

Solution 1.2

(a) We're working in a three-dimensional binary vector space. We can set the additive constants to zero, since they have no effect on invertibility. Let's write out the action of the general gate on all eight inputs,

$$\begin{aligned} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} &\longrightarrow \mathbf{0} , \\ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} &\longrightarrow \mathbf{M}_1 , \\ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} &\longrightarrow \mathbf{M}_2 , \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{M}_3 , \\ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &\longrightarrow \mathbf{M}_1 \oplus \mathbf{M}_2 \oplus \mathbf{N}_3 , \\ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{M}_1 \oplus \mathbf{M}_3 \oplus \mathbf{N}_2 , \\ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{M}_2 \oplus \mathbf{M}_3 \oplus \mathbf{N}_1 , \\ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{M}_1 \oplus \mathbf{M}_2 \oplus \mathbf{M}_3 \oplus \mathbf{N}_1 \oplus \mathbf{N}_2 \oplus \mathbf{N}_3 \oplus \mathbf{p} , \end{aligned}$$

From the first four outputs, we have immediately that \mathbf{M}_1 , \mathbf{M}_2 , and \mathbf{M}_3 , i.e., the three columns of M , must be different from the zero vector and different from each other. There are two ways to achieve this. The first is to make the three columns of M linearly independent, and the second is to have \mathbf{M}_1 , \mathbf{M}_2 , and \mathbf{M}_3 nonzero and different, but not linearly independent. In the second case, the columns of M are the three nonzero vectors in a two-dimensional subspace, which implies that each one is the sum of the other two and the sum of all three is the zero vector.

We specialize to the first case throughout the following; i.e., we assume that the columns of M are linearly independent.

(b) The first four outputs are four different vectors in our vector space, and by our assumption of linear independence, the vectors \mathbf{M}_1 , \mathbf{M}_2 , and \mathbf{M}_3 are a basis for the vector

space. The other four vectors in the space are

$$\begin{aligned}\mathbf{V}_1 &= \mathbf{M}_2 \oplus \mathbf{M}_3 , \\ \mathbf{V}_2 &= \mathbf{M}_1 \oplus \mathbf{M}_3 , \\ \mathbf{V}_3 &= \mathbf{M}_1 \oplus \mathbf{M}_2 , \\ \mathbf{V}_4 &= \mathbf{M}_1 \oplus \mathbf{M}_2 \oplus \mathbf{M}_3 .\end{aligned}$$

Notice that \mathbf{V}_1 , \mathbf{V}_2 , and \mathbf{V}_3 lie in a two-dimensional subspace, with each of these three vectors being the sum of the other two and the sum of all three being zero. The last four outputs can be written as

$$\begin{aligned}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} &\longrightarrow \mathbf{V}_3 \oplus \mathbf{N}_3 , \\ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{V}_2 \oplus \mathbf{N}_2 , \\ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{V}_1 \oplus \mathbf{N}_1 , \\ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} &\longrightarrow \mathbf{V}_4 \oplus \mathbf{N}_1 \oplus \mathbf{N}_2 \oplus \mathbf{N}_3 \oplus \mathbf{p} ,\end{aligned}$$

Reversibility requires that the last four outputs be the four \mathbf{V} vectors, which means these outputs must sum to \mathbf{V}_4 . Doing the sum, we get $\mathbf{V}_4 \oplus \mathbf{p}$, so we conclude that $\mathbf{p} = 0$.

(c) The effect of the matrix N must be to permute the four \mathbf{V} vectors. Since the first three vectors—we'll call them the *trio*—are equivalent under interchanging the input labels, the essential classes of permutations are the following.

1. Do nothing, i.e., $\mathbf{N}_1 = \mathbf{N}_2 = \mathbf{N}_3 = 0$. These are the linear three-bit gates, which are the only ones that can be constructed from reversible two-bit gates, all of which are linear.
2. Swap two of the trio, leaving the other two vectors fixed, e.g., $\mathbf{V}_1 \leftrightarrow \mathbf{V}_2$, which follows from $\mathbf{N}_1 = \mathbf{N}_2 = \mathbf{V}_3 = \mathbf{M}_1 \oplus \mathbf{M}_2$ and $\mathbf{N}_3 = 0$.
3. Cycle the three vectors of the trio, e.g., $\mathbf{V}_1 \rightarrow \mathbf{V}_2 \rightarrow \mathbf{V}_3 \rightarrow \mathbf{V}_1$, which follows from $\mathbf{N}_1 = \mathbf{V}_3 = \mathbf{M}_1 \oplus \mathbf{M}_2$, $\mathbf{N}_2 = \mathbf{V}_1 = \mathbf{M}_2 \oplus \mathbf{M}_3$, and $\mathbf{N}_3 = \mathbf{V}_2 = \mathbf{M}_1 \oplus \mathbf{M}_3$.
4. Swap one vector of the trio with \mathbf{V}_4 , leaving the other two vectors of the trio fixed, e.g., $\mathbf{V}_1 \leftrightarrow \mathbf{V}_4$, which follows from $\mathbf{N}_1 = \mathbf{V}_1 \oplus \mathbf{V}_4 = \mathbf{M}_1$ and $\mathbf{N}_2 = \mathbf{N}_3 = 0$.
5. Swap one vector of the trio with \mathbf{V}_4 , and swap the two other vectors of the trio, e.g., $\mathbf{V}_1 \leftrightarrow \mathbf{V}_4$ and $\mathbf{V}_2 \leftrightarrow \mathbf{V}_3$, which follows from $\mathbf{N}_1 = \mathbf{V}_1 \oplus \mathbf{V}_4 = \mathbf{M}_1$ and $\mathbf{N}_2 = \mathbf{N}_3 = \mathbf{V}_1 = \mathbf{M}_2 \oplus \mathbf{M}_3$.
6. Cycle two vectors of the trio and \mathbf{V}_4 , e.g., $\mathbf{V}_1 \rightarrow \mathbf{V}_2 \rightarrow \mathbf{V}_4 \rightarrow \mathbf{V}_1$, which follows from $\mathbf{N}_1 = \mathbf{V}_3 = \mathbf{M}_1 \oplus \mathbf{M}_2$, $\mathbf{N}_2 = \mathbf{V}_2 \oplus \mathbf{V}_4 = \mathbf{M}_2$, and $\mathbf{N}_3 = 0$.

7. Cycle all four vectors, e.g., $\mathbf{V}_1 \rightarrow \mathbf{V}_2 \rightarrow \mathbf{V}_3 \rightarrow \mathbf{V}_4 \rightarrow \mathbf{V}_1$, which follows from $\mathbf{N}_1 = \mathbf{V}_3 = \mathbf{M}_1 \oplus \mathbf{M}_2$, $\mathbf{N}_2 = \mathbf{V}_1 = \mathbf{M}_2 \oplus \mathbf{M}_3$, and $\mathbf{N}_3 = \mathbf{V}_3 + \mathbf{V}_4 = \mathbf{M}_3$.

(d) FREDKIN is the controlled swap. With the control on the last bit, FREDKIN does the following:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} \bar{z}x \oplus zy \\ zx \oplus \bar{z}y \\ z \end{pmatrix} = \begin{pmatrix} x \oplus zx \oplus zy \\ y \oplus zx \oplus zy \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} yz \\ xz \\ xy \end{pmatrix} .$$

This corresponds to

$$\begin{aligned} \mathbf{M}_1 &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & \mathbf{M}_2 &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} & \mathbf{M}_3 &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} , \\ \mathbf{V}_1 &= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} & \mathbf{V}_2 &= \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} & \mathbf{V}_3 &= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} & \mathbf{V}_4 &= \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} , \\ \mathbf{N}_1 &= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} & \mathbf{N}_2 &= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} & \mathbf{N}_3 &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} . \end{aligned}$$

Thus $\mathbf{N}_1 = \mathbf{N}_2 = \mathbf{V}_3$ and $\mathbf{N}_3 = 0$; i.e., FREDKIN is an example of class 2 and, in fact, it is the example given in (c).

TOFFOLI is the controlled-controlled-NOT. If we put the target on the last bit, TOFFOLI does the following:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \oplus xy \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} yz \\ xz \\ xy \end{pmatrix} .$$

This corresponds to

$$\begin{aligned} \mathbf{M}_1 &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & \mathbf{M}_2 &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} & \mathbf{M}_3 &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} , \\ \mathbf{V}_1 &= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} & \mathbf{V}_2 &= \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} & \mathbf{V}_3 &= \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} & \mathbf{V}_4 &= \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} , \\ \mathbf{N}_1 &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \mathbf{N}_2 &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} & \mathbf{N}_3 &= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} . \end{aligned}$$

Thus $\mathbf{N}_1 = \mathbf{N}_2 = 0$ and $\mathbf{N}_3 = \mathbf{M}_3$; i.e., TOFFOLI is an example of class 4.