Notes & Elaborations on Mermin's (2007) *Quantum Computer Science: An Introduction*

Warren (Hoss) Craft

Summer 2019

EQ 1.35 (SWAP operator in terms of projections and flips)

On pg 12, Mermin [1] notes that the SWAP operator S_{ij} can be written as:

$$\boldsymbol{S}_{ij} = \boldsymbol{n}_i\boldsymbol{n}_j + \widetilde{\boldsymbol{n}}_i\widetilde{\boldsymbol{n}}_j + (\boldsymbol{X}_i\boldsymbol{X}_j)(\boldsymbol{n}_i\widetilde{\boldsymbol{n}}_j + \widetilde{\boldsymbol{n}}_i\boldsymbol{n}_j) \tag{1.35}$$

and he goes on to remark that:

> At the risk of belaboring the obvious, I note that (1.35) acts as the swap operator because if both Cbits are in the state $|1\rangle$ (so swapping their states does nothing) then only the first term in the sum acts (*i.e.* each of the other three terms gives 0) and multiplies the state by 1; if both Cbits are in the state $|0\rangle$, only the second term acts and again multiplies the state by 1; if Cbit i is in the state $|1\rangle$ and Cbit j is in the state $|0\rangle$, only the third term acts and the effect of flipping both Cbits is to swap their states; and if Cbit i is in the state $|0\rangle$ and Cbit j is in the state $|1\rangle$, only the fourth term acts and the effect of the two Xs is again to swap their states.

Mermin's comment that "each of the other three terms gives 0", for example, can be confusing, and the interpretation of the summation operations could use some clarification as well. To see more clearly what is happening in (1.35), it can help to consider the SWAP operator S_{01} (and its equivalent in terms of the projections and flips as shown in Eq (1.35)) applied in the concrete case of a 2 Cbit system $|xy\rangle$.

Generally, we have $S_{01}|xy\rangle = |yx\rangle$, and more specifically we have:

$S_{01}|00\rangle = |00\rangle$
$S_{01}|01\rangle = |10\rangle$
$S_{01}|10\rangle = |01\rangle$
$S_{01}|11\rangle = |11\rangle$

That is clear conceptually, but it is also useful to remind ourselves of the underlying algebraic processing using the matrix representations and tensor and matrix multiplication. For example,

$$\begin{aligned} S_{01}|10\rangle &= S_{01}(|1\rangle \otimes |0\rangle) = S_{01}(\begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}) \\ &= S_{01}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \\ &= |1\rangle_2 = |01\rangle \end{aligned}$$

The vector/matrix representations are useful in eventually interpreting the right-hand side of (1.35) and Mermin's comments about some terms giving a 0, because the zero vector $\overline{0} = \mathbf{0}$ does not admit of a ket-based representation (*i.e.*, the Cbit $|0\rangle = (10\ldots0)^T$ is not the same thing as the 2^N-dimensional zero vector $(00\ldots0)^T$).

Toward a better understanding, then, of the right-hand size of (1.35), let us again consider a 2-Cbit system $|xy\rangle$ and recall the matrix representations of the projections ($\boldsymbol{n}$, $\widetilde{\boldsymbol{n}}$) and NOT (or "flip") $\boldsymbol{X}$ operators:

$$\boldsymbol{n} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\widetilde{\boldsymbol{n}} = \mathbf{1} - \boldsymbol{n} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\boldsymbol{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Then we would have:

$$\boldsymbol{n}_1\boldsymbol{n}_0\,|00\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\boldsymbol{n}_1\boldsymbol{n}_0\,|01\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\boldsymbol{n}_1\boldsymbol{n}_0\,|10\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\boldsymbol{n}_1\boldsymbol{n}_0\,|11\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |3\rangle_2 = |11\rangle = \mathbf{1}|11\rangle$$

and we see what Mermin means when he remarks that the first term in the sum (*i.e.*, the $\boldsymbol{n}_i\boldsymbol{n}_j$ term) multiplies the state by 1 when the ith and jth CBits are both $|1\rangle$. We can also see that this concrete example generalizes — by considering what happens, for example, when we have the target states within a larger Cbit system. Suppose we take a 5-Cbit system and consider $\boldsymbol{n}_3\boldsymbol{n}_1$:

$$\begin{aligned}
\boldsymbol{n}_3\boldsymbol{n}_1\,|00000\rangle &= \mathbf{1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{n}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \mathbf{1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{n}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \mathbf{1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \mathbf{0}_{32}
\end{aligned}$$

where $\mathbf{0}_{32}$ indicates a zero vector (consisting of a column vector of 32 zeroes). Whenever a 2×1 zero vector appears as a factor anywhere in the tensor product, we end up with a column vector of all zeros. Thus $\boldsymbol{n}_i\boldsymbol{n}_j$ will always produce a zero vector for any input where the ith and jth states are not both $|1\rangle$. For the case where the ith and jth states are both $|1\rangle$, we get some sense of the generality by again considering the action of $\boldsymbol{n}_3\boldsymbol{n}_1$ on a

5-Cbit system:

$$\begin{aligned}
\boldsymbol{n}_3\boldsymbol{n}_1\,|11010\rangle &= \mathbf{1}\begin{pmatrix}0\\1\end{pmatrix}\otimes\boldsymbol{n}\begin{pmatrix}0\\1\end{pmatrix}\otimes\mathbf{1}\begin{pmatrix}1\\0\end{pmatrix}\otimes\boldsymbol{n}\begin{pmatrix}0\\1\end{pmatrix}\otimes\mathbf{1}\begin{pmatrix}1\\0\end{pmatrix}\\
&= \begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\
&= \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\\
&= \begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\end{pmatrix}^T\\
&= |26\rangle_5\\
&= |11010\rangle
\end{aligned}$$

We can similarly consider the 2nd term in the sum in (1.35), taking a quick look at the operation of $\widetilde{\boldsymbol{n}}_i\widetilde{\boldsymbol{n}}_j$ on the two Cbits in the simple 2-Cbit system $|xy\rangle$:

$$\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0\,|00\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |0\rangle_2 = |00\rangle = \mathbf{1}|00\rangle$$

$$\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0\,|01\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0\,|10\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0\,|11\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

There we see that $\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0$ produces a zero vector for any inputs with a $|1\rangle$ as a component in its state, and acts as a unit multiplier for the 2-Cbit system with state $|00\rangle$. As with the $\boldsymbol{n}_1\boldsymbol{n}_0$ operator, these observations about the $\widetilde{\boldsymbol{n}}_1\widetilde{\boldsymbol{n}}_0$ operator on the 2-Cbit system are easily generalized to a $\widetilde{\boldsymbol{n}}_i\widetilde{\boldsymbol{n}}_j$ operator on an N-Cbit system.

In part for the practice but also for the sake of completion, we can consider the effects of the 3rd and 4th terms on a 2-Cbit system. First, the $\boldsymbol{n}_i\widetilde{\boldsymbol{n}}_j$ term:

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|00\rangle = \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|01\rangle = \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|10\rangle = \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |2\rangle_2 = |10\rangle = \mathbf{1}|10\rangle$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|11\rangle = \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

So we see that the $\boldsymbol{n}_i\widetilde{\boldsymbol{n}}_j$ term acts as an identity multiplier only for $|10\rangle$ and produces a zero vector for anything else. Then, the $\widetilde{\boldsymbol{n}}_i\boldsymbol{n}_j$ term:

$$\widetilde{\boldsymbol{n}}_1\boldsymbol{n}_0\,|00\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|01\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |1\rangle_2 = |01\rangle = \mathbf{1}|01\rangle$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|10\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\boldsymbol{n}_1\widetilde{\boldsymbol{n}}_0\,|11\rangle = \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

We see that the $\widetilde{\boldsymbol{n}}_i\boldsymbol{n}_j$ term acts as an identity multiplier only for $|01\rangle$ and produces a zero vector for anything else.

The results (appropriately generalized, and echoing the description by Mermin) are summarized in Figure 1

EQ 1.40 (The cNOT operator in terms of $\boldsymbol{X}$ and $\boldsymbol{Z}$)

Using the $\boldsymbol{X}$ (NOT or "flip") and $\boldsymbol{Z}$ operators:

$$\boldsymbol{X} = \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\boldsymbol{Z} = \widetilde{\boldsymbol{n}} - \boldsymbol{n} = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

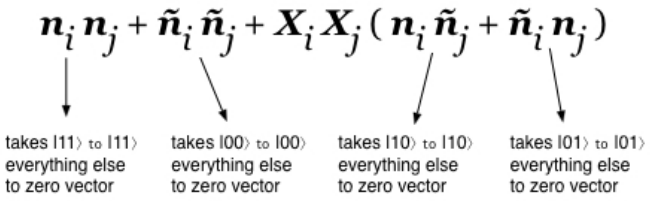

Figure 1: Summary interpretation of terms in Mermin's (2007) Eq (1.35), pg 12. For the ith and jth Cbits each being $|1\rangle$, all the terms but the first collapse to zero vectors and that first term returns the original input. For the ith and jth Cbits each being $|0\rangle$, all the terms but the second one collapse to zero vectors and the second term returns the original input. The third and fourth terms serve as identity multipliers for inputs $|10\rangle$ and $|01\rangle$ respectively, then the X_iX_j operators "flip" the individual states to produce $|01\rangle$ and $|10\rangle$ respectively. The overall effect, then is to take the targeted i, j pair of Cbits and swap their values.

Mermin notes that the cNOT operator can be expressed as:

$$\begin{aligned} \boldsymbol{C}_{ij} &= \frac{1}{2}(\mathbf{1} + \boldsymbol{Z}_i) + \frac{1}{2}\boldsymbol{X}_j(\mathbf{1} - \boldsymbol{Z}_i) \\ &= \frac{1}{2}(\mathbf{1} + \boldsymbol{X}_j) + \frac{1}{2}\boldsymbol{Z}_i(\mathbf{1} - \boldsymbol{X}_j) \end{aligned} \tag{1.40}$$

where "The second form follows from the first because $\boldsymbol{X}_j$ and $\boldsymbol{Z}_i$ commute when $i \neq j$" [pg. 13]

To see this more clearly, we expand the first line, rearrange, and then use the commutativity of $\boldsymbol{X}_j$ and $\boldsymbol{Z}_i$ as follows:

$$\begin{aligned} \boldsymbol{C}_{ij} = \frac{1}{2}(\mathbf{1} + \boldsymbol{Z}_i) + \frac{1}{2}\boldsymbol{X}_j(\mathbf{1} - \boldsymbol{Z}_i) &= \frac{1}{2}\mathbf{1} + \frac{1}{2}\boldsymbol{Z}_i + \frac{1}{2}\boldsymbol{X}_j\mathbf{1} - \frac{1}{2}\boldsymbol{X}_j\boldsymbol{Z}_i \text{ [expanding]} \\ &= \frac{1}{2}\mathbf{1} + \frac{1}{2}\boldsymbol{X}_j\mathbf{1} + \frac{1}{2}\boldsymbol{Z}_i - \frac{1}{2}\boldsymbol{X}_j\boldsymbol{Z}_i \text{ [rearranging]} \\ &= \frac{1}{2}\mathbf{1} + \frac{1}{2}\boldsymbol{X}_j\mathbf{1} + \frac{1}{2}\boldsymbol{Z}_i - \frac{1}{2}\boldsymbol{Z}_i\boldsymbol{X}_j \text{ [commuting } \boldsymbol{X}_j \text{ and } \boldsymbol{Z}_i\text{]} \\ &= \frac{1}{2}(\mathbf{1} + \boldsymbol{X}_j) + \frac{1}{2}\boldsymbol{Z}_i(\mathbf{1} - \boldsymbol{X}_j) \text{ [factoring]} \end{aligned}$$

EQ 1.41 (The Marsh-Hadamard Transformation $\boldsymbol{H}$)

The Hadamard (or Marsh-Hadamard) transformation $\boldsymbol{H}$ is defined by:

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}(\boldsymbol{X} + \boldsymbol{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.41}$$

Mermin observes that (pg 14), since $\boldsymbol{X}^2 = \boldsymbol{Z}^2 = \mathbf{1}$ and $\boldsymbol{XZ} = -\boldsymbol{ZX}$, one easily shows from the definition (1.41) of $\boldsymbol{H}$ in terms of $\boldsymbol{X}$ and $\boldsymbol{Z}$ that

$$\boldsymbol{H}^2 = \mathbf{1} \tag{1.42}$$

and that

$$\boldsymbol{HXH} = \boldsymbol{Z}, \quad \boldsymbol{HZH} = \boldsymbol{X}. \tag{1.43}$$

So let's do the math and show these things. From (1.41) and the anti-commutativity of $\boldsymbol{X}$ and $\boldsymbol{Z}$ we have:

$$\begin{aligned}\boldsymbol{H}^2 &= \frac{1}{2}(\boldsymbol{X}+\boldsymbol{Z})^2 \\ &= \frac{1}{2}(\boldsymbol{X}^2+\boldsymbol{X}\boldsymbol{Z}+\boldsymbol{Z}\boldsymbol{X}+\boldsymbol{Z}^2) \\ &= \frac{1}{2}(\boldsymbol{X}^2+\boldsymbol{X}\boldsymbol{Z}-\boldsymbol{X}\boldsymbol{Z}+\boldsymbol{Z}^2) \\ &= \frac{1}{2}(\boldsymbol{X}^2+\boldsymbol{Z}^2) \\ &= \frac{1}{2}(\mathbf{1}+\mathbf{1}) \\ &= \mathbf{1}\end{aligned}$$

We also have:

$$\begin{aligned}\boldsymbol{H}\boldsymbol{X}\boldsymbol{H} &= \frac{1}{\sqrt{2}}(\boldsymbol{X}+\boldsymbol{Z})\boldsymbol{X}(\frac{1}{\sqrt{2}})(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}+\boldsymbol{Z})\boldsymbol{X}(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}^2+\boldsymbol{Z}\boldsymbol{X})(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}^2\boldsymbol{X}+\boldsymbol{X}^2\boldsymbol{Z}+\boldsymbol{Z}\boldsymbol{X}^2+\boldsymbol{Z}\boldsymbol{X}\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}^2\boldsymbol{X}+\boldsymbol{X}^2\boldsymbol{Z}+\boldsymbol{Z}\boldsymbol{X}^2-\boldsymbol{Z}^2\boldsymbol{X}) \\ &= \frac{1}{2}(\boldsymbol{X}+\boldsymbol{Z}+\boldsymbol{Z}-\boldsymbol{X}) \\ &= \boldsymbol{Z}\end{aligned}$$

and

$$\begin{aligned}\boldsymbol{H}\boldsymbol{Z}\boldsymbol{H} &= \frac{1}{\sqrt{2}}(\boldsymbol{X}+\boldsymbol{Z})\boldsymbol{Z}(\frac{1}{\sqrt{2}})(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}+\boldsymbol{Z})\boldsymbol{Z}(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}\boldsymbol{Z}+\boldsymbol{Z}^2)(\boldsymbol{X}+\boldsymbol{Z}) \\ &= \frac{1}{2}(\boldsymbol{X}\boldsymbol{Z}\boldsymbol{X}+\boldsymbol{X}\boldsymbol{Z}^2+\boldsymbol{Z}^2\boldsymbol{X}+\boldsymbol{Z}^2\boldsymbol{Z}) \\ &= \frac{1}{2}(-\boldsymbol{X}^2\boldsymbol{Z}+\boldsymbol{X}\boldsymbol{Z}^2+\boldsymbol{Z}^2\boldsymbol{X}+\boldsymbol{Z}^2\boldsymbol{Z}) \\ &= \frac{1}{2}(-\boldsymbol{Z}+\boldsymbol{X}+\boldsymbol{X}+\boldsymbol{Z}) \\ &= \boldsymbol{X}\end{aligned}$$

References

[1] N. David Mermin. *Quantum Computer Science: An Introduction.* Cambridge: Cambridge University Press, 2007.