Exercise 10.1

Let $|\psi\rangle = a|0\rangle + b|1\rangle$ and the initial state be $|\psi_0\rangle = a|000\rangle + b|100\rangle$.
Applying a CNOT to the first two qubits we get,
$|\psi_1\rangle = a|000\rangle + b|110\rangle$
Applying a CNOT to the first and last qubits we get,
$|\psi_2\rangle = a|000\rangle + b|111\rangle$

Exercise 10.2

$P_\pm = \frac{1}{2}(|0\rangle \pm |1\rangle)(\langle 0| \pm \langle 1|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| \pm |1\rangle\langle 0| \pm |0\rangle\langle 1|) = \frac{1}{2}(I \pm X)$
Therefore,
$\mathcal{E}(\rho) = (1-2p)\rho + 2pP_+\rho P_+ + 2pP_-\rho P_- = (1-2p)\rho + \frac{1}{2}p(I+X)\rho(I+X) + \frac{1}{2}p(I-X)\rho(I-X) = (1-2p)\rho + p\rho + pX\rho X = (1-p)\rho + pX\rho X$

Exercise 10.3

$Z_2Z_3Z_1Z_2 = [I \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)][(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I] = \underbrace{|000\rangle\langle 000| + |111\rangle\langle 111|}_{P_0} - (\underbrace{|100\rangle\langle 100| + |011\rangle\langle 011|}_{P_1})$

$+ \underbrace{|010\rangle\langle 010| + |101\rangle\langle 101|}_{P_2} - (\underbrace{|001\rangle\langle 001| + |110\rangle\langle 110|}_{P_3})$

Exercise 10.4

1)$|000\rangle\langle 000|$, $|111\rangle\langle 111|$: no bit flip
$|100\rangle\langle 100|$, $|011\rangle\langle 011|$: first bit flipped
$|010\rangle\langle 010|$, $|101\rangle\langle 101|$: second bit flipped
$|001\rangle\langle 001|$, $|110\rangle\langle 110|$: third bit flipped
2) If our state is $|\psi\rangle = a|000\rangle + b|111\rangle$, then the measurement will collapse the state into $|000\rangle$ or $|111\rangle$ with probabilities $|a|^2$ or $|b|^2$, respectively. Hence, only the computational basis states $|000\rangle$ and $|111\rangle$ can be corrected.
3)Assuming the initial state is $|000\rangle$ the probability that one or fewer bit flips occur is $(1-p)^3 + p(1-p)^2$, hence $F \geq \sqrt{(1-p)^3 + p(1-p)^2}$.

Exercise 10.5

Assuming no more than one error has occurred, $X_1X_2X_3X_4X_5X_6$ will be 1 if no phase flip occurred and -1 and if one occurred on the first or second block. Identically for $X_4X_5X_6X_7X_8X_9$. Hence, if both give -1 the error is on the second block, otherwise it's on the first block if $X_1X_2X_3X_4X_5X_6$ gives -1 and on the third block if $X_4X_5X_6X_7X_8X_9$ gives -1. If both give 1 then no error has occurred.

Exercise 10.6

The eigenvalues of Z are ± 1, hence
$Z_1Z_2Z_3(|000\rangle - |111\rangle) = |000\rangle - (-1)^3|111\rangle = |000\rangle + |111\rangle$

Exercise 10.7

Need to prove that $PE_i^\dagger E_j P = \alpha_{ij} P$. I and X are Hermitian, hence suffices to show for IX_1,II,X_1X_1 and X_1X_2.
$P\sqrt{(1-p)^3}I\sqrt{p(1-p)^2}X_1P = (1-p)^2\sqrt{p(1-p)}(|000\rangle\langle 000|+|111\rangle\langle 111|)X_1(|000\rangle\langle 000|+|111\rangle\langle 111|) = (1-p)^2\sqrt{p(1-p)}(|000\rangle\langle 000|+|111\rangle\langle 111|)(|100\rangle\langle 000|+|011\rangle\langle 111|) = 0$
$P\sqrt{(1-p)^3}I\sqrt{(1-p)^3}IP = (1-p)^3PP = (1-p)^3P$
$P\sqrt{p(1-p)^2}X_1\sqrt{p(1-p)^2}X_1P = p(1-p)^2PIP = p(1-p)^2P$
$P\sqrt{p(1-p)^2}X_1\sqrt{p(1-p)^2}X_2 = p(1-p)^2(|000\rangle\langle 000|+|111\rangle\langle 111|)(|110\rangle\langle 000|+|001\rangle\langle 111|) = 0$
Hence, the quantum error-correction conditions are satisfied.

Exercise 10.8

$P = |+++\rangle\langle +++| + |---\rangle\langle ---|$, hence like in the previous exercise.
$PE_i^\dagger E_jP = 0$, $i \neq j$
$PE_i^\dagger E_jP = P$, $i = j$
Hence, the quantum error-correction conditions are satisfied.

Exercise 10.9

$PIIP = P$
$PIP_1P = (|+++\rangle\langle +++|+|---\rangle\langle ---|)(|0\rangle\langle 0|\otimes I\otimes I)(|+++\rangle\langle +++|+|---\rangle\langle ---|) = (|+++\rangle\langle +++|+|---\rangle\langle ---|)\frac{1}{\sqrt{2}}(|0++\rangle\langle +++|+|0--\rangle\langle ---|) = \frac{1}{2}(|+++\rangle\langle +++|+|---\rangle\langle ---|) = \frac{1}{2}P$
Identically,
$PIQ_1P = \frac{1}{2}P$
$PP_1Q_1 = 0$
$PP_1P_1P = PP_1P = \frac{1}{2}P$
$PQ_1Q_1P = PQ_1P = \frac{1}{2}P$
$PP_1P_2P = (|+++\rangle\langle +++| + |---\rangle\langle ---|)(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I)(|+++\rangle\langle +++| + |---\rangle\langle ---|) = (|+++\rangle\langle +++|+|---\rangle\langle ---|)\frac{1}{2}(|00+\rangle\langle +++|+|00-\rangle\langle ---|) = \frac{1}{4}(|+++\rangle\langle +++| + |---\rangle\langle ---|) = \frac{1}{4}P$
$PP_1Q_2P = (|+++\rangle\langle +++| + |---\rangle\langle ---|)(|0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes I)(|+++\rangle\langle +++| + |---\rangle\langle ---|) = (|+++\rangle\langle +++|+|---\rangle\langle ---|)\frac{1}{2}(|01+\rangle\langle +++|-|01-\rangle\langle ---|) = \frac{1}{4}(|+++\rangle\langle +++| + |---\rangle\langle ---|) = \frac{1}{4}P$
Hence, the quantum error-correction conditions are satisfied.

Exercise 10.10

$P = |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$
Due to phase and bit flips,
$PIX_iP = PIY_iP = PIZ_iP = 0$
$PIIP = PX_iX_iP = PY_iY_iP = PZ_iZ_iP = P$
The X_i and Y_i change the individual qubits, hence if $i \neq j$ $PX_iY_jP = 0$, e.g. for PX_1Y_2P looking at the first triplet, we have
$(\langle 000| + \langle 111|)i(|110\rangle - |001\rangle) = 0$
$X_iY_i = iZ_i$, hence $PX_iY_iP = 0$
For Z_iZ_j if i and j belong to different triplets then we have a phase flip on 2 separate triplets,

hence $PZ_iZ_jP = 0$.
However, if i and j are in the same triplet, then we apply 2 phase shifts to the triplet which is equivalent to no change, hence $PZ_iZ_jP = P$.
For X_iZ_j and Y_iZ_j we perform a bit and phase flip, hence for all i and j $PX_iZ_jP = PY_iZ_jP = 0$.

Exercise 10.11

$\mathcal{E}(\rho) = \frac{I}{2}$
Consider the operation elements found for the general depolarizing channel in Exercise 8.19 $\{\sqrt{\frac{p}{d}}\,|i\rangle\langle j|\}$. Taking $p = 1$ and $d = 2$, we get $\{\frac{1}{2}|0\rangle\langle 0|, \frac{1}{2}|1\rangle\langle 1|, \frac{1}{2}|0\rangle\langle 1|, \frac{1}{2}|1\rangle\langle 0|\}$.

Exercise 10.12

$F(|0\rangle, \mathcal{E}(|0\rangle\langle 0|)) = \sqrt{\langle 0|\,\mathcal{E}(|0\rangle\langle 0|)\,|0\rangle}$
$= \sqrt{\langle 0|\,((1-p)|0\rangle\langle 0| + \frac{p}{3}(X|0\rangle\langle 0|X + Y|0\rangle\langle 0| + Z|0\rangle\langle 0|Z))\,|0\rangle} = \sqrt{1-p+\frac{p}{3}} = \sqrt{1-\frac{2p}{3}}$
As the depolarizing channel is symmetric, for any pure state $|\psi\rangle$,
$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{1-\frac{2p}{3}}$.
As fidelity is jointly concave, for any ρ and some $|\psi\rangle$ we have,
$F(\rho, \mathcal{E}(\rho)) \geq F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{1-\frac{2p}{3}}$

Exercise 10.13

Let $|\psi\rangle = a|0\rangle + b|1\rangle$
$F(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = \sqrt{\langle\psi|\,\mathcal{E}(|\psi\rangle\langle\psi|)\,|\psi\rangle}$
$\sqrt{|\langle\psi|E_0|\psi\rangle|^2 + |\langle\psi|E_1|\psi\rangle|^2} = \sqrt{||a|^2 + |b|^2\sqrt{1-\gamma}|^2 + |a|b|^2\sqrt{\gamma}|^2}$
Minimum will occur when $a = 0$ and $b = 1$, hence
$F_{min}(|\psi\rangle, \mathcal{E}(|\psi\rangle\langle\psi|)) = F(|1\rangle, \mathcal{E}(|1\rangle\langle 1|)) = \sqrt{1-\gamma}$

Exercise 10.14

G will be a $rk \times k$ matrix.

$$G = rk\left\{\begin{bmatrix} 1 & 0 & \dots & 0 \\ r\vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}\right.$$

Exercise 10.15

Let c_1 and c_2 be columns of G. Then
$G = [c_1|c_2|G']$
$G'' = [c_1|c_1 + c_2|G']$
Let $x = (x_1, x_2, \ldots, x_n)$.
$Gx = c_1x_1 + c_2x_2 + \ldots$
$G''x = c_1x_1 + (c_1 + c_2)x_2 + \ldots$
$G''x - Gx = c_1x_2 \in C$
Therefore, as C is linear with G as generator, G'' is a generator for C as well, as the difference of the two codes is still in C.

Exercise 10.16

Let r_1 and r_2 be rows of H. Then

$$H = \begin{bmatrix} r_1 \\ \hline r_2 \\ \hline H' \end{bmatrix}$$

$$H'' = \begin{bmatrix} r_1 \\ \hline r_1 + r_2 \\ \hline H' \end{bmatrix}$$

Let $x = (x_1, x_2, \ldots, x_n)$.

$$Hx = \begin{bmatrix} r_1x \\ r_2x \\ \vdots \end{bmatrix} = 0$$

Therefore, $r_1x = r_2x = 0$. Hence,

$$H''x = \begin{bmatrix} r_1x \\ r_1x + r_2x \\ \vdots \end{bmatrix} = 0$$

Hence, H'' is a parity check matrix for the same code.

Exercise 10.17

$y_1 = (1, 1, 1, 0, 0, 0)$, $y_2 = (0, 0, 0, 1, 1, 1)$, hence we can take y_3 to y_6 as,
$y_3 = (1, 1, 0, 0, 0, 0)$
$y_4 = (1, 0, 1, 0, 0, 0)$
$y_5 = (0, 0, 0, 0, 1, 1)$
$y_6 = (0, 0, 0, 1, 0, 1)$
Therefore,

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

Exercise 10.18

Let x be an arbitrary message to be encoded. Then,
$y = Gx \in C$
Hence, $HGx = Hy = 0$ for $\forall x$
Hence, $HG = 0$

Exercise 10.19

Using that $HG = 0$ we have,

$$HG = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1k} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \\ a_{(n-k)1} & a_{(n-k)2} & \dots & a_{(n-k)k} & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1k} \\ \vdots & \vdots & \vdots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nk} \end{bmatrix} = 0$$

Hence,

$$\sum_{i \leq k} a_{1i} b_{i1} + b_{(k+1)1} = 0 \dots \sum_{i \leq k} a_{(n-k)i} b_{i1} + b_{n1} = 0$$

$$\vdots$$

$$\sum_{i \leq k} a_{1i} b_{ik} + b_{(k+1)k} = 0 \dots \sum_{i \leq k} a_{(n-k)i} b_{ik} + b_{nk} = 0$$

We see that for example, taking for $2 \leq i \leq k$ $b_{i1} = 0$, $b_{11} = 1$ and $b_{(k+1)1} = -a_{11}$ gives a solution.
Therefore for $i, j \leq k$ $b_{ij} = \delta_{ij}$ and for $i, j > k$ $b_{ij} = -a_{(i-k)j}$, i.e.

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

Exercise 10.20

Let x be a codeword such that $\mathrm{wt}(x) \leq d-1$. Let $H = c_1|c_2 \dots c_n$ for code C. Consider Hx,
$Hx = \sum_i c_i x_i$ for $d-1$ columns. Therefore, as any $d-1$ columns are linearly independent, this sum cannot equal 0. Hence, $d(C) \geq d$. However, as any d columns are linearly dependant there exists a codeword y with $\mathrm{wt}(y) = d$ such that $Hy = 0$. Therefore, $d(C) = d$.

Exercise 10.21

The parity check matrix is a $n-k$ by n matrix, hence the maximum number of linearly independent columns is $n-k$. Therefore, from Exercise 10.20 $n-k \geq d-1$.

Exercise 10.22

The Hamming parity check matrix is constructed from columns which are all the possible $n-k$ bit strings, of which there are $2^r - 1$ of excluding the 0 string. Hence, any two columns will be linearly independent as all are different, however there always will be 3 linearly dependant columns, e.g. $(1, 0, 0, \dots)$, $(0, 1, 0, \dots)$ and $(1, 1, 0, \dots)$. Therefore, as per exercise 10.20 the code will have distance 3.

Exercise 10.23

Exercise 10.24

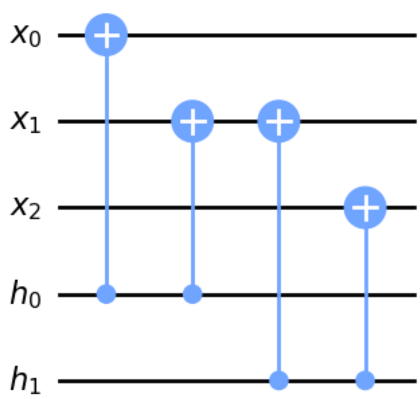
If $C^\perp \subseteq C$, $\forall x\ y = Gx \in C^\perp$ and $G^T = H^\perp$. Hence, $\forall x\ G^T Gx = H^\perp y = 0$, i.e. $G^T G = 0$.
If $G^T G = 0$, $\forall x\ G^T Gx = H^\perp y = 0$, therefore $y \in C^\perp$, hence $C^\perp \subseteq C$.

Exercise 10.25

$x = H^T z_0$
If $x \in C^\perp$,
$$\sum_{y \in C} (-1)^{x.y} = \sum_z (-1)^{(H^T z_0)^T Gz} = \sum_z (-1)^{z_0^T HGz} = \sum_z (-1)^0 = |C|$$
If $x \notin C^\perp$,
$$\sum_{y \in C} (-1)^{x.y} = \sum_z (-1)^{x^T Gz}$$
Let, $x^T G = z_1^T$, then
$$\sum_{y \in C} (-1)^{x.y} = \sum_z (-1)^{z_1.z}$$
As we're summing over all z, $z_1.z = 0$ or 1 both with probability $\frac{1}{2}$. Hence,
$$\sum_{y \in C} (-1)^{x.y} = 0$$

Exercise 10.26

To perform the transformation $|x\rangle |0\rangle \to |x\rangle |Hx\rangle$ we perform the following. Let $|x\rangle = |x_1, x_2, \ldots, x_n\rangle$ and $|0\rangle = |0_1, 0_2, \ldots, 0_m\rangle$. For each 0_i, consider the i^{th} row of H and for each column j which is 1 apply a CNOT between x_j and the 0_i with x_j the control. After, applying this for all the qubits of $|0\rangle$ we obtain the desired transformation. As an example here's the circuit for $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$,



Exercise 10.27

Consider a bit error e_1 and flip error e_2. We get,

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

Applying the parity matrix H_1 to $|x+C_2\rangle|0\rangle$ we get,

$$\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{u.y}(-1)^{(x+y+v).e_2}\left|x+y+v\right\rangle\left|H_1(v+e_1)\right\rangle$$

As v is known so is $H_1 v$, hence we can calculate the syndrome $H_1 e_1$. Therefore, removing the bit error we get,

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

Applying Hadamard gates to each qubit we get,

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

Let $e_2+z=z'+u$, then we have,

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

Using Exercise 10.25 we get,

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

Once again by knowing $H_2 u$ we calculate the syndrome $H_2 e_2$, where H_2 is the parity check matrix for $C_2^{\perp}$, and hence correct the error e_2 to get,

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

Applying the Hadamards again we get,

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

Hence, this has the same error-correcting properties as the $CSS(C_1,C_2)$.

Exercise 10.28

For the $[7,4,3]$ Hamming code we have,

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

$$HH[C_2]^T=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix}=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

Hence, $H[C_2]^T=G[C_1]$.

Exercise 10.29

Let $|x\rangle, |y\rangle \in V_S$, i.e. $\forall g \in S\ g|x\rangle = |x\rangle$ and $g|y\rangle = |y\rangle$. Consider $a|x\rangle + b|y\rangle$ for some a and b. As g are linear operators we have,
$g(a|x\rangle + b|y\rangle) = ag|x\rangle + bg|y\rangle = a|x\rangle + b|y\rangle$
Hence, $a|x\rangle + b|y\rangle \in V_S$.
Let $|x\rangle \in V_S \implies \forall g \in S\ g|x\rangle = |x\rangle \implies \forall g \in S\ |x\rangle \in V_g \implies |x\rangle \in \bigcap_{g\in S} V_G$

Exercise 10.30

Let $\pm iI \in S$ then as S is a group $(\pm iI)(\pm iI) \in S$, hence $-I \in S$, which is a contradiction therefore $\pm iI \notin S$.

Exercise 10.31

If g_i and g_j commute then all the elements of S commute, as S is generated by the g_i's. If all the elements of S commute then necessarily g_i and g_j also commute as they're elements of S.

Exercise 10.32

$g_1|0_L\rangle = \frac{1}{\sqrt{8}}(|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle + |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle) = |0_L\rangle$
Similarly, for g_2 and g_3.
For g_3 to g_6, each block has an even number of phase flips, hence overall no overall phase flip takes place.
Similarly as above for the $|1_L\rangle$.

Exercise 10.33

Let $r(g) = [\vec{x}|\vec{z}]$ and $r(g') = [\vec{x'}|\vec{z'}]$. Then,
$r(g)\Lambda r(g')^T = \vec{x}.\vec{z'} + \vec{z}.\vec{x'}$
If g and g' commute then in total there are even number of anti-commuting Pauli operators, hence the sum of the 2 scalar products mod 2 will be 0. If $r(g)\Lambda r(g')^T = 0$ then both scalar products will have to be 0 or 1, hence there are an even number of anti-commuting Pauli operators, hence g and g' commute.

Exercise 10.34

A counterexample is $S = < X, Z >$. $XZXZ = (-iY)(-iY) = -I$.

Exercise 10.35

Each g is a tensor product of Pauli operators with prefactors $\pm i$ or ± 1, hence $g^2 = \pm I$. However, $g^2 \in S$, but $-I \notin S$, therefore $g^2 = I$.

Exercise 10.36

$$UX_2U^\dagger = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} X & 0 \\ 0 & I \end{bmatrix} = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} = X_2$$

$$UZ_1U^\dagger = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & -X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} = Z_1$$

$$UZ_2U^\dagger = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} Z & 0 \\ 0 & Z \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} Z & 0 \\ 0 & -iY \end{bmatrix} = \begin{bmatrix} Z & 0 \\ 0 & -Z \end{bmatrix} = Z_1Z_2$$

Exercise 10.37

$$UY_1U^\dagger = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} 0 & -iI \\ iI & 0 \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}\begin{bmatrix} 0 & -iX \\ iI & 0 \end{bmatrix} = \begin{bmatrix} 0 & -iX \\ iX & 0 \end{bmatrix} = Y_1X_2$$

Exercise 10.38

Exercise 10.39

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

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

Exercise 10.40

1) First, consider $UZU^\dagger = Z$, for this to be true we require $U = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$. For this U we see that, $UXU^\dagger = \pm X, \pm Y$, with $e^{i\phi} = \pm 1, \pm i$. Therefore, we see that U can be constructed using only phase gates.
From Chapter 4 we know that for and Pauli operator σ there exists R constructed from Hadamards and phase gates, such that $R\sigma R^\dagger = Z$.
Let's consider a normalizer U for G_1. Then, $\exists g \in G_1$ such that $UgU^\dagger = Z$. Let $U = VR$, where R is defined as above. Then, $UgU^\dagger = VRgR^\dagger V^\dagger = VZV^\dagger = Z$, hence from above V consists of only phase gates and R consists of phase and Hadamard gates, therefore U consists of only phase and Hadamard gates.
Therefore, phase and Hadamard gates can be used to construct any normalizer one G_1.
2) Let the process described by the circuit be $\bar{U}$. We like to show $\langle a|\,\bar{U}\,|b\rangle\,|\psi\rangle = \langle a|\,U\,|b\rangle\,|\psi\rangle$ $\forall a, b, \psi$.
First we get the following from the conditions on U,
$UZ_1 = (X_1 \otimes g)U$
$X_1U = (I \otimes g)UZ_1 = gUZ_1$
$UX_1 = (Z_1 \otimes g')U$
$Z_1U = (I \otimes g')UX_1 = g'UX_1$
Now consider $U'\,|\psi\rangle$
$U'\,|\psi\rangle = \sqrt{2}\,\langle 0|\,U(|0\rangle\,|\psi\rangle) = \sqrt{2}\,\langle 0|\,X_1gUZ_1(|0\rangle\,|\psi\rangle) = \sqrt{2}\,\langle 1|\,gU(|0\rangle\,|\psi\rangle)$
$U'\,|\psi\rangle = \sqrt{2}\,\langle 0|\,Z_1g'UX_1(|0\rangle\,|\psi\rangle) = \sqrt{2}\,\langle 0|\,g'U(|1\rangle\,|\psi\rangle)$
$U'\,|\psi\rangle = \sqrt{2}\,\langle 1|\,Z_1gg'UX_1(|0\rangle\,|\psi\rangle) - \sqrt{2}\,\langle 1|\,gg'U(|1\rangle\,|\psi\rangle)$
Now consider, $\langle a|\,\bar{U}\,|b\rangle\,|\psi\rangle$.
$\langle 0|\,\bar{U}\,|0\rangle\,|\psi\rangle = \langle 0|\,\frac{1}{\sqrt{2}}(|0\rangle \otimes U'\,|\psi\rangle + |1\rangle \otimes gU'\,|\psi\rangle) = \frac{1}{\sqrt{2}}U'\,|\psi\rangle = \langle 0|\,U\,|0\rangle\,|\psi\rangle$
$\langle 0|\,\bar{U}\,|1\rangle\,|\psi\rangle = \langle 0|\,\frac{1}{\sqrt{2}}(|0\rangle \otimes g'U'\,|\psi\rangle - |1\rangle \otimes gg'U'\,|\psi\rangle) = \frac{1}{\sqrt{2}}g'U'\,|\psi\rangle = \langle 0|\,U\,|1\rangle\,|\psi\rangle$
$\langle 1|\,\bar{U}\,|1\rangle\,|\psi\rangle = \langle 1|\,\frac{1}{\sqrt{2}}(|0\rangle \otimes g'U'\,|\psi\rangle - |1\rangle \otimes gg'U'\,|\psi\rangle) = -\frac{1}{\sqrt{2}}gg'U'\,|\psi\rangle = -\,\langle 1|\,U\,|1\rangle\,|\psi\rangle$

$\langle 1|\,\bar{U}\,|0\rangle\,|\psi\rangle = \langle 1|\,\frac{1}{\sqrt{2}}(|0\rangle \otimes U'\,|\psi\rangle + |1\rangle \otimes gU'\,|\psi\rangle) = \frac{1}{\sqrt{2}}gU'\,|\psi\rangle = \langle 1|\,U\,|0\rangle\,|\psi\rangle$
Hence, $\langle a|\,\bar{U}\,|b\rangle\,|\psi\rangle = \langle a|\,U\,|b\rangle\,|\psi\rangle\ \forall a, b, \psi$, therefore $U = \bar{U}$.
Overall, U is composed of U' and $O(n)$ phase and Hadamard gates. As construction of a gate $U \in N(G_{n+1})$ requires a gate $U' \in N(G_n)$, for gate U we need $\sum_{i=1}^{n} O(i) = O(n^2)$ phase and Hadamard gates.
3) Consider $UZ_1U^\dagger = g$ and $UX_1U^\dagger = g'$. Then $\{g, g^\dagger\} = 0$ as $\{Z_1, X_1\} = 0$. Hence, g and g' have at some position j $\sigma_j \neq \sigma'_j$. Hence, we use the SWAP operator to turn the situation of that of part (2).
$\mathbf{SWAP}_{1j}UZ_1U^\dagger\mathbf{SWAP}_{1j}^\dagger = \sigma \otimes g_1$
$\mathbf{SWAP}_{1j}UX_1U^\dagger\mathbf{SWAP}_{1j}^\dagger = \sigma' \otimes g'_1$
As we can construct pauli operators using Hadamard and phase gates, if $\sigma \neq \sigma'$ then $R\sigma R^\dagger = Z_1$ and $R\sigma' R^\dagger = X_1$ for some R constructed from phase and Hadamard gates. Then,
$R\mathbf{SWAP}_{1j}UZ_1U^\dagger\mathbf{SWAP}_{1j}^\dagger R^\dagger = Z_1 \otimes g_1$
$R\mathbf{SWAP}_{1j}UZ_1U^\dagger\mathbf{SWAP}_{1j}^\dagger R^\dagger = X_1 \otimes g_1$
which is the situation of part (2).
Therefore, as the **SWAP** is made out of 3 **CNOT**s, we conclude that any normalizer can be written as a composition of $O(n^2)$ phase, Hadamard and **CNOT** gates.

Exercise 10.41

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

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

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

$U = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$

$UZ_1U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -I & 0 \\ 0 & 0 & 0 & -I \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -I & 0 \\ 0 & 0 & 0 & -XX \end{bmatrix} = Z_1$

$UZ_2U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & -I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & -I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & -XX \end{bmatrix} = Z_2$

$UX_3U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} X & 0 & 0 & 0 \\ 0 & X & 0 & 0 \\ 0 & 0 & X & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} X & 0 & 0 & 0 \\ 0 & X & 0 & 0 \\ 0 & 0 & X & 0 \\ 0 & 0 & 0 & XXX \end{bmatrix} = X_3$

$$UX_1U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \\ I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{bmatrix} =$$
$$\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \\ I & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix} = X_1 \otimes \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = X_1 \otimes \frac{\begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} + \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} + \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} + \begin{bmatrix} -X & 0 \\ 0 & X \end{bmatrix}}{2} =$$
$$X_1 \otimes \frac{I + Z_2 + X_3 - Z_2X_3}{2}$$
$$UX_2U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \\ 0 & 0 & I & 0 \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & X \\ 0 & 0 & I & 0 \end{bmatrix} =$$
$$\begin{bmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & X \\ 0 & 0 & X & 0 \end{bmatrix} = \frac{1}{2}\left\{ \begin{bmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \\ 0 & 0 & I & 0 \end{bmatrix} + \begin{bmatrix} 0 & I & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & 0 & -I \\ 0 & 0 & -I & 0 \end{bmatrix} + \begin{bmatrix} 0 & X & 0 & 0 \\ X & 0 & 0 & 0 \\ 0 & 0 & 0 & X \\ 0 & 0 & X & 0 \end{bmatrix} + \begin{bmatrix} 0 & -X & 0 & 0 \\ -X & 0 & 0 & 0 \\ 0 & 0 & 0 & X \\ 0 & 0 & X & 0 \end{bmatrix} \right\}$$
$$= X_2 \otimes \frac{I + Z_1 + X_3 - Z_1X_3}{2}$$
$$UZ_3U^\dagger = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & XZX \end{bmatrix} = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix} =$$
$$\frac{1}{2}\left\{ \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix} + \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & -Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix} + \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & -Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix} + \begin{bmatrix} -Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix} \right\}$$
$$= Z_3 \otimes \frac{I + Z_1 + Z_2 - Z_1Z_2}{2}$$

Exercise 10.42

Initially $S =< IXX, IZZ >$ with $\bar{Z} = ZII$ and $\bar{X} = XII$. Considering the effect of the circuit on the generators we get,

$IXX \xrightarrow{CNOT} IXX \xrightarrow{H} IXX \xrightarrow{\text{Mes. } X_1} IXX \xrightarrow{\text{Mes. } Z_2} IZI$

$IZZ \xrightarrow{CNOT} ZZZ \xrightarrow{H} XZZ \xrightarrow{\text{Mes. } X_1} XZZ \xrightarrow{\text{Mes. } Z_2} XZZ$

For the final $S_f =< IZI, XZZ >$ we have $\bar{Z} = IIZ$ and $\bar{X} = IIX$, hence the circuit does indeed teleport the initial state.

Exercise 10.43

$\forall g \in S$ we have $g \in N(S)$ as $gg'g^\dagger \in S$ $\forall g' \in S$ due to S being a group. Therefore, $S \subseteq N(S)$.

Exercise 10.44

Exercise 10.45

Exercise 10.46

$S =< X_1X_2, X_2X_3 >= \{I, X_1X_2, X_2X_3, X_1X_3\}$
The subspace fixed by X_1X_2 is spanned by $|+++\rangle, |++-\rangle, |---\rangle$ and $|--+\rangle$. The subspace fixed by X_2X_3 is spanned by $|+++\rangle, |-++\rangle, |---\rangle$ and $|-++\rangle$. Hence, the subspace fixed by S is spanned by $|+++\rangle$ and $|---\rangle$, which is the subspace for the three qubit phase flip code. Therefore, X_1X_2 and X_2X_3 generate the stabilizer for the three qubit phase flip code.

Exercise 10.47

The generators 1-6 have 2 Z's with both Z's being in one of the triplets, hence the phase flips are cancelled and $|0_L\rangle$ and $|1_L\rangle$ are fixed by them.
Generators 7 and 8 have Xs on all elements of any of the triplets or none. Hence, they fix $|0_L\rangle$. As 2 triplets are acted on, the phase flip from the triplets is cancelled and hence $|1_L\rangle$ is also fixed. Therefore, theses are the generators for the Shor-code.

Exercise 10.48

Each generator has an even number of Z's or X's, hence commute with $\bar{Z}$ and $\bar{X}$. Counting Y's as both an X and a Z, any product of the generators has an even number of Z's and an even number of X's, therefore as $\bar{Z}$ has an odd number of Z's and $\bar{X}$ has an odd number of X's they are independent of the generators. Lastly, $\bar{X}\bar{Z} = (XZ)^{\otimes 9} = (-1)^9(ZX)^{\otimes 9} = -\bar{Z}\bar{X}$. Therefore, $\bar{Z}$ and $\bar{X}$ act as logical Z and X operators for the Shor-code.

Exercise 10.49

Consider the set $E = \{X_1, \ldots X_5, Y_1 \ldots Y_5, Z_1, \ldots Z_5\}$. Consider for example the combination X_1Z_2. It commutes with g_2 hence $X_1Z_2 \notin N(S)$. Similarly, we can show that $\forall E_iE_j$, $E_iE_j \notin N(S)$ or $E_iE_j \in S$, and hence $E_iE_j \notin N(S) - S$, therefore by Theorem 10.8 the five qubit code can protect against an arbitrary single qubit error.

Exercise 10.50

For the five qubit code $t = 1$, $n = 5$ and $k = 1$. Hence, the Hamming bound is
$\binom{5}{0}3^02^1 + \binom{5}{1}3^12^1 = 2 + 5 \times 6 = 32 = 2^5$
Therefore, the five qubit code saturates the Hamming bound.

Exercise 10.51

The given check matrix is split into generators with only X's and generators only into Z's. Consider the set E of all possible t operator tensor products of X's and Z's. Consider E_iE_j. As both C_1 and C_2 correct up to t errors, $\exists g \in S$ such that for the $2t$ length row E_iE_j $E_iE_jgE_iE_j \notin S$ or $E_iE_j \in S$. Hence, $E_iE_j \notin N(S) - S$, therefore, by Theorem 10.8 E is a length t set of correctable errors.

Exercise 10.52

Using figure 10.6 for the stabilizers. Each generator has an even number of Z's or X's, hence commute with $\bar{Z}$ and $\bar{X}$. Counting Y's as both an X and a Z, any product of the generators has an even number of Z's and an even number of X's, therefore as $\bar{Z}$ has an odd number of Z's and $\bar{X}$ has an odd number of X's they are independent of the generators. Lastly, $\bar{X}\bar{Z} = (XZ)^{\otimes 7} = (-1)^7(ZX)^{\otimes 7} = -\bar{Z}\bar{X}$. Therefore, $\bar{Z}$ and $\bar{X}$ act as logical Z and X operators for the Steane-code.

Exercise 10.53

As G_z includes I, the rank of G_z is k, hence all of its rows are independent and therefore the encoded Z operators are independent of each other.

Exercise 10.54

$G_x = [0E^T I|C^T 00]$

For the first r generators we have $I \times (C^T)^T + C \times I = 0$ and for the other $n-k-r$ generators $I \times (E^T)^T + E \times I = 0$, therefore the encoded X operators commute with the generators. The encoded X operators commute with each other, as in each block we have only X or only Z operators. The independence from the generators follows from the I in the left corner of the check matrix, and the 0s in the last $n-k-r$ generators, as it's not possible to get the X section of G_x with these, due to the 0 in the first block in G_x. As G_x includes I, the rank of G_x is k, hence all of its rows are independent and therefore the encoded X operators are independent of each other. Comparing G_x and G_z, in the first two blocks we have only X's or only Z's, hence those parts commute. The third block for both the X and Z section is the identity, hence for $\bar{X}_i$ the third block corresponds with the i^{th} row of I in the X section and similarly for $\bar{Z}_j$ to the j^{th} row of I in the Z section. Hence, $\bar{X}_i$ and $\bar{Z}_j$ have an X and a Z respectively in the same location only if $i = j$. Therefore, $\bar{X}_i$ and $\bar{Z}_j$ commute unless $i = j$ in which case they anti-commute.

Exercise 10.55

$E = (1,1,0)$ and $C = (0,0,0)$, $\bar{X} = X_4X_5X_7$.

Exercise 10.56

Consider $g_i\bar{X}_i$, as g_i commutes with and is independent of all the g's and $\bar{X}$'s and $\bar{Z}$'s, $g_i\bar{X}_i$ still commutes with and is independent of all of them. Also, from the previous statement $g_i\bar{X}_i$ commutes with all $\bar{Z}_j$ unless $i = j$. Similarly, for $g_i\bar{Z}_i$. Therefore, gX and gZ still are encoded X and Z operators and hence their action on the code doesn't change.

Exercise 10.57

For the five qubit code swap q_2 and q_5, replace g_1 by g_1g_4 and afterwards g_3 with g_3g_1.

$$G_4 = \left[\begin{array}{ccccc|ccccc} 1&0&0&1&0&0&1&1&0&0\\ 0&1&0&0&1&0&0&1&1&0\\ 1&0&1&0&0&0&0&0&1&1\\ 0&1&0&1&0&1&0&0&0&1 \end{array}\right] = \left[\begin{array}{ccccc|ccccc} 1&0&0&0&1&1&1&1&0&1\\ 0&1&0&0&1&0&0&1&1&0\\ 0&0&1&0&1&1&0&1&1&1\\ 0&0&0&1&1&1&1&0&0&0 \end{array}\right]$$

For the nine qubit code replace g_3 by g_3g_4, g_5 by g_5g_6, g_7 by g_7g_8. Then swap q_1 and q_3, q_2

and q_4, q_2 and q_5, q_2 and q_6, q_2 and q_8

$$G_9 = \left[\begin{array}{ccccccccc|ccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{array}\right] =$$

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

Exercise 10.58

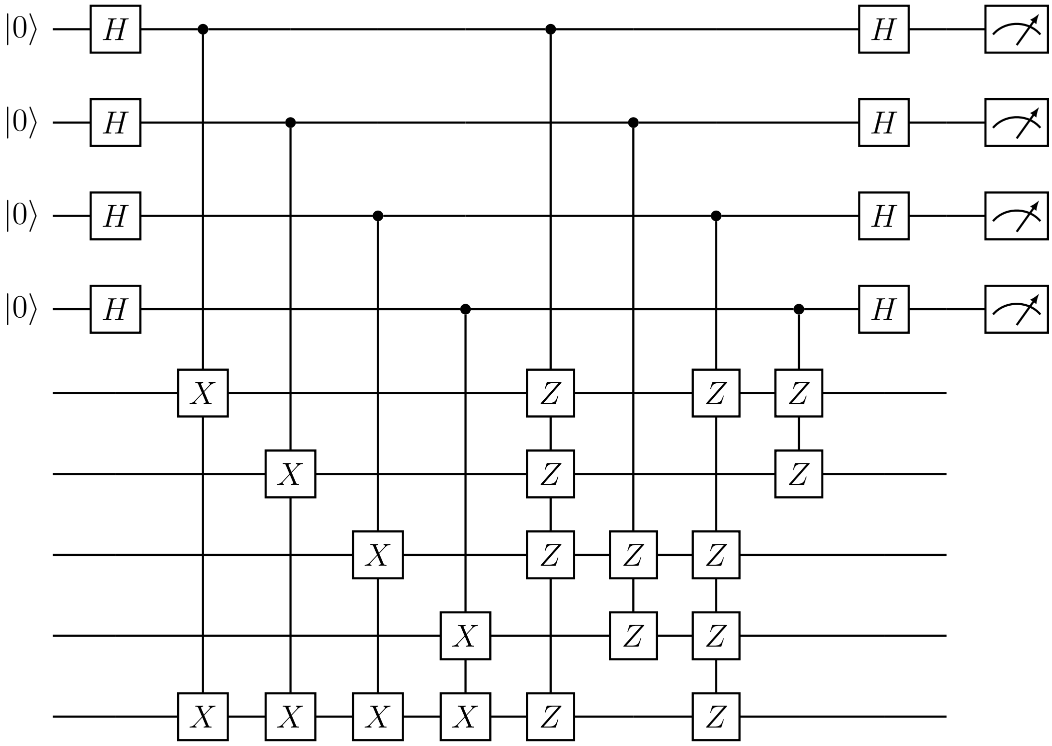
From Exercise 4.34 the circuits function as described. The equivalence of Figure 10.14 follows from Exercise 4.20 and the equivalence of Figure 10.15 follows from Exercise 4.18 and that $HZH = X$.

Exercise 10.59

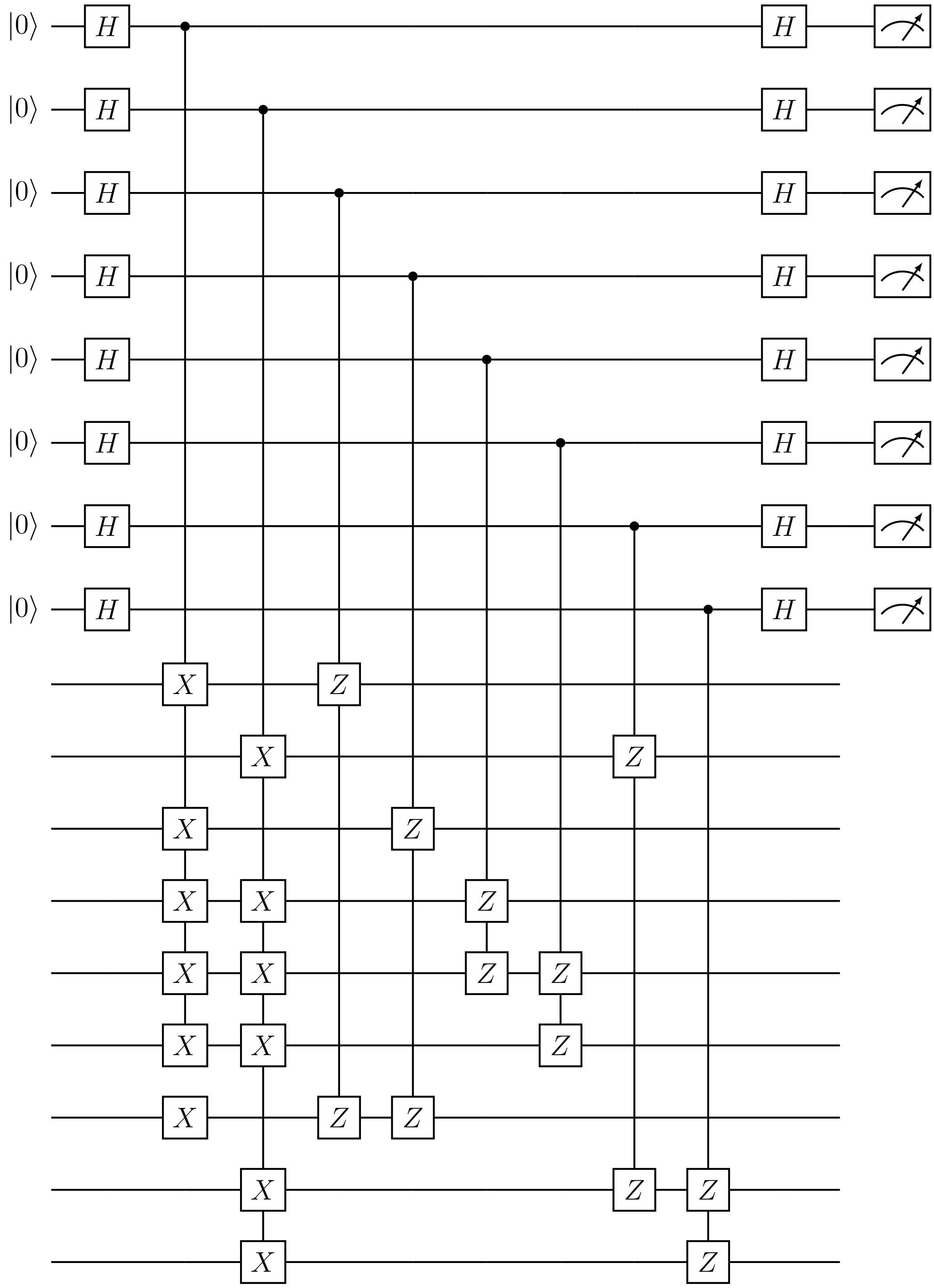
Each single control multiple targets gate can be written as multiple single control single target gates. As $HH = I$ we can add Hadamard pairs between the single control single target gates, which then gives multiple subcircuits in the form of Figures 10.14 and 15. Applying, the equivalence of the circuits using $HH = I$ and collecting the single control single target gates together under single target multiple targets gates gives the circuit in Figure 10.17.

Exercise 10.60

Using the check matrices from Exercise 10.57 we get,
For the five qubit code,



For the nine qubit code,



Exercise 10.61

E_j are all the possible single qubit errors. For each E_j we consider, $E_j g_l E_j^\dagger = \beta_l g_l$ where β_l is the syndrome measurement. Hence, for each syndrome we compare the β_l's and decide based on that which E_j has occurred and apply $E_j^\dagger$ to recover. We also have seen that if multiple E_j give rise to the same syndrome then it suffices to choose one of them and applying $E_j^\dagger$ for that error operator corrects all the errors with the same syndrome.

Exercise 10.62

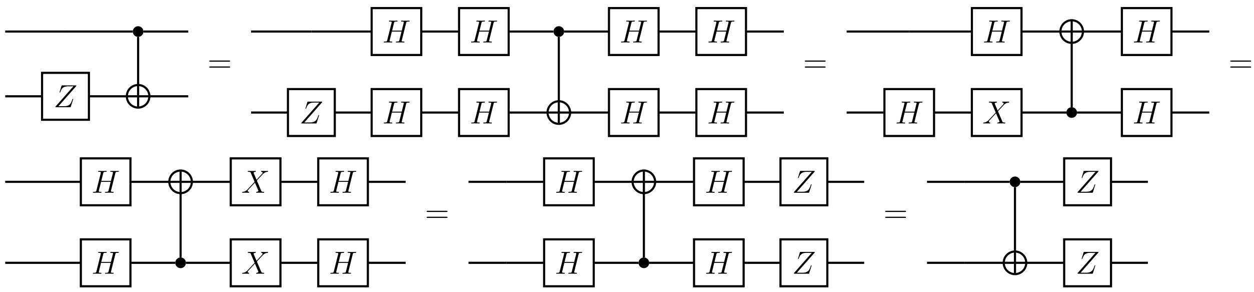
Let S_1 be the generator for $[n_1, 1]$ and S_2 the generator for $[n_2, 1]$. After concatenating the generators for the stabilizer will need to stabilize both $[n_1, 1]$ and $[n_2, 1]$. Hence, the generators will be all the combinations $g_i g'_j$ where $g_i \in S_1$ and $g'_j \in S_2$. Therefore, this will create a $[n_1 n_2, 1]$ code.

Exercise 10.63

$\bar{U}|0_L\rangle = \bar{U}\bar{Z}|0_L\rangle = \bar{X}\bar{U}|0_L\rangle$
$\bar{U}|1_L\rangle = -\bar{U}\bar{Z}|1_L\rangle = -\bar{X}\bar{U}|1_L\rangle$
Hence, $\bar{U}|0_L\rangle$ and $\bar{U}|1_L\rangle$ correspond to the ± 1 eigenstates of $\bar{X}$, hence up to a phase factor $\bar{U}|0_L\rangle = \frac{1}{\sqrt{2}}(|0_L\rangle + |1_L\rangle)$ and $\bar{U}|1_L\rangle = \frac{1}{\sqrt{2}}(|0_L\rangle - |1_L\rangle)$.

Exercise 10.64

Using Exercise 10.36 $UZ_2 = UZ_2U^\dagger U = Z_1 Z_2 U$.
Using Exercise 4.20, $HZ = XH$ and the propagation of an X error on the control qubit,

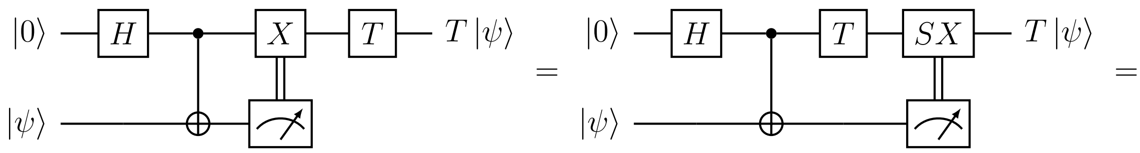


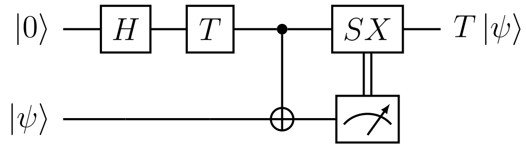
Exercise 10.65

Let $|\psi\rangle = a|0\rangle + b|1\rangle$. For the first circuit we have,
$a|00\rangle + b|01\rangle \xrightarrow{\text{CNOT}_{21}} a|00\rangle + b|11\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(a|00\rangle + a|01\rangle + b|10\rangle - b|11\rangle) =$
$\frac{1}{\sqrt{2}}((a|0\rangle + b|1\rangle)|0\rangle + (a|0\rangle - b|1\rangle)|1\rangle) \xrightarrow{\text{Mes}} \begin{cases} |\psi\rangle & \text{if measurement gives} + 1 \\ Z(a|0\rangle - b|1\rangle) = |\psi\rangle & \text{if measurement gives} - 1 \end{cases}$
For the second circuit we have,
$a|00\rangle + b|01\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}(|0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(a|0\rangle + b|1\rangle)) \xrightarrow{\text{CNOT}_{12}}$
$\frac{1}{\sqrt{2}}(|0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(a|1\rangle + b|0\rangle)) =$
$\frac{1}{\sqrt{2}}((a|0\rangle + b|1\rangle)|0\rangle + (a|1\rangle + b|0\rangle)|1\rangle) \xrightarrow{\text{Mes}} \begin{cases} |\psi\rangle & \text{if measurement gives} + 1 \\ X(b|0\rangle + a|1\rangle) = |\psi\rangle & \text{if measurement gives} - 1 \end{cases}$

Exercise 10.66

Mistake in the question, should be $TXT^\dagger = exp(-i\pi/4)SX$,i.e. $TX = exp(-i\pi/4)SXT$.





Exercise 10.67

$$\text{a)}LHS = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix}$$

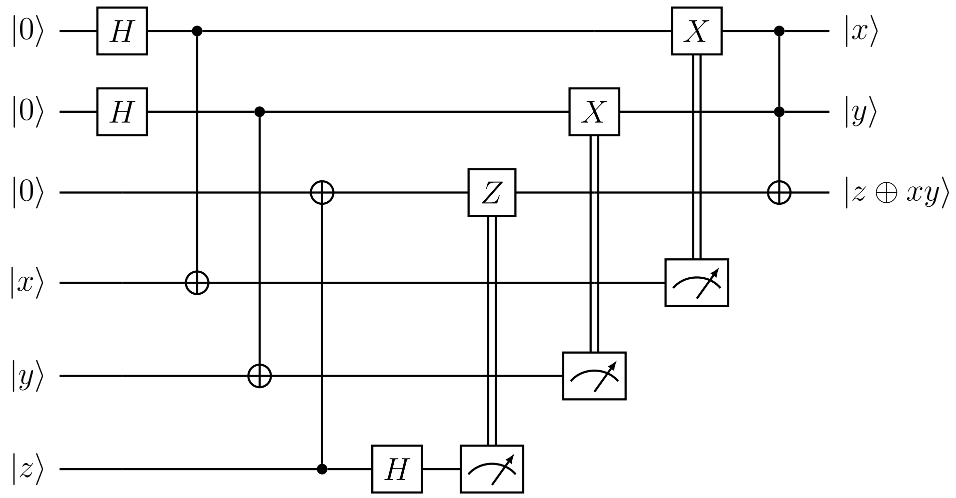
$$RHS = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \\ I & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & XX \\ I & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & X & 0 & 0 \end{bmatrix}$$

$$\text{b)}LHS = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & Z \end{bmatrix} = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & XZ \end{bmatrix}$$

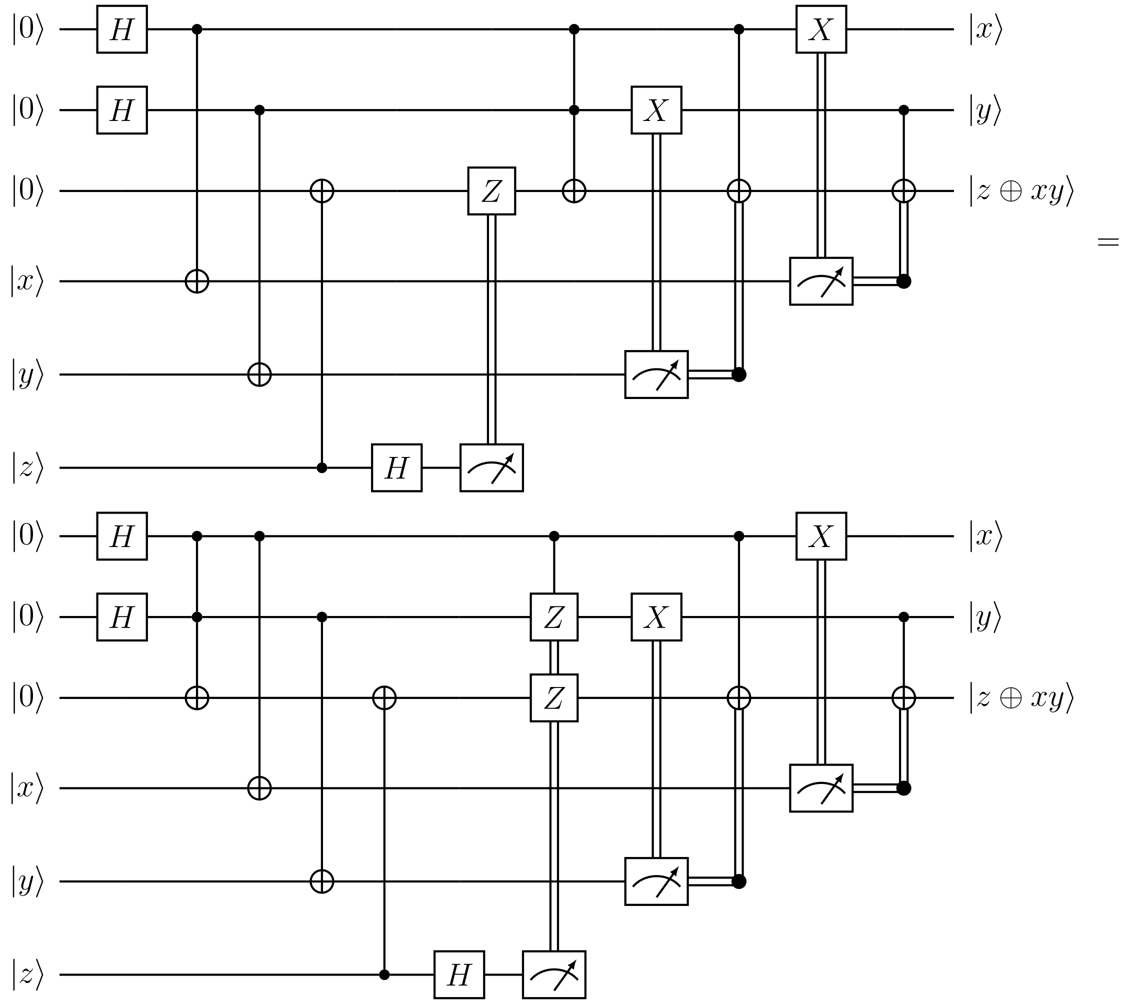
$$RHS = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -Z \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & -ZX \end{bmatrix} = \begin{bmatrix} Z & 0 & 0 & 0 \\ 0 & Z & 0 & 0 \\ 0 & 0 & Z & 0 \\ 0 & 0 & 0 & XZ \end{bmatrix}$$

Exercise 10.68

1)$|x\rangle$ and $|y\rangle$ are swapped using the first circuit in Exercise 10.65 and $|z\rangle$ is swapped using the second circuit. Then, applying the Toffoli gives the indicated result.
2)Using Exercise 10.67 (a) twice and then (b) we get the following,



$=$



3)If the ancilla preparation is done fault-tolerantly then, there will be at most an error on most a single qubit after the preparation. The first three CNOTs as shown prior are fault tolerant as the error doesn't propagate in more than one qubit due to the measurement (assuming fault-tolerant measurement). Using the Steane code the rest of the CNOT's and controlled-Z gates can be performed fault-tolerantly, therefore the whole circuit is a fault-tolerant implementation of the Toffoli gate.

Exercise 10.69

An X error on the second and third qubits won't propagate between the ancilla, while an X error on the first qubit will propagate to the second and third qubits and hence will be detected by the verification step. For a Y error $UY_1 = Y_1X_2U$ and $UY_2 = Z_1Y_2U$. Hence, a Y error on the the first qubit will propagate an X error to the other 2 qubits which will be detected by the verification step. A Y error on one of the other qubits will propagate a Y error which will be detected by the verification step.

Exercise 10.70

$UZ_1 = Z_1U$ hence the Z errors will not propagate to the data qubits, but will change the parity of the 'cat' state and therefore alter the measurement result.