* 之前的分解/引理，略写要点。)

解答. 这一题主要是让你理解「$\mathrm{C}^2(U)$ 如何拆成 CNOT + 单比特门」的思路，不需要把所有细节都写成公式。我们按步骤画一下“路线图”。

(1) 第一步：把 U 写成 $AXBXC$ 的形式

前面已经知道：任意单比特酉 U 可以写成

$$U = e^{i\alpha} R_{\hat{n}}(\theta)$$

的形式，也可以进一步写成

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

其中 A, B, C 是单比特酉，X 是 Pauli-X 门（翻转）。

这个 $AXBXC$ 的好处是：如果我们有一个控制比特，可以在目标比特上插入两个 CNOT，让目标只在「控制 =1」时经历 X 的翻转，从而我们可以利用这两个 X，把 $AXBXC$ 拼出一个受控 U。

(2) 第二步：利用 $AXBXC$ 构造 $\mathrm{C}^1(U)$

考虑两比特系统，第 1 比特为控制 c，第 2 比特为目标 t。构造以下门列：

$$(I \otimes A) \xrightarrow{\mathrm{CNOT}_{c\to t}} (I \otimes B) \xrightarrow{\mathrm{CNOT}_{c\to t}} (I \otimes C).$$

分情况讨论：

- 如果 $c=0$，则两次 CNOT 都不起作用，目标线上只经历 $ABC=I$，所以整体作用是恒等；- 如果 $c=1$，则目标线上经历两次 X：

$$C\ X\ B\ X\ A\ \ =AXBXC\ \ =U.$$

这样，这条线路实现了「当控制 =1 时对目标施加 U，否则不变」，也就是 $\mathrm{C}^1(U)$。

(3) 第三步：把单控结构提升到双控结构

双控 U，$\mathrm{C}^2(U)$，有两个控制比特 c_1, c_2，一个目标比特 t。理想作用是：

- 如果 $c_1=c_2=1$，对 t 施加 U；- 其他情况对 t 不变。

构造思路：

1. 用一个类似 *Toffoli* 的结构，把 c_1, c_2 的“与”结果（c_1c_2）暂时存到某个比特（可以是目标或辅助比特）上；2. 对这个“与结果”作为控制，施加刚才的 $\mathrm{C}^1(U)$ 结构；3. 再把第一步的存储“解回去”，恢复所有控制比特的原始状态。

在具体实现中，你会用到：

- “三 CNOT 恒等式”来构造等价于 Toffoli 的门路；- 一些对角门与控制门的对易关系，把对角门平移到更方便的位置；- 最后整理成只依赖 CNOT 和单比特门的标准形式。

本题只要求记住这三大步的**思路**，具体细节在下文中通过引理逐个证明。

这里我们把上文中出现的几个引理，用比较直观的语言复述一遍，以便在后面分解 Toffoli、$\mathrm{C}^2(U)$ 时调用。

引理一：三门 CNOT 恒等式

典型形式：

$$\mathrm{CNOT}_{a\to b}\ \mathrm{CNOT}_{b\to a}\ \mathrm{CNOT}_{a\to b}$$

等价于某种「交换加翻转」的操作。这个恒等式的本质是：在计算基上，CNOT 只是在做“翻转/置换”，所以有些组合可以相互抵消、合成。

推论：有些 CNOT 可以互相对易，有些可以吸收到一起，减少门数。

引理二：对角算符 Λ 与受控门可交换

设

$$\Lambda=\lambda_0P_0+\lambda_1P_1$$

是单比特对角算符（也就是在 $|0\rangle, |1\rangle$ 基下只在对角线有元素）。形如

$$P_0\otimes I+P_1\otimes A$$

的受控门，只是根据控制比特是 $|0\rangle$ 还是 $|1\rangle$，选择对目标应用 I 或 A。

因为 Λ 只是对 $|0\rangle$、$|1\rangle$ 乘上不同相位，**不会改变控制比特是谁**，所以可以在受控门前后随意平移：

$$(\Lambda\otimes I)\big(P_0\otimes I+P_1\otimes A\big)=\big(P_0\otimes I+P_1\otimes A\big)(\Lambda\otimes I).$$

引理三：某类算符在双比特空间是对角的

例如

$$\sum_{j=0}^{1} \lambda_j \left|j\right\rangle \left\langle j\right| \otimes U_j$$

在控制比特上是用 $|0\rangle, |1\rangle$ 分块的算符。对控制比特来说，它就是

$$\begin{pmatrix} \lambda_0 U_0 & 0 \\ 0 & \lambda_1 U_1 \end{pmatrix}$$

这样的块对角形式。在分解受控门时，往往需要将这种“块对角结构”穿过其他控制节点，而不改变电路逻辑。

小结

这些引理共同的作用是：

- 用来移动某些单比特或对角门；- 用来化简 CNOT 组合（合并、抵消、重排）；- 最终把复杂的多控结构整理成“少量 CNOT + 单比特门”的组合。

你可以暂时把它们当作“线路变形的工具箱”，在后面看到具体电路时，再一条一条套用。 □

练习 4.23. *仅用 CNOT 与单比特门构造 $C^1(R_y(\theta))$ 与 $C^1(R_x(\theta))$ 。*

解答. 目标：构造“**一控** $R_y(\theta)$”和“一控 $R_x(\theta)$”的线路，也就是：

- 如果控制比特是 $|0\rangle$，目标比特不变；- 如果控制比特是 $|1\rangle$，目标比特施加 $R_y(\theta)$ 或 $R_x(\theta)$。

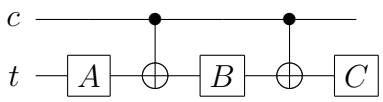
通用模板：若 $U = AXBXC$，则两 CNOT 实现 $\mathrm{C}^1(U)$

假设单比特酉 U 可以写成

$$U = AXBXC, \qquad ABC = I,$$

其中 A, B, C 是单比特酉，X 是 Pauli-X。

考虑两比特线路（控制：第 1 比特 c，目标：第 2 比特 t）：



我们分别看 $c = 0$ 和 $c = 1$ 两种情况。

情况一：控制比特 $c = |0\rangle$。

此时 CNOT 的控制为 0，因此两次 CNOT 都不起作用，目标比特只经历

$$CBA = I,$$

所以目标实际上没有被改变，符合「控制 =0 时不做操作」。

情况二：控制比特 $c = |1\rangle$。

此时两次 CNOT 都会在目标上施加 X 门。目标上的总算符是按右到左相乘：

$$C\ X\ B\ X\ A = AXBXC = U.$$

因此控制 =1 时，对目标施加 U。这就是一控 U。

所以，只要能把 $R_y(\theta)$、$R_x(\theta)$ 写成 $AXBXC$ 的形式，就能用这个模板构造一控版本。

(1) 为 $R_y(\theta)$ 构造 $AXBXC$ 分解

我们利用恒等式

$$XR_y(\theta)X = R_y(-\theta).$$

思路是把 $R_y(\theta)$ 分成两个角度为 $\theta/2$ 的旋转，并在中间插入 X：

$$\begin{aligned} R_y(\theta) &= R_y\Big(\frac{\theta}{2}\Big)\cdot R_y\Big(\frac{\theta}{2}\Big) \\ &= R_y\Big(\frac{\theta}{2}\Big)\Big[XR_y\Big(-\frac{\theta}{2}\Big)X\Big], \end{aligned}$$

其中第二步由 $XR_y(\theta/2)X = R_y(-\theta/2)$ 得来。

于是

$$R_y(\theta) = \underbrace{R_y(\tfrac{\theta}{2})}_{A}\ X\ \underbrace{R_y(-\tfrac{\theta}{2})}_{B}\ X\ \underbrace{I}_{C}.$$

可以验证

$$ABC = R_y(\tfrac{\theta}{2})R_y(-\tfrac{\theta}{2})I = I.$$

所以我们得到了 $R_y(\theta) = AXBXC$ 的一组选择：

$$A = R_y\Big(\frac{\theta}{2}\Big),\quad B = R_y\Big(-\frac{\theta}{2}\Big),\quad C = I.$$

把 U 换成 $R_y(\theta)$，套用上面的通用模板，就得到 $\mathrm{C}^1(R_y(\theta))$ 的线路：在目标线上依次加上 A, B, C，中间两次由控制触发的 CNOT。

(2) 为 $R_x(\theta)$ 构造 $AXBXC$ 分解

首先用 Hadamard 把 R_x 转换为 R_z：

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

对 $R_z(\theta)$ 重复刚才对 $R_y(\theta)$ 的处理。也有

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

因此

$$R_z(\theta) = R_z\Big(\frac{\theta}{2}\Big)\,X\,R_z\Big(-\frac{\theta}{2}\Big)\,X.$$

套到 $R_x(\theta)$ 中：

$$\begin{aligned} R_x(\theta) &= HR_z(\theta)H \\ &= H\Big[R_z\Big(\frac{\theta}{2}\Big)\,X\,R_z\Big(-\frac{\theta}{2}\Big)\,X\Big]H \\ &= \Big[HR_z(\tfrac{\theta}{2})\Big]\,X\,\Big[R_z(-\tfrac{\theta}{2})H\Big]\,X. \end{aligned}$$

于是可以取

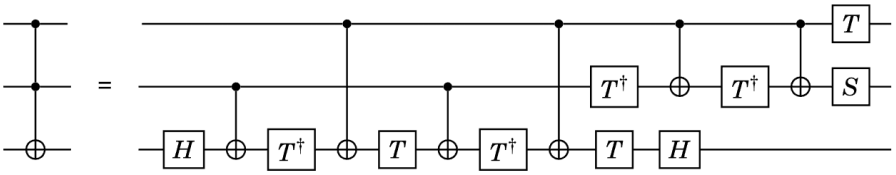
$$A = HR_z\Big(\frac{\theta}{2}\Big), \quad B = R_z\Big(-\frac{\theta}{2}\Big)H, \quad C = I.$$

同样可以验证 $ABC = I$。

这样，$R_x(\theta)$ 也写成了 $AXBXC$ 的形式。用同一个两 CNOT 模板，就可以实现 $\mathrm{C}^1(R_x(\theta))$。

总结：关键是学会把单比特酉写成 $AXBXC$ 形式，然后照模板“夹”两个 CNOT，就得到一控版本。 □

练习 4.24 (Toffoli 门的验证)**.** 验证下图所示的量子线路实现了 *Toffoli* 门。令 $V = \frac{(1+i)(I-iX)}{2}$

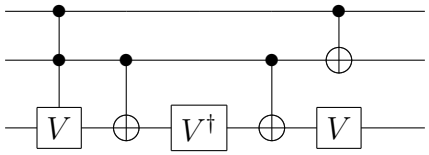


满足 $V^2 = X$。给出 $V = e^{i\alpha}AXBXC$ 的分解并据此证明图 *4.9* 的 *Toffoli* 门等式。

解答. 这题的关键有两步：

1. 验证 $V^2 = X$；2. 找到 $V = e^{i\alpha}AXBXC$ 的具体 A, B, C, α，然后用前面一控/二控分解的套路。

Toffoli 分解线路图：



(1) 验证 $V^2 = X$

先把 V 写清楚：

$$V = \frac{1+i}{2}(I - iX).$$

记 $\lambda = \frac{1+i}{2}$。则

$$V^2 = \lambda^2(I - iX)^2.$$

我们分两部分计算：

第一部分：$(I - iX)^2$：

$$\begin{aligned}(I - iX)^2 &= (I - iX)(I - iX)\\ &= I \cdot I + I \cdot (-iX) + (-iX) \cdot I + (-iX) \cdot (-iX)\\ &= I - iX - iX + (-i)^2X^2\\ &= I - 2iX - X^2.\end{aligned}$$

因 $X^2 = I$，所以

$$(I - iX)^2 = I - 2iX - I = -2iX.$$

第二部分：λ^2：

$$\lambda^2 = \left(\frac{1+i}{2}\right)^2 = \frac{(1+i)^2}{4} = \frac{1+2i+i^2}{4} = \frac{1+2i-1}{4} = \frac{2i}{4} = \frac{i}{2}.$$

合在一起：

$$V^2 = \lambda^2(I - iX)^2 = \frac{i}{2}(-2iX) = -i^2X = X.$$

所以 $V^2 = X$ 确认无误。

(2) V 的 $AXBXC$ 分解

题目给出一个方便的选择：

$$A = HT, \quad B = T^\dagger, \quad C = H, \quad \alpha = \frac{\pi}{4},$$

其中

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

你可以像前面题一样，真正写出这些矩阵，按顺序算

$$e^{i\alpha}AXBXC$$

并和 V 的矩阵逐项对比。这是纯代数运算，比较长，但没有新概念。

这里我们只指出关键：

- 先算 $XC = XH$；- 再算 $B(XH) = T^\dagger XH$；- 接着左乘 X，得到 $XT^\dagger XH$；- 最后左乘 $A = HT$，得到 $HTXT^\dagger XH$；- 整体乘上相位 $e^{i\pi/4}$，结果等于 V。

验证过程中会用到已知恒等式：

- $T = e^{i\pi/8}R_z(\pi/4)$；- $HR_z(\theta)H = R_x(\theta)$；- 各种 Pauli 矩阵的乘法规则。

(3) 用 V 的分解构造 Toffoli

Toffoli 门是**双控非门**，也就是 $\mathrm{C}^2(X)$。因为我们找到了一个单比特 V 使得 $V^2 = X$，就可以用“受控 V”和“受控 $V^\dagger$”来拼出“受控 X”，类似地再上升一层得到双控结构。

主要思路是：

1. 先用 $V = e^{i\alpha}AXBXC$ 的分解构造 $\mathrm{C}^1(V)$、$\mathrm{C}^1(V^\dagger)$；2. 再按 4.21、4.22 的引理构造 $\mathrm{C}^2(V)$、$\mathrm{C}^2(V^\dagger)$；3. 利用 $V^2 = X$，对双控结构组合出 $\mathrm{C}^2(X)$，并用对角门平移、CNOT 恒等式简化线路，得到教科书图 4.9 的 Toffoli 分解。

因为这一步主要是“电路等价变形”，画图比写公式更清楚，这里不再展开长篇矩阵计算，只强调：

- $V^2 = X$ 是关键；- $V = e^{i\alpha}AXBXC$ 让我们可以用 CNOT+ 单比特门实现受控 V；- 再在两条控制线上“叠加”这个结构，就能得到 Toffoli。 □

练习 4.25 (Fredkin 门的构造). *(1) 用 3 个 Toffoli 构造受控交换门；(2) 证明第 1 与最后一个 Toffoli 可由 CNOT 替代；(3) 用图 4.8 的分解将中间 Toffoli 替为 6 个双比特门；(4) 能否减到 5 个？*

解答. Fredkin 门（受控 SWAP）有一个控制比特 c 和两个目标比特 a, b。理想作用：

$$|c, a, b\rangle \mapsto \begin{cases} |0, a, b\rangle, & c = 0, \\ |1, b, a\rangle, & c = 1. \end{cases}$$

(1) 三个 Toffoli 构造受控交换

普通的 SWAP（交换 a, b）可以用三条 CNOT 实现：

$$\mathrm{SWAP}_{a,b} = \mathrm{CNOT}_{a\to b}\,\mathrm{CNOT}_{b\to a}\,\mathrm{CNOT}_{a\to b}.$$

现在，如果想要“在$c = 1$ 时 才交换 a, b”：

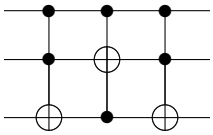
- 把每一条 CNOT 都“升级”为双控非门：第一个控制是 c，第二个控制是原来的控制位。

例如：

- 原来的 $\mathrm{CNOT}_{a\to b}$ 升级为 $\mathrm{Toffoli}_{(c,a)\to b}$；- 原来的 $\mathrm{CNOT}_{b\to a}$ 升级为 $\mathrm{Toffoli}_{(c,b)\to a}$。

当 $c = 0$ 时，三条 Toffoli 都不起作用（因为 Toffoli 的所有控制都要为 1 才触发），于是整个线路是恒等（不交换）；当 $c = 1$ 时，这三条 Toffoli 退化成原来的三条 CNOT，也就把 a, b 交换了。这恰好是 Fredkin。

Fredkin 线路图 (Toffoli 版):



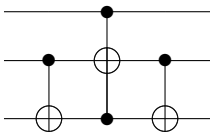
(2) 第 1 与最后一个 Toffoli 可由 CNOT 替代

观察三 Toffoli 线路中中间那条门：它同时依赖 c 和某个目标比特，确实需要双控结构；而前后两条 Toffoli 在某些输入态上第二控制其实永远不会为 1，因而可以简化为单控的 CNOT。具体做法是：

- 写出 Fredkin 门的真值表（8 行，对应 $(c, a, b) \in \{0, 1\}^3$）；- 写出三 Toffoli 线路的真值表；- 比较两者，找出哪些门在某些输入下是“冗余”的；- 将这些冗余的 Toffoli 降级为 CNOT（只依赖一个控制）。

这样可以减少实现 Fredkin 所需的 Toffoli 数量，从 3 个变为 1 个（中间那条），另外两条用 CNOT 即可。

Fredkin 线路图 (CNOT + 1 Toffoli 版):



(3) 用图 4.8 的分解替换中间 Toffoli

图 4.8 给出了 Toffoli 门的分解：用 CNOT 和单比特门拼出 Toffoli（上一题已经讨论过 V 门的作用）。把中间那条 Toffoli 用这套分解替换之后，就得到一个完全没有 Toffoli，只含 CNOT + 单比特门的 Fredkin 门线路。

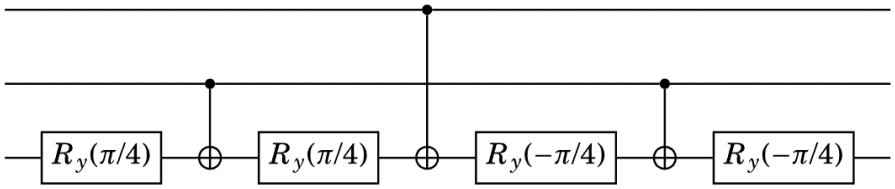
通常一个 Toffoli 需要 6 个双比特门（比如 6 个 CNOT），再加若干单比特门。所以 Fredkin 总共需要 $6+2=8$ 个双比特门左右。

(4) 能否减到 5 个双比特门？

已有文献证明：Fredkin 门在不使用辅助比特的前提下，至少需要 5 个双比特门才能实现。通过精巧的重排和对易，可以把 8 个双比特门的实现优化到 5 个，但不能再少。

这题主要想让你知道：从 “3 个 Toffoli” 到 “1 个 Toffoli + 2 个 CNOT”，再到 “全 CNOT + 单比特门”，门数是可以一步步减少的，但存在理论下界。 □

练习 4.26. 证明给定线路与 *Toffoli* 仅差相对相位：$|c_1,c_2,t\rangle \mapsto e^{i\theta(c_1,c_2,t)}\,|c_1,c_2,t\oplus c_1c_2\rangle$。



解答. “仅差相对相位” 的意思是：对每个计算基态 $|c_1,c_2,t\rangle$（$c_1,c_2,t\in\{0,1\}$），该线路的输出和理想 Toffoli 的输出**只差一个模为 1 的复数因子**。

理想 Toffoli 的作用是

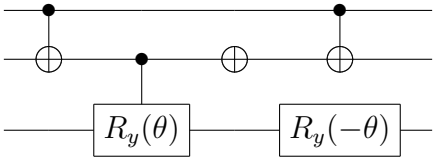
$$|c_1,c_2,t\rangle \mapsto |c_1,c_2,t\oplus c_1c_2\rangle\,.$$

题目给出的线路中，包含了若干 $R_y(\theta)$、CNOT 等门。利用前面练习中的恒等式

$$XR_y(\theta)X = R_y(-\theta),\quad X^2=I,$$

可以对电路逐段化简。

相对相位 Toffoli 线路:



一个典型的验证方法是：

- 对 (c_1,c_2) 固定，分成四类：00、01、10、11；
- 对每一类，把线路中在这条 “分支” 上实际起作用的门写出来（有的门在这一分支上相当于 I）；
- 用矩阵乘法（或直接对 $|t\rangle$）进行合并；

- 比较结果和理想 Toffoli 是否一致，或仅多出一个总体相位。

例如，在某一类输入（比如 $(c_1, c_2) = (1, 0)$）上，线路中可能会额外产生一个 Z 作用在目标位上，而

$$Z\,|0\rangle = |0\rangle\,, \quad Z\,|1\rangle = -\,|1\rangle\,,$$

也就是说只是给 $|1\rangle$ 多了一个 -1 的相位，但不改变比特是否翻转。因此整体变换可以写成

$$|1, 0, t\rangle \mapsto e^{i\theta(1,0,t)}\,|1, 0, t \oplus 0\rangle\,,$$

仍然是 Toffoli 的作用再乘一个相位。

对其他三类输入同样分析，就可以得到

$$|c_1, c_2, t\rangle \longmapsto e^{i\theta(c_1,c_2,t)}\,|c_1, c_2, t \oplus c_1c_2\rangle\,,$$

其中 $e^{i\theta(c_1,c_2,t)}$ 的模长都是 1（可能是 $1, -1, i, -i$ 之类）。

这种“相位不一样但态的 0/1 结构一样”的门，通常称为“相对相位 Toffoli”，在很多量子算法中是足够使用的。 □

练习 4.27. *仅用 CNOT 与 Toffoli 构造实现给定 8×8 循环置换的线路。*

解答. 一个 8×8 循环置换对应三比特空间上 8 个基态的“循环轮换”，例如

$$|000\rangle \mapsto |001\rangle \mapsto |010\rangle \mapsto \cdots \mapsto |111\rangle \mapsto |000\rangle\,.$$

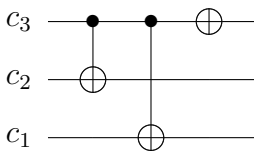
这在本质上就是对三比特二进制数做

$$\text{值} \mapsto (\text{值} + 1) \bmod 8.$$

要用 CNOT 和 Toffoli 来实现，可以按“二进制加一”的方法来构造电路：

- 把 $|c_1, c_2, c_3\rangle$ 看作一个三位二进制数 $c_1c_2c_3$；
- 对最低位加 1；
- 如果有进位，再对更高一位加 1，以此类推；
- 最后用适当的 Toffoli 来处理“从 $|111\rangle$ 回到 $|000\rangle$”的特殊情况。

加 1 循环线路:



构造过程可以这样操作：

1. 先写出给定循环置换的真值表；2. 从 $|000\rangle$ 一行开始，用一条 CNOT 或 Toffoli 把它变成想要的输出态；3. 再看下一行，选门使得已经处理好的行不被破坏，只改变当前行；4. 如此往复，直到 8 行全部匹配。

因为 CNOT 和 Toffoli 可以实现任意布尔函数的组合（它们在经典逻辑上是万能的），所以总能构造出这样的线路。具体线路的形式不是唯一的，本题重点在于“你知道可以用 CNOT/Toffoli 实现任何置换”，包括这个 8×8 的循环。 □

练习 4.28. 设 $U = V^2$（V 酉）。仿图 *4.10* 构造 $C^5(U)$ 而不用工作量子比特，仅可用受控 V 和受控 $V^\dagger$。

解答. 这题的结论是：**在不加辅助比特的情况下，通常做不到**。书上往往用行列式和特征值的分析来证明这一点，这里给出一个直观版的说明。

1. 看 $C^5(U)$ 的特征值结构

$C^5(U)$ 是在 6 比特空间（5 个控制 + 1 个目标）上的酉算符。在计算基下，只有当 5 个控制全为 1 时，目标比特才施加 U，否则都是恒等。因此，$C^5(U)$ 的特征值基本上是：

- 大量的 1（对应那些没有被 U 作用的子空间）；- 再加上 U 的两个特征值 λ_1, λ_2（只在一小块 2 维子空间出现）。

所以

$$\det(C^5(U)) = \det(U).$$

2. 看受控 V、受控 $V^\dagger$ 的行列式

单比特酉 V 满足 $|\det(V)| = 1$。那么一个受控 V（比如一控 V）在整个 Hilbert 空间上的行列式就是 $\det(V)$。同理，受控 $V^\dagger$ 的行列式是 $\det(V)^{-1}$。

如果我们不用辅助比特，只是在同一组 6 条线上串联若干个受控 V 和受控 $V^\dagger$，那么整条线路的行列式是

$$\det(\text{总线路}) = \det(V)^k \cdot \det(V^\dagger)^\ell = \det(V)^{k-\ell},$$

其中 k 是受控 V 的数量，ℓ 是受控 $V^\dagger$ 的数量。

又因为 $U = V^2$，有

$$\det(U) = \det(V)^2.$$

如果总线路要等于 $C^5(U)$，就必须有

$$\det(V)^{k-\ell} = \det(C^5(U)) = \det(U) = \det(V)^2,$$

从而

$$k - \ell = 2.$$

3. 特征值结构的矛盾

更进一步，还可以看整个算符的特征值结构：每个受控 V 或受控 $V^\dagger$ 都会在很多子空间上改变相位，而 $C^5(U)$ 只允许在一个很小的子空间（对应所有控制为 1）上改动谱，其

余地方必须完全是单位矩阵。要用一批“全局分布”的受控 V、受控 $V^\dagger$ 来“只修改一个点”，在没有辅助比特的情况下是不可能的。

详细的线性代数证明可以在教材和文献中找到。这里你只要理解：*受控 V 和受控 $V^\dagger$ 的组合不够“局部”，无法仅对单个 2 维子空间施加 U，而对其他所有子空间都完全不动。*

因此，本题的正确结论是：在题目给的限制下，$C^5(U)$ 一般不可构造；也就是说，这个练习的答案是“做不到”，理由来自谱结构与行列式的不匹配。 □

练习 4.29 (多重受控非门 $C^n(X)$)**.** *设 $n > 3$。在不使用工作量子比特的前提下，用 Toffoli 门、CNOT 和单比特门构造一个包含 $O(n^2)$ 个基本门的线路，实现多重受控非门 $C^n(X)$。*

解答. 目标是实现：当且仅当 n 个控制比特全为 $|1\rangle$ 时，对目标比特施加 X；否则目标不变。

一个常见做法是“逐步压缩”控制比特的 AND 信息，然后再“解压”，过程中只用 Toffoli 门，不额外引入工作比特：

设控制比特为 $c_1, \ldots, c_n$，目标为 t。

(1) **正向压缩：** 利用 Toffoli 将前若干个控制的 AND 临时写入后面的控制线上。例如：

$$\text{Toffoli}(c_1, c_2 \to c_2), \qquad \text{Toffoli}(c_2, c_3 \to c_3), \qquad \ldots$$

这样做的效果是：在每一步，若之前所有控制都为 1，则当前控线被翻转，从而把“前面全为 1”的信息一路传递下去。最终可在某一条线上（如 c_{n-1}）得到“所有控制为 1”的标志。

(2) **用压缩好的控制翻转目标：** 当 AND 结果已经写在某个比特（譬如 c_{n-1}）上后，再用一记 Toffoli

$$\text{Toffoli}(c_{n-1}, c_n \to t)$$

就等价于“若 $c_1, \ldots, c_n$ 全为 1，则对 t 施加 X”。

(3) **反向解压：** 为恢复所有控制比特的原始值，将第一步中的 Toffoli 反向再做一遍（按相反顺序应用同一串 Toffoli）。这样所有控制比特恢复，只有目标比特在“全 1”时被翻转一次。

上述“压缩 + 解压”用到的 Toffoli 门数是 $O(n)$。每个 Toffoli 又可以用常数个 CNOT 和单比特门分解（参考前面 Toffoli 的分解练习），所以总的双比特门数是

$$O(n) \times O(n) = O(n^2),$$

满足题目要求。

这给出了不使用额外工作量子比特实现 $C^n(X)$ 的一种构造，门数量级为 $O(n^2)$。 □

练习 4.30 (一般的多重受控酉 $C^n(U)$)**.** *设 U 是一个单量子比特酉运算，不使用工作量子比特，求一个包含 $O(n^2)$ 个 Toffoli 门、受控非门和单量子比特门的线路，实现 $C^n(U)$ $(n > 3)$。*

解答. 上一题已经给出了在不使用工作量子比特的情况下，构造 $C^n(X)$ 的 $O(n^2)$ 门规模线路。现在我们把任意单比特酉 U 化到这种情形。

根据 4.2 节的结论：任意单比特酉 U 都可以写成

$$U = e^{\mathrm{i}\alpha} R_z(\beta) R_y(\gamma) R_z(\delta),$$

并且可以找到单比特酉 A, B, C 使得

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

在此基础上构造 $C^n(U)$ 的思路与「一控」「二控」的情况完全类似，只是把两次受控 X 换成“多重受控 X”：

考虑下面的门列（控制为前 n 个比特，目标为第 $n+1$ 比特）：

$$(I^{\otimes n} \otimes A)\, C^n(X)\, (I^{\otimes n} \otimes B)\, C^n(X)\, (I^{\otimes n} \otimes C).$$

对输入按“控制是否全为 $|1\rangle$”分两类讨论：

- **若至少有一个控制比特为 $|0\rangle$：**

  此时两次 $C^n(X)$ 都不起作用（因为触发条件是“全部控制为 1”）。目标比特只经历

  $$CBA = I,$$

  因为 $ABC = I$。所以目标保持不变，正是 $C^n(U)$ 的“否则恒等”。

- **若所有控制比特全为 $|1\rangle$：**

  两次 $C^n(X)$ 都在目标上施加 X，目标所经历的单比特算符是

  $$C\,X\,B\,X\,A = AXBXC = e^{-\mathrm{i}\alpha} U,$$

  这与 U 只差一个整体相位 $e^{-\mathrm{i}\alpha}$，在量子力学中整体相位不可观测，因此等价于在目标上施加 U。

因此，上述线路在计算基上实现的正是 $C^n(U)$。

门数方面，这个构造只比 $C^n(X)$ 多了常数个单比特门（A, B, C 及一个全局相位可以忽略），并使用两次 $C^n(X)$。由于上一题中 $C^n(X)$ 已经有一个 $O(n^2)$ 规模的实现，所以整个 $C^n(U)$ 的线路规模仍然是

$$O(n^2).$$

这样就在“不使用工作量子比特”的前提下，用 Toffoli 门、CNOT 和单比特门实现了一般的 $C^n(U)$。 □

练习 4.31 (更多的线路恒等式). 令 C 为第 1 比特控、第 2 比特目标的 $CNOT$。证明：

$$CX_1C = X_1X_2, \qquad CY_1C = Y_1X_2, \qquad CZ_1C = Z_1,$$
$$CX_2C = X_2, \qquad CY_2C = Z_1Y_2, \qquad CZ_2C = Z_1Z_2,$$
$$R_{z,1}(\theta)C = CR_{z,1}(\theta), \qquad R_{x,2}(\theta)C = CR_{x,2}(\theta).$$

解答. 这里我们用**对基态逐个作用**的方法，让每一个恒等式都变成 4 个小算例。

CNOT 的作用规则：

$C = \mathrm{CNOT}_{1\to 2}$ 在计算基上的作用是：

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle.$$

单比特 Pauli 在两比特上的作用：

$$X_1 = X \otimes I：\text{翻转第 1 比特}, \qquad X_2 = I \otimes X：\text{翻转第 2 比特},$$

Y_1, Y_2, Z_1, Z_2 同理。

我们会不断用到这些简单事实，例如

$$X_1 |ab\rangle = |\bar{a}, b\rangle, \quad X_2 |ab\rangle = \left|a, \bar{b}\right\rangle,$$

其中 $\bar{a}$ 表示把 0 变 1，1 变 0。

一、先证明六个关于 X, Y, Z 的共轭恒等式

每个恒等式都是算符等式，我们只要对 4 个基态 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ 检查两边结果相同即可。

1）$CX_1C = X_1X_2$

先算左边 CX_1C 对各基态的作用：

- 对 $|00\rangle$：

$$C|00\rangle = |00\rangle, \quad X_1|00\rangle = |10\rangle, \quad C|10\rangle = |11\rangle.$$

所以

$$CX_1C|00\rangle = |11\rangle.$$

- 对 $|01\rangle$：

$$C|01\rangle = |01\rangle, \quad X_1|01\rangle = |11\rangle, \quad C|11\rangle = |10\rangle.$$

所以

$$CX_1C|01\rangle = |10\rangle.$$

- 对 $|10\rangle$：

$$C|10\rangle = |11\rangle, \quad X_1|11\rangle = |01\rangle, \quad C|01\rangle = |01\rangle.$$

所以

$$CX_1C|10\rangle = |01\rangle.$$

- 对 $|11\rangle$：

$$C|11\rangle = |10\rangle, \quad X_1|10\rangle = |00\rangle, \quad C|00\rangle = |00\rangle.$$

所以

$$CX_1C|11\rangle = |00\rangle.$$

再算右边 X_1X_2：

- $|00\rangle \xrightarrow{X_2} |01\rangle \xrightarrow{X_1} |11\rangle$；
- $|01\rangle \xrightarrow{X_2} |00\rangle \xrightarrow{X_1} |10\rangle$；
- $|10\rangle \xrightarrow{X_2} |11\rangle \xrightarrow{X_1} |01\rangle$；
- $|11\rangle \xrightarrow{X_2} |10\rangle \xrightarrow{X_1} |00\rangle$。

得到的 4 个输出状态和左边完全一致，因此

$$CX_1C = X_1X_2.$$

2）$CY_1C = Y_1X_2$

Y 的作用是

$$Y|0\rangle = i|1\rangle, \quad Y|1\rangle = -i|0\rangle.$$

因此

$$Y_1|ab\rangle = \begin{cases} i|1b\rangle, & a = 0, \\ -i|0b\rangle, & a = 1. \end{cases}$$

同样逐个基态计算左边：

- $|00\rangle$:

$$C|00\rangle = |00\rangle, \quad Y_1|00\rangle = i|10\rangle, \quad C(i|10\rangle) = i|11\rangle.$$

所以

$$CY_1C|00\rangle = i|11\rangle.$$

- $|01\rangle$:

$$C|01\rangle = |01\rangle, \quad Y_1|01\rangle = i|11\rangle, \quad C(i|11\rangle) = i|10\rangle.$$

所以

$$CY_1C|01\rangle = i|10\rangle.$$

- $|10\rangle$:

$$C|10\rangle = |11\rangle, \quad Y_1|11\rangle = -i|01\rangle, \quad C(-i|01\rangle) = -i|01\rangle.$$

所以

$$CY_1C|10\rangle = -i|01\rangle.$$

- $|11\rangle$:

$$C|11\rangle = |10\rangle, \quad Y_1|10\rangle = -i|00\rangle, \quad C(-i|00\rangle) = -i|00\rangle.$$

所以

$$CY_1C|11\rangle = -i|00\rangle.$$

现在算右边 Y_1X_2：

- $|00\rangle \xrightarrow{X_2} |01\rangle \xrightarrow{Y_1} i\,|11\rangle$；
- $|01\rangle \xrightarrow{X_2} |00\rangle \xrightarrow{Y_1} i\,|10\rangle$；
- $|10\rangle \xrightarrow{X_2} |11\rangle \xrightarrow{Y_1} -i\,|01\rangle$；
- $|11\rangle \xrightarrow{X_2} |10\rangle \xrightarrow{Y_1} -i\,|00\rangle$。

完全一致，因此

$$CY_1C = Y_1X_2.$$

3）$CZ_1C = Z_1$

Z 的作用是

$$Z\,|0\rangle = |0\rangle\,, \quad Z\,|1\rangle = -\,|1\rangle\,.$$

因此

$$Z_1\,|ab\rangle = \begin{cases} |0b\rangle\,, & a = 0, \\ -\,|1b\rangle\,, & a = 1. \end{cases}$$

算左边 CZ_1C：

- $|00\rangle$:

$$C\,|00\rangle = |00\rangle\,,\ Z_1\,|00\rangle = |00\rangle\,,\ C\,|00\rangle = |00\rangle\,.$$

所以 $CZ_1C\,|00\rangle = |00\rangle$。

- $|01\rangle$:

$$C\,|01\rangle = |01\rangle\,,\ Z_1\,|01\rangle = |01\rangle\,,\ C\,|01\rangle = |01\rangle\,.$$

所以 $CZ_1C\,|01\rangle = |01\rangle$。

- $|10\rangle$:

$$C\,|10\rangle = |11\rangle\,,\ Z_1\,|11\rangle = -\,|11\rangle\,,\ C(-\,|11\rangle) = -\,|10\rangle\,.$$

- $|11\rangle$:

$$C\,|11\rangle = |10\rangle\,,\ Z_1\,|10\rangle = -\,|10\rangle\,,\ C(-\,|10\rangle) = -\,|11\rangle\,.$$

整理一下：

$$CZ_1C\,|00\rangle = |00\rangle\,, \quad CZ_1C\,|01\rangle = |01\rangle\,, \quad CZ_1C\,|10\rangle = -\,|10\rangle\,, \quad CZ_1C\,|11\rangle = -\,|11\rangle\,.$$

这正是 Z_1 的作用（只看第 1 比特），所以

$$CZ_1C = Z_1.$$

4）$CX_2C = X_2$

X_2 翻转第二比特：

$$X_2 |ab\rangle = \left|a, \bar{b}\right\rangle .$$

算左边 CX_2C：

- $|00\rangle$:

$$C|00\rangle = |00\rangle ,\ X_2|00\rangle = |01\rangle ,\ C|01\rangle = |01\rangle .$$

所以 $CX_2C|00\rangle = |01\rangle$。

- $|01\rangle$:

$$C|01\rangle = |01\rangle ,\ X_2|01\rangle = |00\rangle ,\ C|00\rangle = |00\rangle .$$

所以 $CX_2C|01\rangle = |00\rangle$。

- $|10\rangle$:

$$C|10\rangle = |11\rangle ,\ X_2|11\rangle = |10\rangle ,\ C|10\rangle = |11\rangle .$$

所以 $CX_2C|10\rangle = |11\rangle$。

- $|11\rangle$:

$$C|11\rangle = |10\rangle ,\ X_2|10\rangle = |11\rangle ,\ C|11\rangle = |10\rangle .$$

所以 $CX_2C|11\rangle = |10\rangle$。

而 X_2 本身的作用是

$$|00\rangle \leftrightarrow |01\rangle , \quad |10\rangle \leftrightarrow |11\rangle ,$$

与你刚刚算出的结果一致，所以

$$CX_2C = X_2.$$

5）$CY_2C = Z_1Y_2$

Y_2 在第二比特上作用：

$$Y_2|a0\rangle = i|a1\rangle , \quad Y_2|a1\rangle = -i|a0\rangle .$$

先算左边 CY_2C：

- $|00\rangle$:

$$C|00\rangle = |00\rangle ,\ Y_2|00\rangle = i|01\rangle ,\ C(i|01\rangle) = i|01\rangle .$$

所以 $CY_2C|00\rangle = i|01\rangle$。

- $|01\rangle$:

$$C|01\rangle = |01\rangle ,\ Y_2|01\rangle = -i|00\rangle ,\ C(-i|00\rangle) = -i|00\rangle .$$

所以 $CY_2C|01\rangle = -i|00\rangle$。

- $|10\rangle$:

$$C|10\rangle = |11\rangle,\ Y_2|11\rangle = -i|10\rangle,\ C(-i|10\rangle) = -i|11\rangle.$$

所以 $CY_2C|10\rangle = -i|11\rangle$。

- $|11\rangle$:

$$C|11\rangle = |10\rangle,\ Y_2|10\rangle = i|11\rangle,\ C(i|11\rangle) = i|10\rangle.$$

所以 $CY_2C|11\rangle = i|10\rangle$。

现在算右边 Z_1Y_2：

- 对 $|00\rangle$：先 $Y_2|00\rangle = i|01\rangle$，再 $Z_1(i|01\rangle) = i|01\rangle$；
- 对 $|01\rangle$：先 $Y_2|01\rangle = -i|00\rangle$，再 $Z_1(-i|00\rangle) = -i|00\rangle$；
- 对 $|10\rangle$：先 $Y_2|10\rangle = i|11\rangle$，再 $Z_1(i|11\rangle) = -i|11\rangle$；
- 对 $|11\rangle$：先 $Y_2|11\rangle = -i|10\rangle$，再 $Z_1(-i|10\rangle) = i|10\rangle$。

一一对应，完全一致，所以

$$CY_2C = Z_1Y_2.$$

6）$CZ_2C = Z_1Z_2$

Z_2 在第二比特上作用：

$$Z_2|a0\rangle = |a0\rangle, \quad Z_2|a1\rangle = -|a1\rangle.$$

算左边 CZ_2C：

- $|00\rangle$:

$$C|00\rangle = |00\rangle,\ Z_2|00\rangle = |00\rangle,\ C|00\rangle = |00\rangle.$$

- $|01\rangle$:

$$C|01\rangle = |01\rangle,\ Z_2|01\rangle = -|01\rangle,\ C(-|01\rangle) = -|01\rangle.$$

- $|10\rangle$:

$$C|10\rangle = |11\rangle,\ Z_2|11\rangle = -|11\rangle,\ C(-|11\rangle) = -|10\rangle.$$

- $|11\rangle$:

$$C|11\rangle = |10\rangle,\ Z_2|10\rangle = |10\rangle,\ C|10\rangle = |11\rangle.$$

所以

$$CZ_2C\left|00\right\rangle = \left|00\right\rangle, \quad CZ_2C\left|01\right\rangle = -\left|01\right\rangle, \quad CZ_2C\left|10\right\rangle = -\left|10\right\rangle, \quad CZ_2C\left|11\right\rangle = \left|11\right\rangle.$$

再看 Z_1Z_2 的作用：

- $Z_1Z_2\left|00\right\rangle = \left|00\right\rangle$；- $Z_1Z_2\left|01\right\rangle = -\left|01\right\rangle$（第二比特 1 给 -1，第一比特 0 给 +1）；- $Z_1Z_2\left|10\right\rangle = -\left|10\right\rangle$（第一比特 1 给 -1）；- $Z_1Z_2\left|11\right\rangle = (-1)\cdot(-1)\left|11\right\rangle = \left|11\right\rangle$。

完全一致，所以

$$CZ_2C = Z_1Z_2.$$

二、再证明两个关于旋转门的对易关系

7）$R_{z,1}(\theta)C = CR_{z,1}(\theta)$

$R_z(\theta)$ 在单比特上是

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

所以在两比特上

$$R_{z,1}(\theta) = R_z(\theta)\otimes I = e^{-i\theta/2}\left|0\right\rangle\left\langle 0\right| \otimes I + e^{i\theta/2}\left|1\right\rangle\left\langle 1\right| \otimes I.$$

也就是说，$R_{z,1}(\theta)$ 只是对第一比特为 $\left|0\right\rangle$、$\left|1\right\rangle$ 的分支乘上不同相位，不会把 $\left|0\right\rangle$ 和 $\left|1\right\rangle$ 混在一起。

CNOT 的控制也是看第一比特是 0 还是 1 来决定是否翻转第二比特。因为这两种判断基于的是同一个分解（第一比特 $\left|0\right\rangle / \left|1\right\rangle$），所以先乘相位再看控制，还是先看控制再乘相位，结果一样。

你也可以像前面那样，对 4 个基态逐个验证：

$$R_{z,1}(\theta)C\left|ab\right\rangle = CR_{z,1}(\theta)\left|ab\right\rangle,$$

会发现两边都只是对 $\left|10\right\rangle, \left|11\right\rangle$ 乘上 $e^{\pm i\theta/2}$ 这种相位，而不影响 CNOT 是否触发。

8）$R_{x,2}(\theta)C = CR_{x,2}(\theta)$

$R_{x,2}(\theta) = I\otimes R_x(\theta)$，而

$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X.$$

CNOT 在矩阵上是

$$C = P_0\otimes I + P_1\otimes X,$$

而 $R_{x,2}(\theta) = I\otimes R_x(\theta)$ 可以写成

$$R_{x,2}(\theta) = P_0\otimes R_x(\theta) + P_1\otimes R_x(\theta),$$

也就是说，它对第二比特做 $R_x(\theta)$，不管第一比特是 0 还是 1。

因为 X 和 $R_x(\theta)$ 在单比特空间中是**同轴**的旋转（R_x 是 X 的指数），所以

$$XR_x(\theta) = R_x(\theta)X.$$

从而整块的

$$P_0 \otimes I + P_1 \otimes X$$

与

$$I \otimes R_x(\theta)$$

对易。写成公式就是

$$R_{x,2}(\theta)C = CR_{x,2}(\theta).$$

直观解释：CNOT 只有在控制比特为 $|1\rangle$ 时才在第二比特上做 X，而 $R_x(\theta)$ 是绕同一个轴（x 轴）旋转。两个关于同一轴的旋转是可以互换顺序的，所以整体对易。 □