10 Quantum error-correction

Exercises: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 10.16, 10.17, 10.18, 10.19, 10.20, 10.21, 10.22, 10.23, 10.24, 10.25, 10.26, 10.27, 10.28, 10.29, 10.30, 10.31, 10.32, 10.33, 10.34, 10.35, 10.36, 10.37, 10.38, 10.39, 10.40, 10.41, 10.42, 10.43, 10.44, 10.45, 10.46, 10.47, 10.48, 10.49, 10.50, 10.51, 10.52, 10.53, 10.54, 10.55, 10.56, 10.57, 10.58, 10.59, 10.60, 10.61, 10.62, 10.63, 10.64, 10.65, 10.66, 10.67, 10.68, 10.69, 10.70, 10.71, 10.72, 10.73, 10.74.

10.1

Initially we have the state $|\psi\rangle|0\rangle|0\rangle = a|000\rangle + b|100\rangle$, so the action of the circuit is

$$\begin{aligned} a|000\rangle + b|100\rangle &\xrightarrow{CX_{(1,2)}} a|000\rangle + b|110\rangle \\ &\xrightarrow{CX_{(1,3)}} a|000\rangle + b|111\rangle . \end{aligned}$$

10.2

The two projectors P_+ and P_- can be put in the form

$$\begin{aligned} P_+ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) = \frac{|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}(I+X), \\ P_- &= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right) = \frac{|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}(I-X), \end{aligned}$$

Thus the quantum operation $\mathcal{E}(\rho) = (1-2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_-$ can be rewritten as

$$\begin{aligned} \mathcal{E}(\rho) &= (1-2p)\rho + \frac{p}{2}(I+X)\rho(I+X) + \frac{p}{2}(I-X)\rho(I-X) \\ &= (1-2p)\rho + \frac{p}{2}(\rho + X\rho + \rho X + X\rho X) + \frac{p}{2}(\rho - X\rho - \rho X + X\rho X) \\ &= (1-2p)\rho + p(\rho + X\rho X) \\ &= (1-p)\rho + pX\rho X. \end{aligned}$$

10.3

Operators Z_1Z_2 and Z_2Z_3 can be thought of as projective measurements by looking at their respective spectral decomposition which, by defining projectors

$$\begin{aligned} P_{+1}^{(Z_1Z_2)} &\equiv (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I, \\ P_{-1}^{(Z_1Z_2)} &\equiv (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I, \\ P_{+1}^{(Z_2Z_3)} &\equiv I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|), \\ P_{-1}^{(Z_2Z_3)} &\equiv I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|), \end{aligned}$$

can be written as

$$Z_1Z_2 = P_{+1}^{(Z_1Z_2)} - P_{-1}^{(Z_1Z_2)},$$

$$Z_2Z_3 = P_{+1}^{(Z_2Z_3)} - P_{-1}^{(Z_2Z_3)}.$$

Now let us analyze the four possible cases. First, if both Z_1Z_2 and Z_2Z_3 yield $+1$ we have

$$\begin{aligned} P_{+1}^{(Z_2Z_3)} P_{+1}^{(Z_1Z_2)} &= [(I \otimes |00\rangle\langle 00| + |11\rangle\langle 11|)]\,[(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I] \\ &= |000\rangle\langle 000| + |111\rangle\langle 111| = P_0. \end{aligned}$$

If Z_1Z_2 yields -1 and Z_2Z_3 yields $+1$ we have

$$\begin{aligned} P_{-1}^{(Z_2Z_3)} P_{+1}^{(Z_1Z_2)} &= [(I \otimes |00\rangle\langle 00| + |11\rangle\langle 11|)]\,[(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I] \\ &= |100\rangle\langle 100| + |011\rangle\langle 011| = P_1. \end{aligned}$$

If both Z_1Z_2 and Z_2Z_3 yield -1 we have

$$\begin{aligned} P_{-1}^{(Z_2Z_3)} P_{-1}^{(Z_1Z_2)} &= [(I \otimes |01\rangle\langle 01| + |10\rangle\langle 10|)]\,[(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I] \\ &= |010\rangle\langle 010| + |101\rangle\langle 101| = P_2. \end{aligned}$$

And finally if Z_1Z_2 yields $+1$ and Z_2Z_3 yields -1 we have

$$\begin{aligned} P_{+1}^{(Z_2Z_3)} P_{-1}^{(Z_1Z_2)} &= [(I \otimes |01\rangle\langle 01| + |10\rangle\langle 10|)]\,[(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I] \\ &= |001\rangle\langle 001| + |110\rangle\langle 110| = P_3. \end{aligned}$$

10.4

The eight projectors onto the computational basis are $|000\rangle\langle 000|$, $|001\rangle\langle 001|$, $|010\rangle\langle 010|$, $|011\rangle\langle 011|$, $|100\rangle\langle 100|$, $|101\rangle\langle 101|$, $|110\rangle\langle 110|$, and $|111\rangle\langle 111|$. If we measure either $|000\rangle\langle 000|$ or $|111\rangle\langle 111|$ we know that the state prior to the measurement was $a\,|000\rangle + b\,|111\rangle$, meaning no bit flip occurred. If we measure either $|100\rangle\langle 100|$ or $|011\rangle\langle 011|$ we know that the state prior to measurement was $a\,|100\rangle + b\,|011\rangle$, meaning qubit 1 suffered a bit flip. If we measured either $|010\rangle\langle 010|$ or $|101\rangle\langle 101|$ we know that the state prior to measurement was $a\,|010\rangle + b\,|101\rangle$, meaning qubit 2 suffered a bit flip. And if we measure either $|001\rangle\langle 001|$ or $|110\rangle\langle 110|$ we know that the state prior to measurement was $a\,|001\rangle + b\,|110\rangle$, meaning qubit 3 suffered a bit flip.

Since these projective measurements cause the state to collapse to one of the computational basis states it could only be recovered if it was already one of them instead of a superposition. In other words, the state is not altered by the measurement only if either $a = 0$ or $b = 0$, meaning only computational basis states can be recovered.

After the three physical qubits go through the bit flip channel we obtain the state

$$\begin{aligned} \mathcal{E}(|\psi\rangle\langle\psi|) = (1-p)^3\,|\psi\rangle\langle\psi| &+ p(1-p)^2 X_1\,|\psi\rangle\langle\psi|\,X_1 + p(1-p)^2 X_2\,|\psi\rangle\langle\psi|\,X_2 + p(1-p)^2 X_3\,|\psi\rangle\langle\psi|\,X_3 \\ &+ p^2(1-p) X_1X_2\,|\psi\rangle\langle\psi|\,X_1X_2 + p^2(1-p) X_1X_3\,|\psi\rangle\langle\psi|\,X_1X_3 \\ &+ p^2(1-p) X_2X_3\,|\psi\rangle\langle\psi|\,X_2X_3 + p^3 X_1X_2X_3\,|\psi\rangle\langle\psi|\,X_1X_2X_3. \end{aligned}$$

If we consider the initial state to be $|\psi\rangle = a\,|000\rangle + b\,|111\rangle$, after the correction process the term

where no flips occur collapses to $|000\rangle$ with probability $|a|^2$ and to $|111\rangle$ with probability $|b|^2$, and the opposite occurs for the term where three flips occur. The terms where one flip occurs collapse to $|000\rangle$ with probability $|a|^2$ and to $|111\rangle$ with probability $|b|^2$, and the opposite occurs for the terms where two flips occur. Therefore the state at the end of the protocol is given by

$$\begin{aligned}\rho = &\left(|a|^2(1-p)^3 + 3|a|^2p(1-p)^2 + 3|b|^2p^2(1-p) + |b|^2p^3\right)|000\rangle\langle 000| \\ &+ \left(|b|^2(1-p)^3 + 3|b|^2p(1-p)^2 + 3|a|^2p^2(1-p) + |a|^2p^3\right)|111\rangle\langle 111|\,.\end{aligned}$$

The minimum fidelity occurs when the quantity

$$\begin{aligned}\langle\psi|\rho|\psi\rangle &= |a|^2\left(|a|^2(1-p)^3 + 3|a|^2p(1-p)^2 + 3|b|^2p^2(1-p) + |b|^2p^3\right) \\ &\quad + |b|^2\left(|b|^2(1-p)^3 + 3|b|^2p(1-p)^2 + 3|a|^2p^2(1-p) + |a|^2p^3\right) \\ &= \left(|a|^4 + |b|^4\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2|a|^2|b|^2\left[3p^2(1-p) + p^3\right]\end{aligned}$$

is minimal. Using the fact that $|b|^2 = 1 - |a|^2$ we can rewrite

$$\langle\psi|\rho|\psi\rangle = \left(2|a|^4 - 2|a|^2 + 1\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2\left(|a|^2 - |a|^4\right)\left[3p^2(1-p) + p^3\right].$$

For convenience, let us define $x \equiv |a|^2$ such that

$$\langle\psi|\rho|\psi\rangle = \left(2x^2 - 2x + 1\right)\left[(1-p)^3 + 3p(1-p)^2\right] + 2\left(x - x^2\right)\left[3p^2(1-p) + p^3\right].$$

If we differentiate with respect to x we obtain

$$\begin{aligned}\frac{\partial}{\partial x}\langle\psi|\rho|\psi\rangle &= (4x-2)\left[(1-p)^3 + 3p(1-p)^2 - 3p^2(1-p) - p^3\right], \\ \frac{\partial^2}{\partial x^2}\langle\psi|\rho|\psi\rangle &= 4\left[(1-p)^3 + 3p(1-p)^2 - 3p^2(1-p) - p^3\right].\end{aligned}$$

Taking $p < 1/2$, the second derivative is a positive constant, meaning the zero of the first derivative, which occurs for $x = 1/2$, is a minimum. Therefore the minimum fidelity is calculated as

$$F_{\min} = \sqrt{\langle\psi|\rho|\psi\rangle}\Big|_{|a|^2=1/2} = \sqrt{\frac{(1-p)^3 + 3p(1-p)^2 + 3p^2(1-p) + p^3}{2}} = \frac{1}{\sqrt{2}},$$

for all $p < 1/2$. This is expected since the protocol is only able to correct computational basis states ($a = 0$ or $b = 0$), so the worst case would occur for $|a| = |b| = 1/\sqrt{2}$. For the case where we initially have a computational basis state, for example, $|\psi\rangle = |000\rangle$, meaning $a = 1$ and $b = 0$, we have

$$F_{\min} = \sqrt{(1-p)^3 + 3p(1-p)^2} > \frac{1}{\sqrt{2}} \quad \text{for } p < 1/2.$$

10.5

For detecting phase flip we must compare the signs of the three blocks of three qubits each, and we do that by applying a three-qubit X operation on two pairs of blocks. Using b_i to denote the i-th block of three qubits, we must measure the operators $X_{\mathrm{b}_1}X_{\mathrm{b}_2}$ and $X_{\mathrm{b}_2}X_{\mathrm{b}_3}$. The first block is composed by

the three first qubits, meaning $X_{\mathrm{b}_1} = X_1X_2X_3$, the second by qubits 4 to 6, meaning $X_{\mathrm{b}_2} = X_4X_5X_6$, and finally, the third block by qubits 7 to 9, meaning $X_{\mathrm{b}_3} = X_7X_8X_9$. Writing the two operators explicitly, we see that we are measuring operators $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$.

10.6

If one of the first three qubits suffered a phase flip then the sign in this block is wrong. Applying $Z_1Z_2Z_3$ results in

$$Z_1Z_2Z_3\left(\frac{|000\rangle \pm |111\rangle}{\sqrt{2}}\right) = Z_2Z_3\left(\frac{|000\rangle \mp |111\rangle}{\sqrt{2}}\right) = Z_3\left(\frac{|000\rangle \pm |111\rangle}{\sqrt{2}}\right) = \frac{|000\rangle \mp |111\rangle}{\sqrt{2}}.$$

Therefore applying $Z_1Z_2Z_3$ is guaranteed to invert the sign of the first block.

10.7

Let us name the operation elements $E_0 \equiv \sqrt{(1-p)^3}I$, and $E_i = \sqrt{p(1-p)^2}X_i$ for $i = 1, 2, 3$. Explicit calculation yields

$$\begin{aligned}
PE_0^\dagger E_0 P &= (1-p)^3 P, \\
PE_0^\dagger E_i P &= \sqrt{p(1-p)^5} P X_i P, \\
PE_i^\dagger E_0 P &= \sqrt{p(1-p)^5} P X_i^\dagger P, \\
PE_i^\dagger E_j P &= p(1-p)^2 P X_i^\dagger X_j P.
\end{aligned}$$

Since $X_i = X_i^\dagger$ for all indices the second and third equations are the same. Now we have that

$$\begin{aligned}
PX_iP &= \left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) X_i \left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) = 0, \\
PX_iX_jP &= \left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) X_iX_j \left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) = \delta_{ij}P.
\end{aligned}$$

Therefore, writing the equations in matrix form, the α_{ij} matrix will be

$$\alpha = \begin{bmatrix}
(1-p)^3 & 0 & 0 & 0 \\
0 & p(1-p)^2 & 0 & 0 \\
0 & 0 & p(1-p)^2 & 0 \\
0 & 0 & 0 & p(1-p)^2
\end{bmatrix},$$

which is a Hermitian matrix, meaning the quantum error-correction conditions are satisfied.

10.8

The projection onto the code space is $P \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$. Thus using the fact that all error operators in the set are Hermitian we have

$$\begin{aligned}
PIIP &= P \\
PIZ_iP &= PZ_iIP = 0,
\end{aligned}$$

$$PZ_iZ_jP = \delta_{ij}P.$$

The α_{ij} matrix is therefore the identity matrix, which is Hermitian, meaning the quantum error-correction conditions are satisfied.

10.9

The projection onto the code space is $R \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$, and for convenience, we will use the following notation for the operators in the error set:

$$P_i \equiv |0_i,+,+\rangle\langle 0_i,+,+| + |0_i,-,+\rangle\langle 0_i,-,+| + |0_i,+,-\rangle\langle 0_i,+,-| + |0_i,-,-\rangle\langle 0_i,-,-|\,,$$
$$Q_i \equiv |1_i,+,+\rangle\langle 1_i,+,+| + |1_i,-,+\rangle\langle 1_i,-,+| + |1_i,+,-\rangle\langle 1_i,+,-| + |1_i,-,-\rangle\langle 1_i,-,-|\,,$$

where the index in either 0 or 1 indicates the position of such 0 and 1, for example, the state $|0_i,+,+\rangle$ represents $|0,+,+\rangle$ for $i=1$, $|+,0,+\rangle$ for $i=2$, and $|+,+,0\rangle$ for $i=3$. Naturally, we have $RIIR = R$. Now using the fact that $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$ and $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ we obtain

$$\begin{aligned} RIP_iR = RP_iIR &= R\left(\frac{1}{\sqrt{2}}|0_i,+,+\rangle\langle+++| + \frac{1}{\sqrt{2}}|0_i,-,-\rangle\langle---|\right) \\ &= \frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---| = \frac{1}{2}R, \end{aligned}$$

$$\begin{aligned} RIQ_iR = RQ_iIR &= R\left(\frac{1}{\sqrt{2}}|1_i,+,+\rangle\langle+++| - \frac{1}{\sqrt{2}}|1_i,-,-\rangle\langle---|\right) \\ &= \frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---| = \frac{1}{2}R. \end{aligned}$$

We also calculate

$$RP_iP_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 0_i,+,+| + |---\rangle\langle 0_i,-,-|\Big)\frac{1}{\sqrt{2}}\Big(|0_j,+,+\rangle\langle+++| + |0_j,-,-\rangle\langle---|\Big),$$

$$RQ_iQ_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 1_i,+,+| - |---\rangle\langle 1_i,-,-|\Big)\frac{1}{\sqrt{2}}\Big(|1_j,+,+\rangle\langle+++| - |1_j,-,-\rangle\langle---|\Big),$$

Notice that if $i=j$ the result is the same as above since $P_i^2 = P_i$ and $Q_i^2 = Q_i$ for all i. If $i \neq j$

$$RP_iP_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---|\right) = \frac{1}{4}R,$$

$$RQ_iQ_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle+++| + \frac{1}{2}|---\rangle\langle---|\right) = \frac{1}{4}R.$$

The only remaining terms are

$$RP_iQ_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 0_i,+,+| + |---\rangle\langle 0_i,-,-|\Big)\frac{1}{\sqrt{2}}\Big(|1_j,+,+\rangle\langle+++| - |1_j,-,-\rangle\langle---|\Big),$$

$$RQ_iP_jR = \frac{1}{\sqrt{2}}\Big(|+++\rangle\langle 1_i,+,+| - |---\rangle\langle 1_i,-,-| \Big)\frac{1}{\sqrt{2}}\Big(|0_j,+,+\rangle\langle +++| + |0_j,-,-\rangle\langle ---| \Big).$$

In this case, if $i = j$ the result will be zero because of the orthogonality of $|0\rangle$ and $|1\rangle$. If $i \neq j$

$$RP_iQ_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| - \left(-\frac{1}{2}\right)|---\rangle\langle ---|\right) = \frac{1}{4}R,$$

$$RQ_iP_jR = \frac{1}{2}\left(\frac{1}{2}|+++\rangle\langle +++| - \left(-\frac{1}{2}\right)|---\rangle\langle ---|\right) = \frac{1}{4}R.$$

If we construct a matrix with entries $RO_{\rm r}O_{\rm c}R$ such that $O_{\rm r}$ are the operators determining the rows and $O_{\rm c}$ are the ones determining the column, and the order of operators is $\{I, P_1, Q_1, P_2, Q_2, P_3, Q_3\}$, we get the α_{ij} matrix to be given by

$$\alpha = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \end{bmatrix},$$

which is Hermitian, meaning the quantum error-correction conditions are satisfied.

10.10

The projection onto the code space is given by $P \equiv |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$ with

$$|0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}},$$
$$|1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}.$$

Naturally, we have $PIIP = P$, and since $X_i^2 = Y_i^2 = Z_i^2 = I$ for all i we conclude that all entries in the diagonal of the α_{ij} matrix are 1. Let us now analyze the elements in the first row and column of the α_{ij} matrix. They have the form $PIX_iP = PX_iIP$, $PIY_iP = PY_iIP$, and $PIZ_iP = PZ_iIP$. Since X_i and Y_i for all i will just flip the corresponding qubit in each component, and $|0\rangle$ and $|1\rangle$ are orthogonal, the result must vanish, meaning

$$PIX_iP = PX_iIP = 0,$$
$$PIY_iP = PY_iIP = 0.$$

For the Z_i notice that we can simplify the $|0_L\rangle$ and $|1_L\rangle$ to $|0_L\rangle = |+_L\rangle|+_L\rangle|+_L\rangle$ and $|1_L\rangle = |-_L\rangle|-_L\rangle|-_L\rangle$, with

$$|+_L\rangle \equiv \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \quad |-_L\rangle \equiv \frac{|000\rangle - |111\rangle}{\sqrt{2}}.$$

Now it is straightforward to see that Z_1, Z_2, and Z_3 all flip the first $|+_L\rangle$ to $|-_L\rangle$ and vice versa, Z_4, Z_5 and Z_6 do the same to the second, and Z_7, Z_8 and Z_9 do the same to the third. Since $|+_L\rangle$ and $|-_L\rangle$ are orthogonal we also conclude

$$PIZ_iP = PZ_iIP = 0.$$

For the elements with two different operators but containing the same index the result must also vanish because of the relations $XY = iZ$, $YZ = iX$, and $ZX = iY$, so they will reduce to the same terms calculated above, therefore

$$PX_iY_iP = PY_iX_iP = PY_iZ_iP = PZ_iY_iP = PZ_iX_iP = PX_iZ_iP = 0.$$

So far we have 136 out of the 784 entries of the α_{ij} with only the diagonal non-vanishing. It remains to find the 216 elements for which the pair of operators are the same but with different indices, which are PX_iX_jP, PY_iY_jP, and PZ_iZ_jP, and the 432 elements with different operators and indices, which are PX_iY_jP, PY_iX_jP, PX_iZ_jP, PZ_iX_jP, PY_iZ_jP, and PZ_iY_jP. Let us then analyze the first group of elements. The operators X_jX_i and Y_jY_i will just flip the i-th and j-th qubit in each component, which will result in a state orthogonal to $|0_L\rangle$ and $|1_L\rangle$, thus

$$PX_iX_jP = PY_iY_jP = 0 \quad \forall\, i \neq j.$$

For Z_iZ_j, if they flip the same block of $|+_L\rangle$ and $|-_L\rangle$ then they amount to an identity operation, otherwise, the result will vanish for the same reason PIZ_iP and PZ_iIP vanish. The identity operation will occur only if Z_i and Z_j are both in one of these sets: $\{Z_1, Z_2, Z_3\}$, $\{Z_4, Z_5, Z_6\}$, or $\{Z_7, Z_8, Z_9\}$. Also, since Z_i and Z_j commute we have $PZ_iZ_jP = PZ_jZ_iP$. Finally, all remaining terms vanish because the presence of either X_i and/or Y_i will flip qubits, leading to a state orthogonal to $|0_L\rangle$ and $|1_L\rangle$. Therefore all entries of the α_{ij} matrix will be zero except the diagonal and some of the terms of the form $PZ_iZ_jP = PZ_jZ_iP$ (symmetrical), which will all be 1. So the matrix is Hermitian and thus the quantum error-correction conditions are satisfied.

10.11

Such quantum operation corresponds to the depolarizing channel with $p = 1$, which is simply

$$\mathcal{E}(\rho) = \frac{I}{2}.$$

We can rewrite $I/2$ as (see Exercise 8.17)

$$\frac{I}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4},$$

thus a set of operation elements for a quantum operation that replaces any state ρ with $I/2$ is

$$E_0 = \frac{I}{2},\ E_1 = \frac{X}{2},\ E_2 = \frac{Y}{2},\ E_3 = \frac{Z}{2}.$$

Notice that since $X^2 = Y^2 = Z^2 = I$ they satisfy $\sum_i E_i^\dagger E_i = I$.

10.12

$$\begin{aligned}
\mathcal{E}(|0\rangle\langle 0|) &= (1-p)\,|0\rangle\langle 0| + \frac{p}{3}\left(X\,|0\rangle\langle 0|\,X + Y\,|0\rangle\langle 0|\,Y + Z\,|0\rangle\langle 0|\,Z\right) \\
&= (1-p)\,|0\rangle\langle 0| + \frac{p}{3}\left(|1\rangle\langle 1| + |1\rangle\langle 1| + |0\rangle\langle 0|\right) \\
&= \left(1 - \frac{2p}{3}\right)|0\rangle\langle 0| + \frac{2p}{3}\,|1\rangle\langle 1|\,.
\end{aligned}$$

The fidelity will be

$$F(|0\rangle\,, \mathcal{E}(|0\rangle\langle 0|)) = \sqrt{\langle 0|\left[\left(1 - \frac{2p}{3}\right)|0\rangle\langle 0| + \frac{2p}{3}\,|1\rangle\langle 1|\right]|0\rangle} = \sqrt{1 - \frac{2p}{3}}.$$

Since the depolarizing channel always returns mixed states the higher the value of p is, the minimal fidelity will occur whenever the initial state is pure. Since $|0\rangle$ is a pure state the obtained fidelity must correspond to the minimum.

10.13

Let us consider $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Then

$$\begin{aligned}
\mathcal{E}(|\psi\rangle\langle\psi|) &= \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} + \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix} \\
&= \begin{bmatrix} |a|^2 + \gamma|b|^2 & \sqrt{1-\gamma}ab^* \\ \sqrt{1-\gamma}a^*b & (1-\gamma)|b|^2 \end{bmatrix}.
\end{aligned}$$

The fidelity will be

$$\begin{aligned}
F(|\psi\rangle\,, \mathcal{E}(|\psi\rangle\langle\psi|)) &= \sqrt{\begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} |a|^2 + \gamma|b|^2 & \sqrt{1-\gamma}ab^* \\ \sqrt{1-\gamma}a^*b & (1-\gamma)|b|^2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}} \\
&= \sqrt{|a|^4 + (1-\gamma)|b|^4 + \left(\gamma + 2\sqrt{1-\gamma}\right)|a|^2|b|^2}.
\end{aligned}$$

Using the fact that $|b|^2 = 1 - |a|^2$ we may rewrite the fidelity only in terms of a. For convenience let us define $x \equiv |a|^2$. We get

$$F(|\psi\rangle\,, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{x^2 + (1-\gamma)(1-x)^2 + \left(\gamma + 2\sqrt{1-\gamma}\right)x(1-x)}$$

$$= \sqrt{2\left(1-\gamma-\sqrt{1-\gamma}\right)x^2 + \left(3\gamma-2+2\sqrt{1-\gamma}\right)x + (1-\gamma)}.$$

Since the square root is a monotonically increasing function the minimum of the fidelity corresponds to the minimum of the function inside the square root, which we will call $f(x)$. By differentiating it with respect to x we obtain

$$\frac{\mathrm{d}f}{\mathrm{d}x} = 4\left(1-\gamma-\sqrt{1-\gamma}\right)x + \left(3\gamma-2+2\sqrt{1-\gamma}\right).$$

This function is non-negative for all $x \in [0,1]$. One way to verify this is to first calculate $\mathrm{d}f/\mathrm{d}x$ at $x = 1$, which results in

$$\left.\frac{\mathrm{d}f}{\mathrm{d}x}\right|_{x=1} = 2-\gamma-2\sqrt{1-\gamma},$$

non-negative for $0 \leq \gamma \leq 1$. Since the term proportional to x is always non-positive, any $f(x<1)$ must also be non-negative. Therefore $f(x)$ never decreases with x, so the minimum occurs for $x = 0$. Plugging it in the fidelity we find

$$F_{\min}(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{1-\gamma}.$$

10.14

The first column of G must have 1 in its r first entries and 0 elsewhere. The second column must have 1 from the $(r+1)$-th to the $(2r)$-th entry and 0 ensewhere. And the same logic applies to the following columns up to the k-th, which will have 1 in its last r entries and zero elsewhere. For indices $i \in [1, rk]$ and $j \in [1, k]$ one possible expression for the generator matrix is

$$G_{ij} = \begin{cases} 1 & \text{for } (j-1)r < i \leq jr; \\ 0 & \text{otherwise.} \end{cases}$$

10.15

All possible codewords can be formed as a linear combination of the columns of G, that is, if G has columns $(y_1, \cdots, y_k)$ any codeword x can be written as

$$x = \sum_{i=1}^{k} x_i y_i = x_1 y_1 + \cdots + x_k y_k,$$

where all x_i are either 0 or 1. If we include one more column resulting from the addition of two columns, say columns j and l, then any codeword may be written as

$$\begin{aligned} x &= x_1 y_1 + \cdots + x_k y_k + x_{k+1}(y_j + y_l) \\ &= x_1 y_1 + \cdots + (x_j + x_{k+1}) y_j + (x_l + x_{k+1}) y_l + \cdots + x_k y_k. \end{aligned}$$

Since $x_j + x_{k+1}$ and $x_l + x_{k+1}$ will also be either 0 or 1, the set of possible x remains the same.

10.16

H is an $(n-k)\times n$ matrix and any codeword x is an n-dimensional vector. Their relation is such that for any codeword we have $Hx=0$. Considering that the rows of H are given by $(y_1,\cdots,y_{n-k})$ and the entries of x are given by $(x_1,\cdots,x_n)$ the resulting $(n-k)$-dimensional vector will be zero if and only if

$$\sum_{j=1}^{n} y_{1j}x_j = \cdots = \sum_{j=1}^{n} y_{(n-k)j}x_j = 0.$$

If we include one more row to H resulting from the addition of two rows, say rows l and m, the vector resulting from Hx will be $(n-k+1)$-dimensional. The last entry will be given by

$$\sum_{j=1}^{n}(y_{lj}+y_{mj})x_j = \sum_{j=1}^{n} y_{lj}x_j + \sum_{j=1}^{n} y_{mj}x_j = 0,$$

thus this action does not change the code.

10.17

We need $6-2=4$ vectors orthogonal modulo 2 to $(1,1,1,0,0,0)$ and $(0,0,0,1,1,1)$. The vectors $(1,1,0,0,0,0)$, $(0,1,1,0,0,0)$, $(0,0,0,1,1,0)$, and $(0,0,0,0,1,1)$ satisfy this and are all linearly independent of each other, thus

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

10.18

Let the $n-k$ rows of the H matrix be $(x_1,\cdots,x_{n-k})$ and let the k columns of G be $(y_1,\cdots,y_k)$. The resulting $(n-k)\times k$ matrix will have entries in the i-th row and j-th column given by $x_i\cdot y_j$. By construction, all x_i are orthogonal modulo 2 to all y_j, meaning $x_i\cdot y_j=0$, thus $HG=0$.

10.19

Given that $H=[A|I_{n-k}]$, with A an $(n-k)\times k$ matrix, its i-th row is given by

$$x_i = (A_{i1},\cdots,A_{ik},0,\cdots,1,\cdots,0),$$

where the 1 from the identity is at the i-th entry after the first k entries with A terms. We know that the generator matrix must be such that $HG=0$ (see Exercise 10.18). Defining the matrix

$$G \equiv \left[\frac{I_k}{-A}\right],$$

we see that its j-th column is given by

$$y_j = (0, \cdots, 1, \cdots, 0, -A_{1j}, \cdots, -A_{(n-k)j}),$$

where the 1 from the identity is at the j-th entry. The condition $HG = 0$ means that $x_i \cdot y_j = 0$ for all i and j. By direct verification we get

$$\begin{aligned} x_i \cdot y_j &= (A_{i1}, \cdots, A_{ik}, 0, \cdots, 1, \cdots, 0) \cdot (0, \cdots, 1, \cdots, 0, -A_{1j}, \cdots, -A_{(n-k)j}) \\ &= 0 + \cdots + A_{ij} + \cdots + 0 + 0 + \cdots + -A_{ij} + \cdots + 0 \\ &= A_{ij} - A_{ij} = 0. \end{aligned}$$

Thus the generator matrix is indeed the one shown above.

10.20

Considering H has entries H_{ij} with $i \in [1, n-k]$ and $j \in [1, n]$, and any codeword x has entries $(x_1, \cdots, x_n)$ we have $\sum_{j=1}^{n} H_{ij} x_j = 0$ for all i, thus summing for all i yields

$$\sum_{i=1}^{n-k} \sum_{j=1}^{n} H_{ij} x_j = x_1 \sum_{i=1}^{n-k} H_{i1} + \cdots + x_n \sum_{i=1}^{n-k} H_{in} = 0.$$

Notice that $\sum_{i=1}^{n-k} H_{ij}$ corresponds to the j-th column of H, naming it h_j we get

$$x_1 h_1 + \cdots + x_n h_n = 0.$$

Since any $d-1$ columns of H are linearly independent, meaning a sum of $d-1$ of them cannot vanish, any codeword with $d-1$ or fewer entries equal to 1 cannot belong in the code since it would be a contradiction. Therefore the minimum number of entries equal to 1 a codeword in the code can have is d, thus $d(C) = d$.

10.21

Since H can always be written as $[A|I_{n-k}]$, A containing only 0 and 1 entries, it has at most $n-k$ linearly independent columns. All $[n, k, d]$ codes have a matrix H with any set of $d-1$ columns being linearly independent (see Exercise 10.20). Both statements combined implies $n - k \geq d - 1$.

10.22

All $2^r - 1$ columns of H are different, meaning it contains all possible 2^r binary strings with length r excluding the one containing all zeros. But because it contains all possible strings with at least one non-zero entry in its columns, any combination of two such strings will result in a string with two non-zero entries, which must also correspond to a column, meaning there are always groups of three columns which are linearly dependent. It follows that any Hemming code has distance 3 (see Exercise 10.20). Given that $3 = 2t + 1$ for $t = 1$, all Hamming codes can correct errors on one bit.

10.23

-

10.24

For any code C it is always true that the generator matrix G and parity check matrix H satisfy $HG = 0$ (see Exercise 10.18). The analogous relation for $C^\perp$ is $G^{\mathrm{T}}H^{\mathrm{T}} = 0$. If C is weakly self-dual, that is $C \subseteq C^\perp$, then any codeword in C is also a codeword of $C^\perp$, meaning the columns of G or a linear combination of them must be present in H^{T}, thus since $G^{\mathrm{T}}H^{\mathrm{T}} = 0$ it follows that $G^{\mathrm{T}}G = 0$. Conversely, if it is given that $G^{\mathrm{T}}G = 0$ then for any two messages x_1 and x_2 we have two codewords $y_1 = Gx_1$ and $y_2 = Gx_2$ in C are such that $y_1 \cdot y_2 = x_1^{\mathrm{T}}G^{\mathrm{T}}Gx_2 = 0$ by hypothesis, therefore all codewords in C are orthogonal to each other, meaning $C \subseteq C^\perp$, so C is weakly self-dual.

10.25

If $x \in C^\perp$ then for all $y \in C$ we have that $x \cdot y = 0$. Thus $(-1)^{x\cdot y} = 1$ for all y, meaning

$$\sum_{y\in C}(-1)^{x\cdot y} = |C|.$$

If $x \notin C^\perp$ we can consider the columns of the generator matrix G to be given by $(y_1, \cdots, y_n)$, ordered such that from y_1 to y_j are codewords that are not orthogonal to x and from y_{j+1} to y_n they are orthogonal to x. Any $y \in C$ can be written as a linear combination of these y_i. If y is a codeword that contains an even number of elements from the set $(y_1, \cdots, y_j)$ then $x \cdot y = 0$ since it would correspond to a sum modulo 2 of an even number of 1's. Analogously, if y contains an odd number of elements from $(y_1, \cdots, y_j)$ then $x \cdot y = 1$. The number of possible codewords with an even number of elements from this set is

$$\sum_{i=0}^{\lfloor j/2\rfloor}\binom{j}{2i} = \frac{2^j}{2} = 2^{j-1},$$

and the number of possible codewords containing an odd number of elements is

$$\sum_{i=0}^{\lfloor (j-1)/2\rfloor}\binom{j}{2i+1} = \frac{2^j}{2} = 2^{j-1}.$$

Since they are equal then in exactly half of the cases we have $(-1)^{x\cdot y} = 1$ and in the other half we have $(-1)^{x\cdot y} = -1$, meaning

$$\sum_{y\in C}(-1)^{x\cdot y} = 0.$$

10.26

First, since H is an $(n - (k_1 - k_2)) \times n$ matrix, the resulting vector Hx has $n - (k_1 - k_2)$ entries, meaning the ancilla $|0\rangle$ is formed by $n-(k_1-k_2)$ qubits, each initially in state zero. The i-th element

of this vector is given by $\sum_{j=1}^{n} H_{ij}x_j$. H_{ij} and x_j are both either 0 or 1. If $H_{ij} = 0$ then this term will contribute nothing to the sum for the i-th qubit of $|Hx\rangle$ independently of x_j. This corresponds to doing nothing to the i-th qubit of the ancilla system. If $H_{ij} = 1$ then this term will either contribute nothing to the sum if $x_j = 0$, and will sum 1 if $x_j = 1$. This corresponds to applying a bit-flip to the i-th qubit if $x_j = 1$, which is a CNOT gate. Therefore, to create the state $|Hx\rangle$ one must apply CNOT gates with the j-th qubit of $|x\rangle$ acting as control and the i-th qubit of the ancilla system as target for each $H_{ij} = 1$, and apply nothing for each $H_{ij} = 0$.

10.27

Naming e_1 the vector with entries 1 where a bit flip occurred and e_2 the vector with entries 1 where a phase flip occurred, the state after the error will be given by

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v)\cdot e_2} |x + y + v + e_1\rangle .$$

Since $x+y \in C_1$ we can use the parity check matrix H_1 of C_1 to create the state $|H_1(x + y + v + e_1)\rangle = |H_1 v + H_1 e_1\rangle$ in an ancilla system A_1. Given that the parametrization state $|v\rangle$ is known we may also create another ancilla system V in state $|H_1 v\rangle$ with the same procedure. If we apply CNOT gates with the i-th qubit of V as control and the i-th qubit of A_1 as target we effectively put A_1 in the state $|H_1 e_1\rangle$. By measuring the syndrome in system A_1 and discarding it we can correct the bit-flip errors and the resulting state in the original system will be

$$\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v)\cdot e_2} |x + y + v\rangle .$$

Applying a Hadamard gate to each qubit we get the state

$$\begin{aligned} &\frac{1}{\sqrt{|C_2|2^n}} \sum_{z} \sum_{y \in C_2} (-1)^{u \cdot y} (-1)^{(x+y+v)\cdot(e_2+z)} |z\rangle \\ = &\frac{1}{\sqrt{|C_2|2^n}} \sum_{z} \sum_{y \in C_2} (-1)^{y\cdot(u+e_2+z)} (-1)^{(x+v)\cdot(e_2+z)} |z\rangle \end{aligned}$$

Defining $z' \equiv z + u + e_2$ we may rewrite the state as

$$\frac{1}{\sqrt{|C_2|2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{y\cdot z'} (-1)^{(x+v)\cdot(z'+u)} |z' + u + e_2\rangle .$$

We know that $\sum_{y \in C_2} (-1)^{y\cdot z'}$ is either $|C_2|$ for $z' \in C_2^{\perp}$ or 0 otherwise (see Exercise 10.25), so we may rewrite the state as

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^{\perp}} (-1)^{(x+v)\cdot(z'+u)} |z' + u + e_2\rangle .$$

Since $z' \in C_2^{\perp}$ for all terms in the sum we can use the parity check matrix H_2 of $C_2^{\perp}$ to create the state $|H_2(z' + u + e_2)\rangle = |H_2 u + H_2 e_2\rangle$ in an ancilla system A_2. Knowing the parametrization state $|u\rangle$ we

can also create another ancilla system U in state $|H_2 u\rangle$. If we apply CNOT gates with the i-th qubit of U as control and the i-th qubit of A_2 as target we effectively put A_2 in the state $|H_2 e_2\rangle$. Just like before, we can measure the syndrome in system A_2 and correct the bit-flip errors (which correspond to the phase flip errors in the original base), and after discarding it and making the corrections we are left in the state

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{(x+v)\cdot(z'+u)} |z'+u\rangle .$$

By applying Hadamard gates on each qubit again we return to what we had before the first application but with $e_2 = 0$, yielding

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u\cdot y} |x + y + v\rangle ,$$

which is the intended state. So such code is equivalent to $\mathrm{CSS}(C_1, C_2)$.

10.28

The transpose of Eq. (10.77) is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} .$$

In order for it to be the generator matrix for the $[7, 4, 3]$ Hamming code it must have all of its columns linearly independent, which is clearly satisfied, and it must be such that $HG = 0$ (see Exercise 10.18), where H is the parity check matrix shown in Eq. (10.76). By direct verification we get

$$HG = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} .$$

10.29

Let $|\psi_1\rangle, |\psi_2\rangle \in V_S$, then for all $\sigma \in S$ we have $\sigma|\psi_1\rangle = |\psi_1\rangle$ and $\sigma|\psi_2\rangle = |\psi_2\rangle$. Thus for a linear combination $|\phi\rangle \equiv a|\psi_1\rangle + b|\psi_2\rangle$ we obtain

$$\sigma|\phi\rangle = \sigma(a|\psi_1\rangle + b|\psi_2\rangle) = a\sigma|\psi_1\rangle + b\sigma|\psi_2\rangle = a|\psi_1\rangle + b|\psi_2\rangle = |\phi\rangle,$$

meaning $|\phi\rangle$ is stalibilized by S, and therefore $|\phi\rangle \in V_S$.

Let $S = \{\sigma_1, \cdots, \sigma_n\}$, and $\{V_1, \cdots, V_n\}$ be the subspaces stabilized by each individual operator in S. By definition, any state $|\psi\rangle \in V_S$ must be contained in the subspaces V_i for all i. Furthermore, any state that fails to be in at least one of the V_i cannot possibly be in V_S. Therefore we can write

$$V_S = \bigcap_{i=1}^{n} V_i.$$

10.30

If S contains $\pm iI$, it cannot be considered a group without the element $-I$ because $(\pm iI)^2 = -I$, meaning it would not be closed, and therefore not a subgroup. Thus, if $-I \notin S$ then $\pm iI \notin S$.

10.31

If $S = \langle g_1, \cdots, g_l\rangle$ then any two elements in S can be written as products of such generators, that is, $\sigma_a \equiv g_{i_1} \cdots g_{i_a}$, and $\sigma_b \equiv g_{j_1} \cdots g_{j_b}$, where all indices from i_1 to i_a and from j_1 to j_b can assume integer values in the range $[1, \cdots, l]$. Since these combinations are arbitrary, any σ_a will commute with any σ_b only if all g_i and g_j commute for each pair i and j. Conversely, if g_i and g_j commute for each pair i and j then S is clearly Abelian, meaning all of its elements commute.

10.32

From Equation (10.78), we can write the codewords of C_2 implicitly with the state

$$|0_L\rangle = \frac{1}{\sqrt{8}}\Big[\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\Big].$$

The stabilizer generators are $g_1 = X_4X_5X_6X_7$, $g_2 = X_2X_3X_6X_7$, $g_3 = X_1X_3X_5X_7$, $g_4 = Z_4Z_5Z_6Z_7$, $g_5 = Z_2Z_3Z_6Z_7$, $g_6 = Z_1Z_3Z_5Z_7$. By direct verification we get

$$g_1|0_L\rangle = \frac{1}{\sqrt{8}}\Big[\,|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle + |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle\,\Big] = |0_L\rangle,$$

$$g_2|0_L\rangle = \frac{1}{\sqrt{8}}\Big[\,|0110011\rangle + |1100110\rangle + |0000000\rangle + |1010101\rangle + |0111100\rangle + |1101001\rangle + |0001111\rangle + |1011010\rangle\,\Big] = |0_L\rangle,$$

$$
\begin{aligned}
g_3 |0_L\rangle = \frac{1}{\sqrt{8}}\Big[& |1010101\rangle + |0000000\rangle + |1100110\rangle + |0110011\rangle \\
& + |1011010\rangle + |0001111\rangle + |1101001\rangle + |0111100\rangle \Big] = |0_L\rangle\,, \\
g_4 |0_L\rangle = \frac{1}{\sqrt{8}}\Big[& |0000000\rangle + (-1)^2 |1010101\rangle + (-1)^2 |0110011\rangle + (-1)^2 |1100110\rangle \\
& + (-1)^4 |0001111\rangle + (-1)^2 |1011010\rangle + (-1)^2 |0111100\rangle + (-1)^2 |1101001\rangle \Big] = |0_L\rangle\,, \\
g_5 |0_L\rangle = \frac{1}{\sqrt{8}}\Big[& |0000000\rangle + (-1)^2 |1010101\rangle + (-1)^4 |0110011\rangle + (-1)^2 |1100110\rangle \\
& + (-1)^2 |0001111\rangle + (-1)^2 |1011010\rangle + (-1)^2 |0111100\rangle + (-1)^2 |1101001\rangle \Big] = |0_L\rangle\,, \\
g_6 |0_L\rangle = \frac{1}{\sqrt{8}}\Big[& |0000000\rangle + (-1)^4 |1010101\rangle + (-1)^2 |0110011\rangle + (-1)^2 |1100110\rangle \\
& + (-1)^2 |0001111\rangle + (-1)^2 |1011010\rangle + (-1)^2 |0111100\rangle + (-1)^2 |1101001\rangle \Big] = |0_L\rangle\,.
\end{aligned}
$$

So these codewords are clearly stabilized. The remaining ones are represented by the state $|1_L\rangle \equiv X^{\otimes 7} |0_L\rangle$. $X^{\otimes 7}$ clearly commutes with g_1, g_2, and g_3, and since g_4, g_5, and g_6 all contain an even number of Z operators, it also commutes with them, thus for all i we have

$$
g_i |1_L\rangle = g_i X^{\otimes 7} |0_L\rangle = X^{\otimes 7} g_i |0_L\rangle = X^{\otimes 7} |0_L\rangle = |1_L\rangle\,.
$$

Therefore these generators stabilize the codewords of the Steane code.

10.33

Let $r(g) \equiv [x|z]$ and $r(g') \equiv [x'|z']$, where x, x', z, and z' denote n-bit strings containing the information about the positions of the Pauli operators within g and g'. Considering that $x = (x_1, \cdots, x_n)$ and $z = (z_1, \cdots, z_n)$, we obtain

$$
r(g)\Lambda = \begin{bmatrix} x_1 & \cdots & x_n & z_1 & \cdots & z_n \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = \begin{bmatrix} z_1 & \cdots & z_n & x_1 & \cdots & x_n \end{bmatrix},
$$

and thus, considering that $x' = (x'_1, \cdots, x'_n)$ and $z' = (z'_1, \cdots, z'_n)$, we get

$$
r(g)\Lambda r(g')^{\mathrm{T}} = \begin{bmatrix} z_1 & \cdots & z_n & x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} x'_1 \\ \vdots \\ x'_n \\ z'_1 \\ \vdots \\ z'_n \end{bmatrix} = \bigoplus_{i=1}^{n} (z_i x'_i \oplus x_i z'_i).
$$

Let us start by considering $r(g)\Lambda r(g') = 0$. This can only happen if $z_i x'_i \oplus x_i z'_i = 0$ for all i, or if $z_i x'_i \oplus x_i z'_i = 1$ for an even number of indices. The first scenario occur for the following situations: either $x_i = z_i = 0$ or $x'_i = z'_i = 0$, meaning either g or g' has I in the i-th entry; or $x_i = x'_i$ and $z_i = z'_i$, meaning both operators have the same Pauli matrix in the i-th entry. In both cases we

get that g and g' commute. The second scenario occurs if, for an even number of indices, we have $z_i x'_i \neq x_i z'_i$, which is only possible if g and g' have different Pauli matrices (which anti-commute) in the i-th entry. With an even number of operators anti-commuting we get that g and g' commute. Therefore if $r(g)\Lambda r(g')^{\mathrm{T}} = 0$ then g and g' commute. Conversely, if g and g' commute, then for all i, their i-th entries must be either an identity operator (meaning either $x_i = z_i = 0$ or $x'_i = z'_i = 0$) or the same operator in both (meaning $x_i = x'_i$ and $z_i = z'_i$), both cases leading to $z_i x'_i \oplus x_i z'_i = 0$. Alternatively they must have an even number of entries where the matrices anti-commute (meaning $z_i x'_i \neq x_i z'_i \Rightarrow z_i x'_i \oplus x_i z'_i = 1$), leading to $\bigoplus_{i=1}^{n}(z_i x'_i \oplus x_i z'_i) = 0$. Therefore if g and g' commute then $r(g)\Lambda r(g')^{\mathrm{T}} = 0$

10.34

If $-I \notin S$ then evidently $g_j \neq -I$ for all j. Furthermore, we must also have $g_j \neq \pm i\sigma$ for all j, where σ is any tensor product of Pauli matrices, because we would have $(\pm i\sigma)^2 = -I$, which would be a contradiction. There can also not be, simultaneously, elements σ and $-\sigma$, because we would have $\sigma(-\sigma) = (-\sigma)\sigma = -I$, which would also be a contradiction. Therefore, if $-I \notin S$, all generators must be tensor products of Pauli matrices with the same phase factors of either 1 or -1, meaning $g_j^2 = I$ and $g_j \neq -I$ for all j. The converse is immediate, but only true if we add that all generators must commute. A counter example would be, for a single qubit, $S = \langle X, Z\rangle$. Here clearly we have $g_j^2 = I$ and $g_j \neq -I$ for all j, but S would contain the element $ZXZX = (iY)(iY) = -I$.

10.35

If $-I \notin S$ then all generators of g_j of S are commuting tensor products of Pauli matrices with the same phase factors of either 1 or -1 (see Exercise 10.34). Since the generators satisfy $g_j^2 = I$ for all j, and any element $g \in S$ can be written as finite product of k generators, that is, $g = g_{i_1} \cdots g_{i_k}$, we get $g^2 = (g_{i_1} \cdots g_{i_k})^2 = (g_{i_1})^2 \cdots (g_{i_k})^2 = I \cdots I = I$. Thus $g^{-1} = g$ for all $g \in S$, and since any tensor product of Pauli matrices is unitary, we have that $g^{-1} = g^\dagger$, meaning $g^\dagger = g$.

10.36

$$UX_1U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = X_1X_2,$$

$$UX_2U^\dagger = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = X_2,$$

$$UZ_1U^\dagger = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix} = Z_1,$$

$$UZ_2U^\dagger = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix} = Z_1Z_2.$$

10.37

$$UY_1U^\dagger = -iUZ_1X_1U^\dagger = -iUZ_1U^\dagger UX_1U^\dagger = -iZ_1X_1X_2 = Y_1X_2.$$

10.38

We have that $UgU^\dagger = VgV^\dagger$ for all $g \in \{Z_1, Z_2, X_1, X_2\}$, which generates the G_2 Pauli group. We can rewrite this equality as $V^\dagger UgU^\dagger V = g$, which means that $U^\dagger V$ commutes with all elements of G_2. This can only happen if $U^\dagger V$ is proportional to the identity, that is,

$$U^\dagger V = \lambda I \quad \Longrightarrow \quad V = \lambda U.$$

Since both U and V are unitary, we have that $|\lambda| = 1$, meaning it is just an immaterial global phase. Thus we can always choose $\lambda = 1$ and conclude that $U = V$.

10.39

$$SXS^\dagger = \begin{bmatrix}1&0\\0&i\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&-i\end{bmatrix} = \begin{bmatrix}0&-i\\i&0\end{bmatrix} = Y,$$

$$SZS^\dagger = \begin{bmatrix}1&0\\0&i\end{bmatrix}\begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}1&0\\0&-i\end{bmatrix} = \begin{bmatrix}1&0\\0&-1\end{bmatrix} = Z.$$

10.40

Given that

$$HXH^\dagger = Z, \quad HZH^\dagger = X, \quad HYH^\dagger = -Y,$$
$$SXS^\dagger = Y, \quad SYS^\dagger = -X, \quad SZS^\dagger = Z,$$

we need $O(1)$ applications of Hadamard and phase gates to perform normalizer operations on a single qubit up to global phase. Let us define $U \in N(G_{n+1})$ as an operator over $n+1$ qubits such that $UZ_1U^\dagger = X_1 \otimes g$ and $UX_1U^\dagger = Z_1 \otimes g'$, with $g, g' \in N(G_n)$. If we take the state $|0\rangle \otimes |\psi\rangle$, where

$|\psi\rangle$ is an n-qubit eigenstate of an element of G_n, we see that

$$U\left(|0\rangle \otimes |\psi\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\phi_0\rangle + |1\rangle \otimes |\phi_1\rangle\right),$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are also n-qubit eigenstates of elements of G_n. We can define U' as a reduction of the action of U to n qubits as

$$U'|\psi\rangle \equiv \sqrt{2}\langle 0| U\left(|0\rangle \otimes |\psi\rangle\right) = |\phi_0\rangle,$$

meaning U' can be seen as a normalizer of G_n. The goal is to analyze how many Hadamard, phase, and CNOT gates are necessary to construct U from U'. As a hypothesis, let us consider that U' can be constructed with $O(n^2)$ Hadamard, phase, and CNOT gates. Then after adding one qubit, constructing U will require at most $O(n)$ CNOT gates connecting the added qubit to the others, $O(n)$ Hadamard and phase gates for the other qubits, and $O(1)$ Hadamard and phase gates for the added qubit, amounting to $O(n)+O(n)+O(1) = O(n)$ extra gates. Therefore, $O(n^2)+O(n) = O(n^2)$ gates would be necessary in total to construct U. By induction, for any number n of qubits it is possible to build a normalizer using $O(n^2)$ Hadamard, phase, and CNOT gates.

10.41

$$TZT^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z,$$

$$TXT^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix} = \begin{bmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1-i \\ 1+i & 0 \end{bmatrix} = \frac{X+Y}{\sqrt{2}}.$$

$$UZ_1U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&-1&0&0&0 \\ 0&0&0&0&0&-1&0&0 \\ 0&0&0&0&0&0&-1&0 \\ 0&0&0&0&0&0&0&-1 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&-1&0&0&0 \\ 0&0&0&0&0&-1&0&0 \\ 0&0&0&0&0&0&-1&0 \\ 0&0&0&0&0&0&0&-1 \end{bmatrix} = Z_1,$$

$$UX_1U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0 \end{bmatrix} = X \otimes CX_{(2,3)}.$$

Notice that in the subspace of two of the qubits, a CNOT gate with the first qubit as control and second as target can be decomposed as

$$CX = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&\frac{1}{2}&0\\ 0&0&0&\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&-\frac{1}{2}&0\\ 0&0&0&-\frac{1}{2} \end{bmatrix} + \begin{bmatrix} 0&\frac{1}{2}&0&0\\ \frac{1}{2}&0&0&0\\ 0&0&0&\frac{1}{2}\\ 0&0&\frac{1}{2}&0 \end{bmatrix} - \begin{bmatrix} 0&\frac{1}{2}&0&0\\ \frac{1}{2}&0&0&0\\ 0&0&0&-\frac{1}{2}\\ 0&0&-\frac{1}{2}&0 \end{bmatrix}$$

$$= \frac{I \otimes I + Z \otimes I + I \otimes X - Z \otimes X}{2},$$

thus, for qubits 2 (control) and 3 (target) we can write $CX_{(2,3)} = \frac{1}{2}(I + Z_2 + X_3 - Z_2X_3)$, and therefore

$$UX_1U^\dagger = X_1 \otimes \frac{I + Z_2 + X_3 - Z_2X_3}{2}.$$

Since the second qubit is a control qubit exactly like the first one, the results for $UZ_2U^\dagger$ and $UX_2U^\dagger$ must be the same just exchanging the indices 1 and 2, that is,

$$UZ_2U^\dagger = Z_2,$$
$$UX_2U^\dagger = X_2 \otimes \frac{I + Z_1 + X_3 - Z_1X_3}{2}.$$

For the remaining relations we get

$$UX_3U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} = X_3,$$

$$UZ_3U^\dagger = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&-1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix} = CZ_{(1,2)} \otimes Z.$$

Analogously to the CNOT gate, in the subspace of two qubits we can make the decomposition

$$CZ = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&-1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&\frac{1}{2}&0\\ 0&0&0&\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&\frac{1}{2}&0&0\\ 0&0&-\frac{1}{2}&0\\ 0&0&0&-\frac{1}{2} \end{bmatrix} + \begin{bmatrix} \frac{1}{2}&0&0&0\\ 0&-\frac{1}{2}&0&0\\ 0&0&\frac{1}{2}&0\\ 0&0&0&-\frac{1}{2} \end{bmatrix}$$

$$
\begin{aligned}
&- \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \\
&= \frac{I + Z \otimes I + I \otimes Z - Z \otimes Z}{2},
\end{aligned}
$$

thus, for qubits 1 and 2 we can write $CZ_{(1,2)} = \frac{1}{2}(I + Z_1 + Z_2 - Z_1 Z_2)$, and therefore

$$
UZ_3U^\dagger = Z_3 \otimes \frac{I + Z_1 + Z_2 - Z_1 Z_2}{2}.
$$

10.42

Let us consider the unknown state $|\psi\rangle$ is stabilized by $S_\psi \equiv aX_1 + bY_1 + cZ_1$. So the total initial state $|\psi\rangle \otimes (|00\rangle + |11\rangle)/\sqrt{2}$ has stabilizer $\langle S_\psi, Z_2Z_3, X_2X_3\rangle$. First a $CX_{(1,2)}$ is applied, transforming the stabilizer as

$$
\langle aX_1 + bY_1 + cZ_1, Z_2Z_3, X_2X_3\rangle \quad \longrightarrow \quad \langle aX_1X_2 + bY_1X_2 + cZ_1, Z_1Z_2Z_3, X_2X_3\rangle ,
$$

and then a Hadamard gate is applied to the first qubit, transforming the stabilizer to

$$
\langle aX_1X_2 + bY_1X_2 + cZ_1, Z_1Z_2Z_3, X_2X_3\rangle \quad \longrightarrow \quad \langle aZ_1X_2 - bY_1X_2 + cX_1, X_1Z_2Z_3, X_2X_3\rangle .
$$

The end of the circuit consists of the measurements of Z_1 and X_2. We see that both Z_1 and X_2 anti-commute with $X_1Z_2Z_3$ and commute with X_2X_3. **Incomplete...**

10.43

Since S is a subgroup it must satisfy the *closure* property, meaning for all $g \in S$ we have $gSg^\dagger \in S$. Thus $g \in N(S)$ for all $g \in S$, and therefore $S \subseteq N(S)$.

10.44

For all $E \in Z(S)$ and $g \in S$, we have $Eg = gE \Rightarrow EgE^\dagger = g \in S$, meaning $Z(S) \subseteq N(S)$. Since $-I \notin S$, all elements in S are commuting elements with the same phase of either 1 or -1 (see Exercise 10.34). For some $g \in S$ and all $E \in N(S)$ we have $EgE^\dagger = g' \in S$. But since g and g' commute, we have $g' = \pm g$. They can't differ by phase, so we conclude $g' = g$, meaning $Eg = gE$ and thus $N(S) \subseteq Z(S)$. Combining both statements, we get $N(S) = Z(S)$.

10.45

-

10.46

The spaces stabilized by X_1X_2 and X_2X_3 are spanned by $\{|++\rangle, |+-\rangle, |--\rangle, |--\rangle\}$, and $\{|++\rangle, |-+\rangle, |+--\rangle, |--\rangle\}$, respectively. Their intersection is the space of the three qubit phase flip code, and thus its stabilizer is $\langle X_1X_2, X_2X_3\rangle$.

10.47

All elements from g_1 to g_6 contain two Z operators on the same block of three qubits, so

$$\begin{aligned}
&g_Z \frac{(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)}{2\sqrt{2}} \\
&= \frac{(|000\rangle \pm (-1)^2 |111\rangle)(|000\rangle \pm (-1)^2 |111\rangle)(|000\rangle \pm (-1)^2 |111\rangle)}{2\sqrt{2}} \\
&= \frac{(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)(|000\rangle \pm |111\rangle)}{2\sqrt{2}},
\end{aligned}$$

where g_Z is any composition of the first 6 generators, thus they stabilize both codewords. Elements g_7 and g_8 both apply a logical X operation over two of the three blocks of qubits, so

$$\begin{aligned}
g_X |0_L\rangle &= g_X |+_L\rangle |+_L\rangle |+_L\rangle = |+_L\rangle |+_L\rangle |+_L\rangle = |0_L\rangle, \\
g_X |1_L\rangle &= g_X |-_L\rangle |-_L\rangle |-_L\rangle = (-1)^2 |-_L\rangle |-_L\rangle |-_L\rangle = |1_L\rangle,
\end{aligned}$$

where g_X is any combination of g_7 and g_8, and $|\pm_L\rangle \equiv (|000\rangle \pm |111\rangle)/\sqrt{2}$, thus they also stabilize both codewords. Since all elements from g_1 to g_8 commute, they generate the stabilizer for the two codewords of the Shor nine qubit code.

10.48

$$\begin{aligned}
\bar{Z} |0_L\rangle &= X_1X_2X_3X_4X_5X_6X_7X_8X_9 \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\
&= \frac{(|111\rangle + |000\rangle)(|111\rangle + |000\rangle)(|111\rangle + |000\rangle)}{2\sqrt{2}} = |0_L\rangle, \\
\bar{Z} |1_L\rangle &= X_1X_2X_3X_4X_5X_6X_7X_8X_9 \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \\
&= \frac{(|111\rangle - |000\rangle)(|111\rangle - |000\rangle)(|111\rangle - |000\rangle)}{2\sqrt{2}} = -|1_L\rangle.
\end{aligned}$$

From this we see $\bar{Z}$ acts as a logical Z on states $|0_L\rangle$ and $|1_L\rangle$.

$$\begin{aligned}
\bar{X} |0_L\rangle &= Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9 \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\
&= \frac{(|000\rangle + (-1)^3 |111\rangle)(|000\rangle + (-1)^3 |111\rangle)(|000\rangle + (-1)^3 |111\rangle)}{2\sqrt{2}} = |1_L\rangle, \\
\bar{X} |1_L\rangle &= Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9 \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}
\end{aligned}$$

$$= \frac{(|000\rangle - (-1)^3 |111\rangle)(|000\rangle - (-1)^3 |111\rangle)(|000\rangle - (-1)^3 |111\rangle)}{2\sqrt{2}} = |0_L\rangle .$$

From this we see that $\bar{X}$ acts as a logical X on states $|0_L\rangle$ and $|1_L\rangle$. Since all generators have an even number of entries with Pauli matrices, both $\bar{Z}$ and $\bar{X}$ commute with them, and since $\bar{Z}$ and $\bar{X}$ have an odd number (nine) of non-commuting entries, they anti-commute.

10.49

The set of all single qubit errors over five qubits is $\{X_i, Y_i, Z_i\}$, with i ranging from 1 to 5. By direct verification we see that

$$\begin{array}{lll} X_1 g_4 = -g_4 X_1, & Y_1 g_1 = -g_1 Y_1, & Z_1 g_1 = -g_1 Z_1, \\ X_2 g_1 = -g_1 X_2, & Y_2 g_1 = -g_1 Y_2, & Z_2 g_2 = -g_2 Z_2, \\ X_3 g_1 = -g_1 X_3, & Y_3 g_1 = -g_1 Y_3, & Z_3 g_3 = -g_3 Z_3, \\ X_4 g_2 = -g_2 X_4, & Y_4 g_1 = -g_1 Y_4, & Z_4 g_1 = -g_1 Z_4, \\ X_5 g_3 = -g_3 X_5, & Y_5 g_2 = -g_2 X_5, & Z_5 g_2 = -g_2 Z_5, \end{array}$$

that is, all single qubit errors anti-commute with at least one of the generators. Therefore, from Theorem 10.8, any arbitrary single qubit error may be corrected.

10.50

The quantum Hamming bound is given by

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n.$$

In this case, we have $n = 5$, $k = 1$, and are able to correct errors on $t = 1$ qubits. The left-hand side of the quantum Hamming bound then yields

$$\binom{5}{0} 3^0 2^1 + \binom{5}{1} 3^1 2^1 = 32 = 2^n,$$

meaning the Hamming bound is saturated.

10.51

Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ codes such that C_1 and $C_2^\perp$ both corrects t errors, and $C_2 \subset C_1$. The check matrix satisfy the commutativity condition because $H(C_2^\perp)H(C_1)^{\mathrm{T}} = G(C_2)^{\mathrm{T}} H(C_1)^{\mathrm{T}} = [H(C_1)G(C_2)]^{\mathrm{T}} = 0$, where we used the fact that $C_2 \subset C_1$. Given that the rows of the parity check matrices $H(C_2^\perp)$ and $H(C_1)$ give, respectively, the entries with X and Z for the corresponding operators, the resulting code has $(n - k_1) + (n - k_2) = 2n - (k_1 + k_2)$ generators. By hypothesis, and using Theorem 10.8, $C_2^\perp$ can correct phase flip errors and C_1 can correct bit flip errors, both on up to t qubits, so the resulting code with $2n - (k_1 + k_2)$ generators can correct arbitrary errors on up to t qubits. This corresponds to the $CSS(C_1, C_2)$ code.

10.52

Using the two codewords shown in Equations (10.78) and (10.79) we get

$$\begin{aligned}
\bar{Z}\left|0_L\right\rangle &= \frac{Z_1Z_2Z_3Z_4Z_5Z_6Z_7}{\sqrt{8}}\Big[\left|0000000\right\rangle + \left|1010101\right\rangle + \left|0110011\right\rangle + \left|1100110\right\rangle \\
&\qquad + \left|0001111\right\rangle + \left|1011010\right\rangle + \left|0111100\right\rangle + \left|1101001\right\rangle\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\left|0000000\right\rangle + (-1)^4\left|1010101\right\rangle + (-1)^4\left|0110011\right\rangle + (-1)^4\left|1100110\right\rangle \\
&\qquad + (-1)^4\left|0001111\right\rangle + (-1)^4\left|1011010\right\rangle + (-1)^4\left|0111100\right\rangle + (-1)^4\left|1101001\right\rangle\Big] = \left|0_L\right\rangle, \\
\bar{Z}\left|1_L\right\rangle &= \frac{Z_1Z_2Z_3Z_4Z_5Z_6Z_7}{\sqrt{8}}\Big[\left|1111111\right\rangle + \left|0101010\right\rangle + \left|1001100\right\rangle + \left|0011001\right\rangle \\
&\qquad + \left|1110000\right\rangle + \left|0100101\right\rangle + \left|1000011\right\rangle + \left|0010110\right\rangle\Big] \\
&= \frac{1}{\sqrt{8}}\Big[(-1)^7\left|1111111\right\rangle + (-1)^3\left|0101010\right\rangle + (-1)^3\left|1001100\right\rangle + (-1)^3\left|0011001\right\rangle \\
&\qquad + (-1)^3\left|1110000\right\rangle + (-1)^3\left|0100101\right\rangle + (-1)^3\left|1000011\right\rangle + (-1)^3\left|0010110\right\rangle\Big] = -\left|1_L\right\rangle, \\
\bar{X}\left|0_L\right\rangle &= \frac{X_1X_2X_3X_4X_5X_6X_7}{\sqrt{8}}\Big[\left|0000000\right\rangle + \left|1010101\right\rangle + \left|0110011\right\rangle + \left|1100110\right\rangle \\
&\qquad + \left|0001111\right\rangle + \left|1011010\right\rangle + \left|0111100\right\rangle + \left|1101001\right\rangle\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\left|1111111\right\rangle + \left|0101010\right\rangle + \left|1001100\right\rangle + \left|0011001\right\rangle \\
&\qquad + \left|1110000\right\rangle + \left|0100101\right\rangle + \left|1000011\right\rangle + \left|0010110\right\rangle\Big] = \left|1_L\right\rangle, \\
\bar{X}\left|1_L\right\rangle &= \frac{X_1X_2X_3X_4X_5X_6X_7}{\sqrt{8}}\Big[\left|1111111\right\rangle + \left|0101010\right\rangle + \left|1001100\right\rangle + \left|0011001\right\rangle \\
&\qquad + \left|1110000\right\rangle + \left|0100101\right\rangle + \left|1000011\right\rangle + \left|0010110\right\rangle\Big] \\
&= \frac{1}{\sqrt{8}}\Big[\left|0000000\right\rangle + \left|1010101\right\rangle + \left|0110011\right\rangle + \left|1100110\right\rangle \\
&\qquad + \left|0001111\right\rangle + \left|1011010\right\rangle + \left|0111100\right\rangle + \left|1101001\right\rangle\Big] = \left|0_L\right\rangle.
\end{aligned}$$

10.53

The fact that a $k \times k$ identity matrix appears in the check matrix $[000|A_2^{\mathrm{T}}0I]$ for the k encoded Z operators means that all operators have at least one entry with Z while all the others have identity in this same entry. Thus, all encoded Z operators are independent of each other.

10.54

-

10.55

We identify $E = (1, 1, 0)^{\mathrm{T}}$ and $C = (0, 0, 0)^{\mathrm{T}}$. The encoded X will have check matrix given by $[0E^{\mathrm{T}}I|C^{\mathrm{T}}00]$, where the number of entries in each block are respectively $\{r = 3, n-k-r = 3, k = 1\}$. Therefore the check matrix for the encoded X will be $[0001101|0000000]$, corresponding to $X_4X_5X_7$. Given that qubits 1 and 4 were swapped, then 3 and 4, then 6 and 7, this corresponds to $X_3X_5X_6$ in the original code. If we multiply this by $g_1g_2g_3 = X_1X_2X_4X_7$ we obtain $\bar{X}$ of Equation (10.107).

10.56

Since all encoded X and Z operators commute with all elements of the stabilizer, for any codeword $|\psi\rangle$ and g in the stabilizer we have

$$gX|\psi\rangle = Xg|\psi\rangle = X|\psi\rangle,$$
$$gZ|\psi\rangle = Zg|\psi\rangle = Z|\psi\rangle,$$

where we used the fact that $g|\psi\rangle = |\psi\rangle$.

10.57

For the five qubit code, using the generators in Figure 10.12 we get the check matrix

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

In this case we have $n = 5$, $k = 1$, and all rows in the first block are independent, such that $r = 4$. Therefore, for the check matrix to be in standard form, it must be shaped $[I^{(4\times4)}A^{(4\times1)}|B^{(4\times4)}C^{(4\times1)}]$. We begin by relabeling qubits 1 and 4, and then 4 and 5, which means swapping the corresponding columns in each block, yielding

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

Now we can sum rows 1 and 2 to row 4, and then sum row 4 to row 2, yielding

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{array}\right],$$

and this is a check matrix in standard form.

For the nine qubit code, using the generators in Figure 10.11, and relabeling them such that g_7 and g_8 become g_2 and g_1 respectively, and the generators from g_1 to g_6 become g_3 to g_8 respectively, we get the check matrix

$$\left[\begin{array}{ccccccccc|ccccccccc} 0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \end{array}\right]$$

In this case we have $n = 9$, $k = 1$, and the first block has only two independent rows, such that $r = 2$. Therefore, the matrix in standard form will be shaped

$$\left[\begin{array}{ccc|ccc} I^{(2\times2)} & A_1^{(2\times6)} & A_2^{(2\times1)} & B^{(2\times2)} & 0^{(2\times6)} & C^{(2\times1)} \\ 0^{(6\times2)} & 0^{(6\times6)} & 0^{(6\times1)} & D^{(6\times2)} & I^{(6\times6)} & E^{(6\times1)} \end{array}\right].$$

We begin by swapping columns 1 and 3, then 1 and 4, then 1 and 5, and finally 1 and 9, yielding

$$\left[\begin{array}{ccccccccc|ccccccccc} 1&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&1&1&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0 \end{array}\right].$$

Now we only need to sum row 8 to row 7, yielding

$$\left[\begin{array}{ccccccccc|ccccccccc} 1&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&1&1&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0 \end{array}\right],$$

and this is a check matrix in standard form.

10.58

For Figure 10.13:

See Exercise 4.34.

For Figure 10.14:

The action of the first circuit is the same as the one shown in Figure 10.13. The action of the second circuit on a state $|\Psi\rangle \equiv |0\rangle (a|+\rangle + b|-\rangle)$ is

$$\begin{aligned} |\Psi\rangle &\xrightarrow{I\otimes H} |0\rangle (a|0\rangle + b|1\rangle) \\ &\xrightarrow{CX_{(2,1)}} a|00\rangle + b|11\rangle \\ &\xrightarrow{I\otimes H} a|0\rangle|+\rangle + b|1\rangle|-\rangle . \end{aligned}$$

This is the same state before measurement that we obtain using the first circuit, so they are equivalent.

For Firgure 10.15:

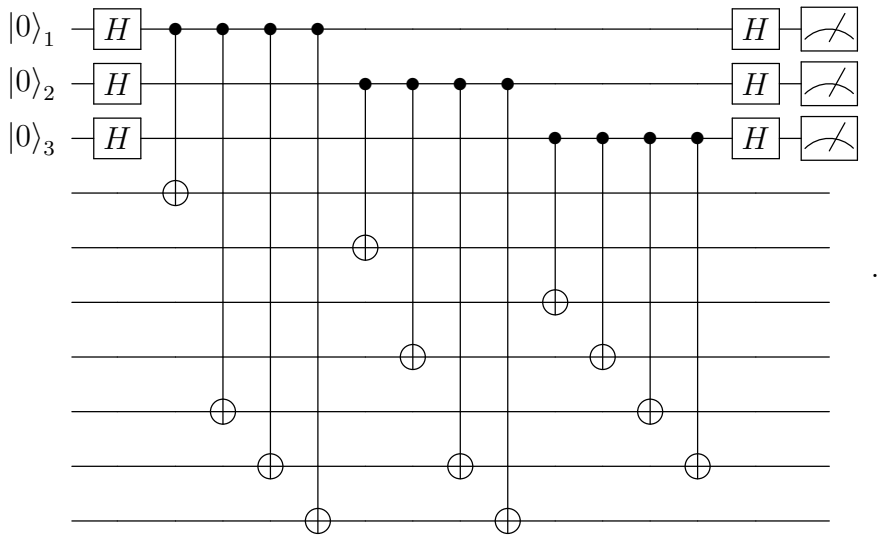
The action os the first circuit is the same as the one shown in Figure 10.13. The action of the second circuit on a state $|\Phi\rangle \equiv |0\rangle (c|0\rangle + d|1\rangle)$ is

$$|\Psi\rangle \xrightarrow{CX_{(2,1)}} a|0\rangle|0\rangle + b|1\rangle|1\rangle .$$

This is the same state before measurement that we obtain using the first circuit, so they are equivalent.

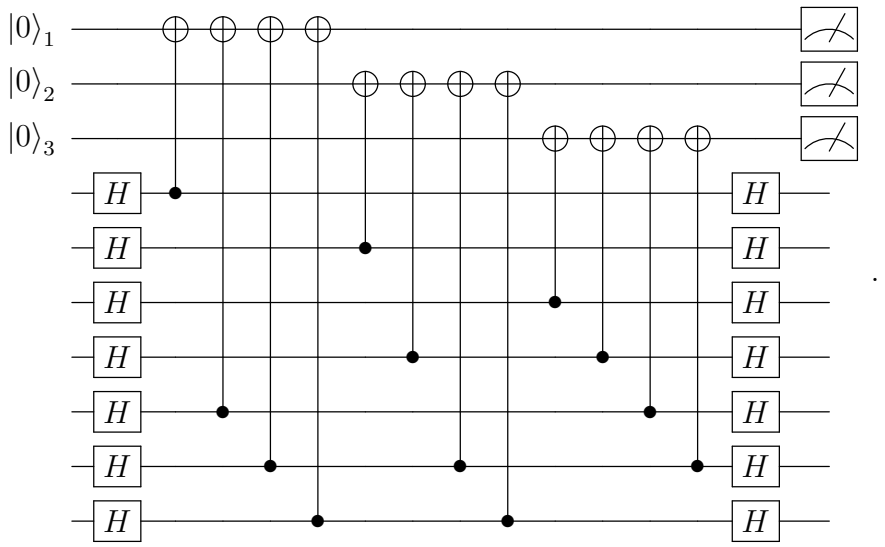
10.59

Let us first take the operations involving only the first three ancillas. Writing the CNOT gates explicitly yields

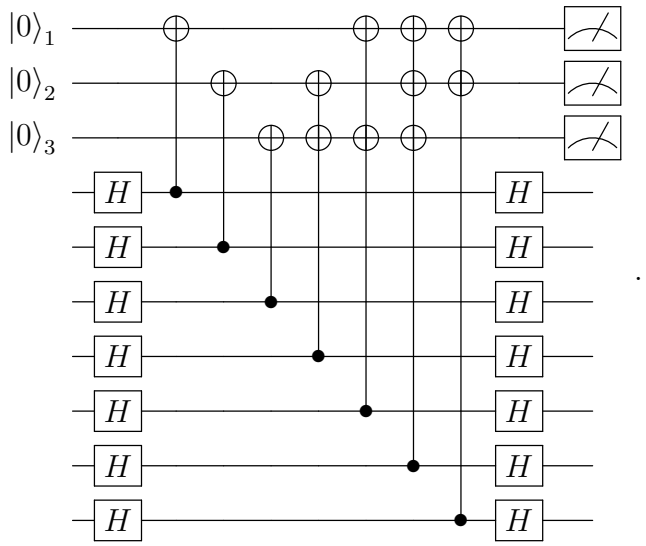


.

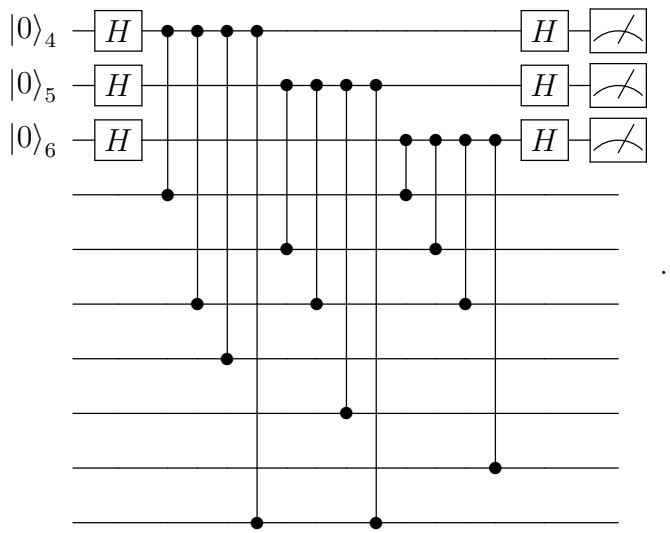
Now, using the identity in Figure 10.14 for each CNOT operation we get



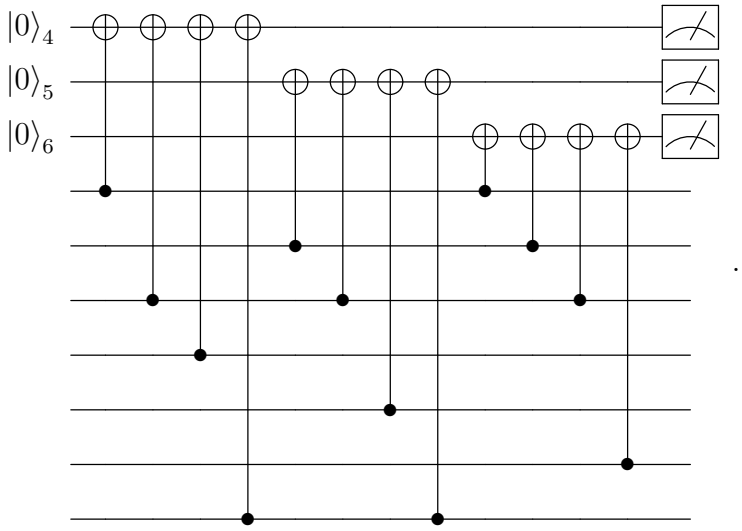
All these CNOT operations commute. Thus, rearranging the order and combining operations that have the same control qubit we obtain



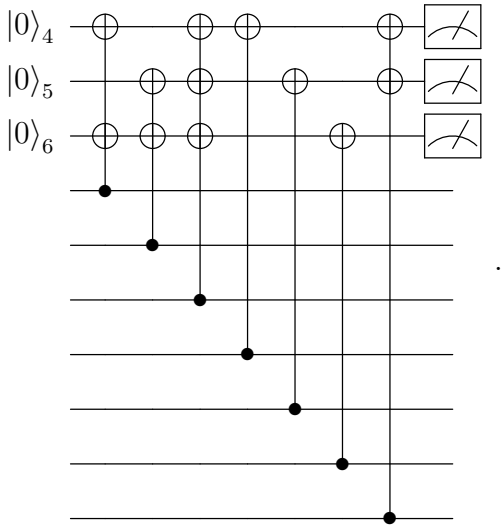
Let us now look at the operations involving the last three ancillas. Writing the Controlled-Z operations explicitly yields



Now, using the identity in Figure 10.15 for each Controlled-Z operation we get



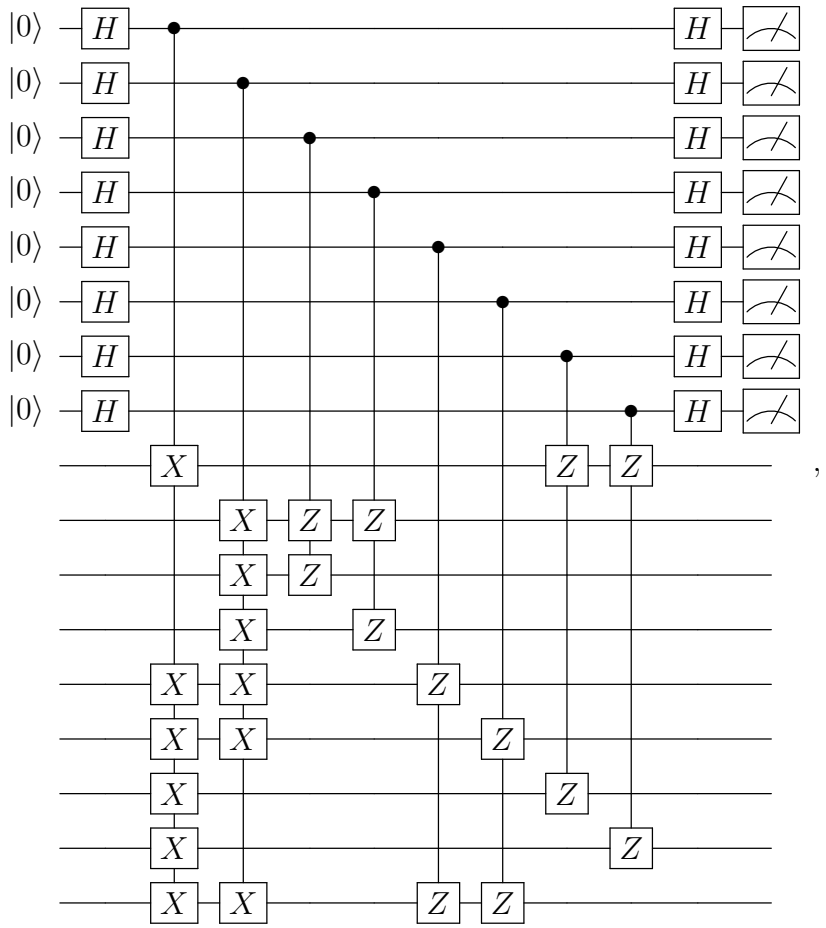
Analogously to the other circuit, we can rearrange the operations and combine those that have the same control qubit, yielding



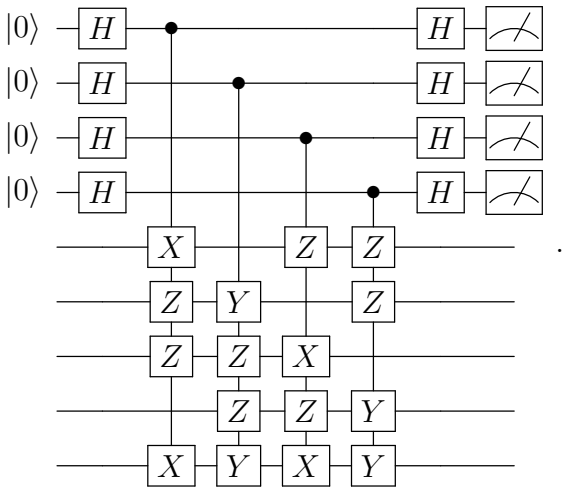
Combining both results into a single circuit, we obtain the circuit of Figure 10.17.

10.60

We can directly use the check matrices in standard form obtained in Exercise 10.57. For the nine qubit code, we get



and for the five qubit code we get



10.61

It is more insightful to use the circuit of Figure 10.17, equivalent to the one shown in Figure 10.16 (see Exercise 10.59). Notice that all qubits serve as control qubits for exactly two controlled operations: one in the middle of Hadamard gates and the other not. The system in logic state $|\psi\rangle$ is encoded, so no errors occurring means all control operations have no effect, so the result of the

array of error syndromes would be $(+1,+1,+1,+1,+1,+1)$. Now, from the relations $HXH = Z$, $HZH = X$, and $HYH = -Y$, we see that if a bit flip error occurs in one qubit, then the initial state for the circuit will be some $X_i |\psi\rangle$ instead of $|\psi\rangle$, then after the first Hadamard gate, the state to be used as control will be $HX_i |\psi\rangle = Z_i H |\psi\rangle$. The Z_i operation will have no effect over the controlled operation, so the target ancilla qubits will not be altered. Then after going through the second Hadamard gate, the control state will be $HZ_iH |\psi\rangle = X_i |\psi\rangle$, meaning the second control operation will flip the target ancilla qubits, and the error syndrome for this error will consist of -1 in the qubits that are the target of the second operation controlled by the i-th system qubit. Analogously, if a phase flip error occurs in one qubit, the initial state will be $Z_i |\psi\rangle$, and the state will be $X_i H |\psi\rangle$ during the first controlled operation, meaning the target ancilla qubits will be flipped. After the second Hadamard, the state will be $Z_i |\psi\rangle$, which does nothing to the target ancilla qubits, so now the error syndrome will consist of -1 in the qubits that are the target of the first operation controlled by the i-th system qubit. Naturally, if both errors occur, the initial state will be proportional to $Y_i |\psi\rangle$, which will affect both controlled operations, so the syndrome would consist of -1 in all qubits targeted by the controlled operations that have the i-th qubit as control.

As an example, let us analyze the syndrome for the case when the first qubit is affected by errors. If it is a bit flip error, ancilla qubits 4 and 6 are flipped, so the syndrome is $(+1,+1,+1,-1,+1,-1)$, and the correction operation is X_1. If it is a phase flip error, ancilla qubit 1 is flipped, so the syndrome is $(-1,+1,+1,+1,+1,+1)$, and the correction operation is Z_1, and if both errors occur, the syndrome is just both cases combined: $(-1,+1,+1,-1,+1,-1)$, and the correction is X_1Z_1, up to global phase. Applying the same logic to the other qubits, we can construct the table

error syndrome	correction operator	error syndrome	correction operator
$(+1,+1,+1,+1,+1,+1)$	not needed	$(+1,-1,-1,+1,+1,+1)$	Z_4
$(+1,+1,+1,-1,+1,-1)$	X_1	$(+1,-1,-1,-1,+1,+1)$	X_4Z_4
$(-1,+1,+1,+1,+1,+1)$	Z_1	$(+1,+1,+1,+1,-1,+1)$	X_5
$(-1,+1,+1,-1,+1,-1)$	X_1Z_1	$(-1,+1,-1,+1,+1,+1)$	Z_4
$(+1,+1,+1,+1,-1,-1)$	X_2	$(-1,+1,-1,+1,-1,+1)$	X_5Z_5
$(+1,-1,+1,+1,+1,+1)$	Z_2	$(+1,+1,+1,+1,+1,-1)$	X_6
$(+1,-1,+1,+1,-1,-1)$	X_2Z_2	$(-1,-1,-1,+1,+1,+1)$	Z_6
$(+1,+1,+1,-1,-1,-1)$	X_3	$(-1,-1,-1,+1,+1,-1)$	X_6Z_6
$(+1,+1,-1,+1,+1,+1)$	Z_3	$(+1,+1,+1,-1,-1,+1)$	X_7
$(+1,+1,-1,-1,-1,-1)$	X_3Z_3	$(-1,-1,+1,+1,+1,+1)$	Z_7
$(+1,+1,+1,-1,+1,+1)$	X_4	$(-1,-1,+1,-1,-1,+1)$	X_7Z_7

10.62

Let the $[n_1, 1]$ stabilizer code have generators $\{g_1, \cdots, g_{n_1-1}\}$, and the $[n_2, 1]$ stabilizer code have generators $\{h_1, \cdots, h_{n_2-1}\}$. After the concatenation, the fully encoded states must be stabilized by all generators $\{g_1 \otimes h_1, \cdots, g_1 \otimes h_{n_2-1}, g_2 \otimes h_1, \cdots, g_2 \otimes h_{n_2-1}, \cdots, g_{n_1-1} \otimes h_1, \cdots, g_{n_1-1} \otimes h_{n_2-1}\}$ in addition to the original ones, which would then be $\{g_1 \otimes I, \cdots, g_{n_1-1} \otimes I\}$ and $\{I \otimes h_1, \cdots, I \otimes h_{n_2-1}\}$. This gives us a total of $(n_1-1)+(n_2-1)+(n_1-1)(n_2-1) = n_1n_2-1$ generators, which corresponds to an $[n_1n_2, 1]$ stabilizer code.

10.63

Given that $\bar{Z}$ and $\bar{X}$ act as logical Z and X operations respectively, and knowing the identities $\bar{H}\bar{Z}\bar{H}^\dagger = \bar{X}$, and $\bar{H}\bar{X}\bar{H}^\dagger = \bar{Z}$, we conclude that U acts as a logical Hadamard gate up to a global phase, that is, $U = e^{i\theta}\bar{H}$ for some θ, therefore its action on the logical basis up to global phase is

$$U\left|0_L\right\rangle = \frac{\left|0_L\right\rangle + \left|1_L\right\rangle}{\sqrt{2}}, \quad \text{and} \quad U\left|1_L\right\rangle = \frac{\left|0_L\right\rangle - \left|1_L\right\rangle}{\sqrt{2}}.$$

10.64

Let qubit 1 be the control and qubit 2 be the target. Using the stabilizer formalism we know that $CX_{(1,2)}Z_2CX_{(1,2)} = Z_1Z_2$ (see Exercise 10.36). Thus if a Z_2 error occurs before the application of the CNOT, the actual operator applied is $Z_2CX_{(1,2)} = CX_{(1,2)}Z_1Z_2$. Therefore, it is equivalent to the CNOT being applied correctly, followed by an error on both qubits, so a Z error on the target qubit propagates to the control qubit when a CNOT is applied.

Using circuits identities, we have that $CX_{(1,2)}\left|\pm\right\rangle\left|+\right\rangle = \left|\pm\right\rangle\left|+\right\rangle$ and $CX_{(1,2)}\left|\pm\right\rangle\left|-\right\rangle = \left|\mp\right\rangle\left|-\right\rangle$ (see Exercise **??**). That is, while X acts as a bit flip on the Z basis, Z acts as a bit flip on the X basis with the roles of control and target exchanged. As it can be seen from these results, if the target is in the $\left|+\right\rangle$ state, nothing happens, but if it is in the $\left|-\right\rangle$ state, then the control is flipped. Therefore, a Z error occurring on the target qubit propagates to the control qubit when a CNOT gate is applied.

10.65

Let $\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$. For the first circuit we get

$$\begin{aligned}
\left|0\right\rangle\left|\psi\right\rangle &\xrightarrow{CX_{(2,1)}} a\left|00\right\rangle + b\left|11\right\rangle \\
&\xrightarrow{I\otimes H} \left(\frac{a\left|0\right\rangle + b\left|1\right\rangle}{\sqrt{2}}\right)\left|0\right\rangle + \left(\frac{a\left|0\right\rangle - b\left|1\right\rangle}{\sqrt{2}}\right)\left|1\right\rangle \\
&\xrightarrow{\text{measurement qubit 2}} \begin{cases} \left(a\left|0\right\rangle + b\left|1\right\rangle\right)\left|0\right\rangle & \text{if outcome is } +1; \\ \left(a\left|0\right\rangle - b\left|1\right\rangle\right)\left|1\right\rangle & \text{if outcome is } -1; \end{cases} \\
&\xrightarrow{Z\otimes I \text{ [if } -1]} \left|\psi\right\rangle\left|0\right\rangle \text{ or } \left|\psi\right\rangle\left|1\right\rangle.
\end{aligned}$$

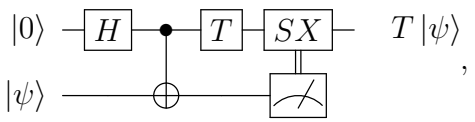
For the second circuit we get

$$\begin{aligned}
\left|0\right\rangle\left|\psi\right\rangle &\xrightarrow{H\otimes I} \left(\frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right)\left(a\left|0\right\rangle + b\left|1\right\rangle\right) \\
&\xrightarrow{CX_{(1,2)}} \left(\frac{a\left|0\right\rangle + b\left|1\right\rangle}{\sqrt{2}}\right)\left|0\right\rangle + \left(\frac{a\left|1\right\rangle + b\left|0\right\rangle}{\sqrt{2}}\right)\left|1\right\rangle \\
&\xrightarrow{\text{measurement qubit 2}} \begin{cases} \left(a\left|0\right\rangle + b\left|1\right\rangle\right)\left|0\right\rangle & \text{if outcome is } +1; \\ \left(a\left|1\right\rangle + b\left|0\right\rangle\right)\left|1\right\rangle & \text{if outcome is } -1; \end{cases} \\
&\xrightarrow{X\otimes I \text{ [if } -1]} \left|\psi\right\rangle\left|0\right\rangle \text{ or } \left|\psi\right\rangle\left|1\right\rangle.
\end{aligned}$$

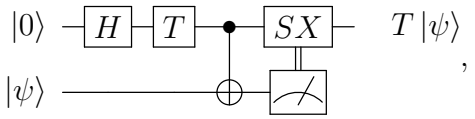
10.66

**From errata:* $TX = exp(-i\pi/4)SX$ should be $TXT^\dagger = exp(-i\pi/4)SX$.

If the measurement outcome is $+1$, then X is not applied to the first qubit, and thus we can obviously commute the operation controlled by the classical qubit with T. If the outcome is -1, we can use the first relation to write $TX = \exp(-i\pi/4)SXT$. Therefore, for all cases we conclude that the circuit is equivalent to



and using the second relation we get



which is the circuit of Figure 10.25.

10.67

Considering the initial state as a (normalized) superposition of all four possibilities for the control qubits 1 and 2 with the target qubit 3, given by $|\Psi\rangle = (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle)\,|\psi\rangle$, for the first relation we obtain

$$\begin{aligned}
\text{left-hand side:}\quad |\Psi\rangle &\xrightarrow{X\otimes I\otimes I} (a\,|10\rangle + b\,|11\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle \\
&\xrightarrow{CCX_{(1,2,3)}} (a\,|10\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle\,;
\end{aligned}$$

$$\begin{aligned}
\text{right-hand side:}\quad |\Psi\rangle &\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)\,|\psi\rangle + d\,|11\rangle\,X\,|\psi\rangle \\
&\xrightarrow{X_1\otimes CX_{(2,3)}} (a\,|10\rangle + c\,|00\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle + d\,|01\rangle\,X^2\,|\psi\rangle \\
&= (a\,|10\rangle + c\,|00\rangle + d\,|01\rangle)\,|\psi\rangle + b\,|11\rangle\,X\,|\psi\rangle\,.
\end{aligned}$$

For the second relation we get

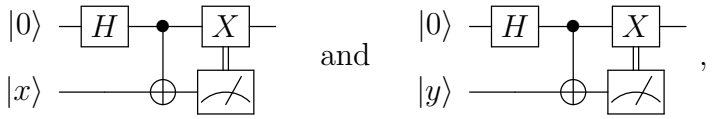
$$\begin{aligned}
\text{left-hand side:}\quad |\Psi\rangle &\xrightarrow{I\otimes I\otimes Z} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle)Z\,|\psi\rangle \\
&\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle + d\,|11\rangle\,XZ\,|\psi\rangle
\end{aligned}$$

$$\begin{aligned}
\text{right-hand side:}\quad |\Psi\rangle &\xrightarrow{CCX_{(1,2,3)}} (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)\,|\psi\rangle + d\,|11\rangle\,X\,|\psi\rangle \\
&\xrightarrow{CZ_{(1,2)}\otimes Z_3} (a\,|0\rangle\,|0\rangle + b\,|0\rangle\,|1\rangle + c\,|1\rangle\,Z\,|0\rangle)Z\,|\psi\rangle + d\,|1\rangle\,Z\,|1\rangle\,ZX\,|\psi\rangle \\
&= (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle - d\,|11\rangle\,ZX\,|\psi\rangle \\
&= (a\,|00\rangle + b\,|01\rangle + c\,|10\rangle)Z\,|\psi\rangle + d\,|11\rangle\,XZ\,|\psi\rangle\,.
\end{aligned}$$

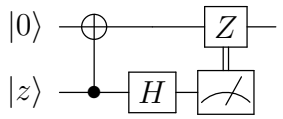
Therefore both circuit identities hold.

10.68

(1) The parts of the circuit involving the first two pairs of ancilla-system qubits $|0\rangle|x\rangle$ and $|0\rangle|y\rangle$, before the final Toffoli gate, can be written as

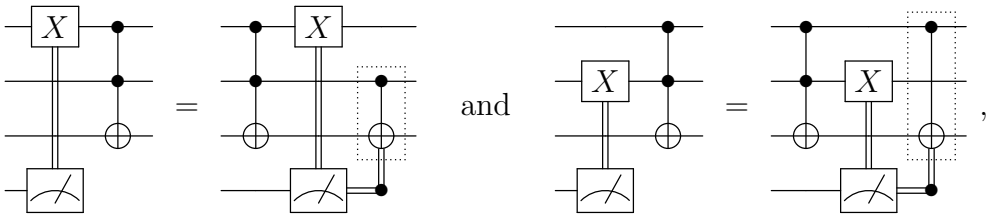


and the part involving the last pair $|0\rangle|z\rangle$ can be written as

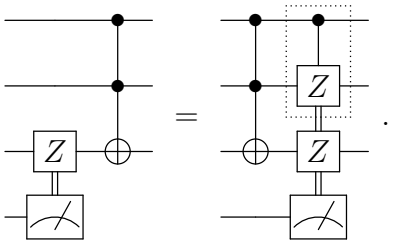


These circuits result, respectively, in the transformations $|0\rangle \to |x\rangle$, $|0\rangle \to |y\rangle$, and $|0\rangle \to |z\rangle$ (see Exercise 10.65). Therefore the circuit indeed implements a SWAP operation of the state $|x\rangle|y\rangle|z\rangle$ to the three qubits originally in the state $|000\rangle$, followed by a final Toffoli gate on these qubits.

(2) Using circuit identity (a) of Exercise 10.67, we get

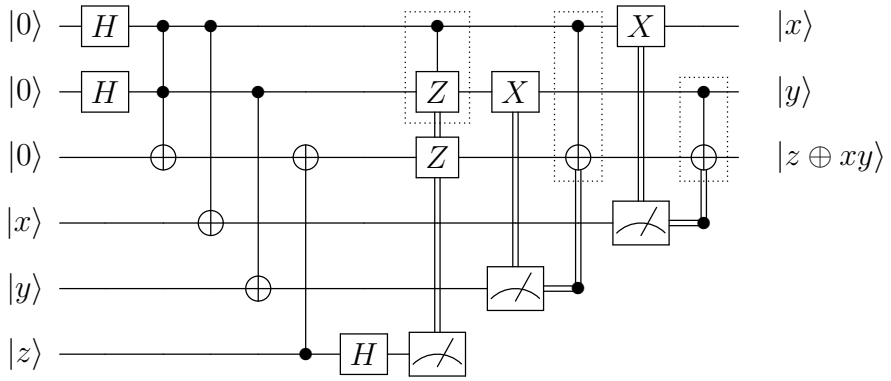


and using identity (b), we get



After the three gates controlled by the measurement outcomes, the Toffoli gate commutes the CNOT gate that has the third ancilla qubit as target, and naturally commutes with the other two CNOT gates, since the first two ancilla qubits are just control qubits for both the Toffoli and the CNOT

gates. So we end up with the circuit



(3) Assuming the operation $CCX_{(1,2,3)}(H \otimes H \otimes I)$ in the ancilla subspace can be implemented fault-tolerantly, the remaining operations are all Hadamard and CNOT gates, which can be implemented fault-tolerantly, and controlled-Z gates, which can be constructed using only Hadamard and CNOT gates, and can therefore, by extension, also be applied fault-tolerantly. Hence, this circuit can be used to obtain a fault-tolerant Toffoli gate.

10.69

If there are any X or Y errors resulting from the preparations, they are detected during the verification step, and the process starts over. So the only errors after the preparation that survive are Z errors on one ancilla qubit. Similarly, if any X or Y errors occur in the extra qubits or ancilla qubits during the verification step, they will result in the wrong parity after measuring the extra qubits, and the process also starts over. The only errors that survive are Z errors, which propagate as Z_iZ_j $(i \neq j)$, considering the faulty extra qubit was connected with CNOT gates to the i-th and j-th ancilla qubits, or just as Z_i errors, considering the faulty qubit was one of the ancilla. So we can identify two possible scenarios: 1. A Z_i error in the ancilla system due to a failure during the preparation or verification step; 2. A Z_iZ_j error due to a failure in the verification step. Let us analyze the ancilla output for the two possibilities.

1. Z_i error:

   If $i = 1$, the error propagates as $Z_1 \to X_1$ after the Hadamard gate application, and if $i \neq 1$, then it propagates as $Z_i \to Z_1Z_i$ after the CNOT operation, then as $Z_1Z_i \to X_1Z_i$ after the Hadamard operation. In any case, there is at most one X error in the ancilla output.

2. Z_iZ_j error $(i \neq j)$:

   If $i = 1$, the error propagates as $Z_1Z_j \to Z_1^2Z_j = Z_j$ after the CNOT operation, and if both i and j are not 1 then the error propagates as $Z_iZ_j \to Z_1^2Z_iZ_j = Z_iZ_j$ after the CNOT operations. In any case, there are no X or Y errors in the ancilla output.

The single X error can also be a Y error if the Z_i error is not a full phase flip, but an arbitrary relative phase error.

10.70

A Z error in the ancilla will cause the cat state to be $|0\cdots0\rangle - |1\cdots1\rangle$ instead of $|0\cdots0\rangle + |1\cdots1\rangle$, that is, it only introduces a relative phase. All controlled operations are indifferent to relative phases, since they only depend on whether the control qubit has a $|1\rangle$ component or not, so the qubits in the code are not affected. For the ancilla system, however, if the Z error occurred in the first qubit, then the error propagates as $Z_1 \to X_1$ after the Hadamard operation, and if it occurs in any of the other ancilla qubits, say, the i-th, then it propagates as $Z_i \to X_1 Z_i$ after the CNOT and Hadamard operations. In any case, the final measurement will be affected.

10.71

-

10.72

-

10.73

-

10.74

-