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.
$PE_i^\dagger E_j P = 0$, $i \neq j$
$PE_i^\dagger E_j P = P$, $i = j$
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 $\{\sqrt{\frac{p}{d}} \left|i\right\rangle \left\langle j\right|\}$. Taking $p = 1$ and $d = 2$, we get $\{\frac{1}{2}\left|0\right\rangle\left\langle 0\right|, \frac{1}{2}\left|1\right\rangle\left\langle 1\right|, \frac{1}{2}\left|0\right\rangle\left\langle 1\right|, \frac{1}{2}\left|1\right\rangle\left\langle 0\right|\}$.

Exercise 10.12

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

Exercise 10.13

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

Exercise 10.14

$$G = rk\left\{\underbrace{\begin{bmatrix} 1 & 0 & \dots & 0 \\ {}_r\vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}}_{k}\right.$$

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

Exercise 10.25

Exercise 10.26