Problem 1. Suppose a parity check matrix for a binary linear code $C$ has 3 rows and 8 columns.

(a) How many words are there in $C$?
(b) How many words are there in the dual code $C^\perp$?

Solution: The parity check matrix for $C$ is a generator matrix for $C^\perp$. Since it has 3 rows, we conclude that $\dim(C^\perp) = 3$. Consequently, $\dim(C) = 8 - 5 = 3$. Thus

(a) $|C| = 2^{\dim(C)} = 2^5 = 32$.
(b) $|C^\perp| = 2^{\dim(C^\perp)} = 2^3 = 8$.

Problem 2. Let $C \subset V(5,3)$ be a ternary linear code of length 5 consisting of words $(x_1, \ldots, x_5)$ satisfying

\begin{align*}
x_1 + x_3 + x_4 + 2x_5 &= 0 \\
2x_1 + 2x_2 + x_3 + 2x_4 + 2x_5 &= 0 \\
2x_1 + x_2 + x_3 + 2x_4 &= 0.
\end{align*}

(Recall that “ternary” means that $q = 3$.)

(a) Find a parity check matrix for $C$.
(b) Find a generator matrix for $C$.
(c) Find the minimal distance of $C$.
(d) Find the minimal distance of the dual code $C^\perp$.

Solution: (a) A candidate for parity check matrix is given by $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 2 & 2 & 1 & 2 & 2 \\ 2 & 1 & 1 & 2 & 0 \end{bmatrix}$.

We need to check that the rows are linearly dependent. To do this, we row reduce.

Replace $R_2$ with $R_2 + R_1$ to get

\begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 2 & 2 & 0 & 1 \\ 2 & 1 & 1 & 2 & 0 \end{bmatrix}.

Replace $R_3$ with $R_1 + R_3$ to get

\begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 2 & 0 & 2 \end{bmatrix}.

Replace $R_3$ with $R_2 + R_3$ to get

\begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.

Replace $R_2$ with $2R_2$ to get

\begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.
Replace $R_1$ with $R_1 - R_3$ to get
\[
\begin{bmatrix}
1 & 0 & 0 & 1 & 2 \\
0 & 1 & 1 & 0 & 2 \\
0 & 0 & 1 & 0 & 0
\end{bmatrix}.
\]

Replace $R_2$ with $R_2 - R_3$ to get
\[
\begin{bmatrix}
1 & 0 & 0 & 1 & 2 \\
0 & 1 & 0 & 0 & 2 \\
0 & 0 & 1 & 0 & 0
\end{bmatrix} = H'.
\]

$H'$ is the Reduced Row Echelon Form for $H$. Since $H'$ has no zero rows, the row space of $H$ is 3-dimensional. Thus the rows of $H$ are linearly independent (if they were dependent, the row space for $H$ would be at most 2-dimensional.)

(b) Since $H'$ is a parity check matrix in standard form for $C$ (or equivalently, a generator matrix for $C^\perp$), we can use it to get a generator matrix for $(C^\perp)^\perp = C$.

\[
G = \begin{bmatrix}
-1 & 0 & 0 & 1 & 0 \\
-2 & -2 & 0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
2 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1
\end{bmatrix}.
\]

Quick Check: The rows of $G$ must be orthogonal to that of $H$.

(c) To find minimal distance in $C$ we need to look at the columns of its parity check matrix $H$. Since there is no zero column we know $d(C) > 1$. On the other hand there are two linearly dependent columns (the first and fourth column are equal) so $d(C) \leq 2$. We conclude that $d(C) = 2$.

(d) For finding minimal distance in $C^\perp$ we look at the columns of its parity check matrix $G$. Since there is a zero column (third column) we deduce $d(C^\perp) = 1$.

**Problem 3.** Suppose $C$ is a binary linear code code of length 5. A coset of $C$ is given by

\[(1, 0, 0, 0, 0), (0, 0, 0, 1, 1), (1, 1, 0, 1, 0), (0, 1, 0, 0, 1), (1, 0, 1, 0, 1), (0, 0, 1, 1, 0), (1, 1, 1, 1, 1), (0, 1, 1, 0, 0).\]

Find a generator matrix for $C$. Explain your answer.

**Solution:** The above coset is $(1, 0, 0, 0, 0) + C$. So in order to find $C$ we subtract $(1, 0, 0, 0, 0)$ from each word in the coset. We deduce the code $C$ consists of the following 8 words:

\[(0, 0, 0, 0, 0), (1, 0, 0, 1, 1), (0, 1, 0, 1, 0), (1, 1, 0, 0, 1), (0, 0, 1, 0, 1), (1, 0, 1, 1, 0), (0, 1, 1, 1, 1), (1, 1, 1, 0, 0).\]

Since all cosets are of the same size and the coset containing $(0, 0, 0, 0, 0)$ is $C$, we deduce that

\[|C| = 8 = 2^3.\]

Thus a generator matrix for $C$ is a $3 \times 5$ matrix. The rows of these matrix can be any 3 linearly independent words in $C$. Among many choices, one is the following

\[(1, 0, 0, 1, 1), (0, 1, 0, 1, 0), (0, 0, 1, 0, 1).\]
This gives rise to the matrix
\[
G = \begin{bmatrix}
1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1
\end{bmatrix}.
\]

Since \( G \) is in standard form, its rows are linearly independent, so \( G \) is a parity check matrix for \( C \).

**Problem 4.** A \( q \)-ary linear code \( C \subset V(n, q) \) of length \( n \) is called self-dual if \( C = C^\perp \).

(a) If there exists a self-dual code \( C \) of length \( n \), then \( n \) is even and \( \dim(C) = \frac{n}{2} \).

(b) Give an example of a self-dual binary code of length 2.

(c) Use part (b) to construct an example of a self-dual binary code of length 4.

(d) Use parts (b) and (c) to show that for every integer \( m \geq 1 \) there exists a self-dual binary code of length \( 2m \).

**Solution:** (a) Since \( \dim(C) + \dim(C^\perp) = n \) and \( \dim(C) = \dim(C^\perp) \) we have \( 2 \dim(C) = n \). Thus \( n \) is even and \( \dim(C) = \frac{n}{2} \).

(b) From part (a) we know \( \dim(C) = 2 \frac{2}{2} = 1 \). The word \((1, 1)\) is orthogonal to itself, so its span, \( \{(0, 0), (1, 1)\} \) is self-dual. (Check!).

Remark: How could we have arrived at this answer? As \( C \) is a 1-dimensional subspace of \( V(2, 2) = \{(0, 0), (1, 0), (0, 1), (1, 1)\} \), there are only 3 possibilities: \( C \) is the span of \( v \), where \( v = (1, 0) \) or \( (0, 1) \) or \( (1, 1) \). But \((1, 0)\) is not orthogonal to itself, and neither is \((0, 1)\).

(c) We extend the previous example by choosing \( C \) to be generated by \((1, 1, 0, 0)\) and \((0, 0, 1, 1)\). Any vector \((a, b, c, d)\) orthogonal to \((1, 1, 0, 0)\) must have \( a = b \) and orthogonal to \((0, 0, 1, 1)\) must have \( c = d \). But then \((a, a, c, c)\) lies in \( C \). Consequently \( C = C^\perp \).

Alternately, another self-dual code is given by generators \((1, 0, 1, 0)\) and \((0, 1, 0, 1)\).

(d) We argue by induction on \( m \). If \( C \) is a binary self-dual linear code of length \( 2m \), we can create a binary self-dual linear code \( C' \) of length \( 2(m + 1) \) as follows. For every word \( x = (x_1, \ldots, x_{2m}) \) in \( C \), create two words, \((x_1, \ldots, x_{2m}, 0, 0)\) and \((x_1, \ldots, x_{2m}, 1, 1)\). The code \( C' \) obtained in this way is readily checked to be self-dual.

An alternative way to describe the code \( C \) of length \( 2m \) resulting from this construction is by the \( m \times 2m \) generating matrix \( G = \begin{bmatrix}
1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1
\end{bmatrix} \). Every word in \( C \) is of the form \((a_1, a_1, a_2, a_2, \ldots, a_m, a_m)\) where \( a_1, \ldots, a_m \) range over \( F_2 \). To see that this code is self-dual, note that \( x = (x_1, x_2, \ldots, x_{2m-1}, x_{2m}) \) lies in \( C^\perp \) if and only if \( x \) is orthogonal to every row of \( G \) if and only if \( x_1 = x_2, x_3 = x_4, \ldots, x_{2m-1} = x_{2m} \) if and only if \( x \in C \).
An alternative self-dual code (same up to column permutation) is given by the generating matrix \( G = [I_m \mid I_m] \).

**Problem 5.** Let \( C \) be the binary linear code of length 5 with parity check matrix

\[
H = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix}.
\]

(a) Write out the coset of \( C \) containing \((0, 0, 1, 1, 1)\).
(b) Suppose a word \( x \) from \( C \) was received as \( y = (1, 0, 1, 0, 0) \). Find \( x \) using syndrome decoding.

**Solution:**
(a) We will use row operations to reduce \( H \) to standard form. Replace \( R_2 \) with \( R_2 + R_3 \) to get

\[
\begin{pmatrix}
1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

Replace \( R_1 \) with \( R_1 + R_2 \) to get

\[
\begin{pmatrix}
1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

Replace \( R_1 \) with \( R_1 + R_3 \) to get

\[
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1
\end{pmatrix}
\]

So a generator matrix is given by

\[
G = \begin{pmatrix}
1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1
\end{pmatrix}
\]

Taking linear combinations of the rows of \( G \), we see that

\[
C = \{(0, 0, 0, 0, 0), (1, 0, 1, 1, 0), (0, 1, 1, 0, 1), (1, 1, 0, 1, 1)\}
\]

The coset containing \((0, 0, 1, 1, 1)\) is \((0, 0, 1, 1, 1) + C\) i.e.

\[
(0, 0, 1, 1, 1), (1, 0, 0, 0, 1), (1, 1, 0, 1, 0), (1, 1, 1, 0, 0)
\]

(b) All syndromes will be calculated with respect to matrix \( H \) as given in the problem. We have \( S(y) = (0, 1, 1) \).
We see that syndrome of \( y \) is the same as the syndrome of \((0,0,0,1,0)\) and that no other word of weight \( \leq 1 \) has this syndrome. Consequently we decode as \( x = y - e = (1,0,1,0,0) - (0,0,0,1,0) = (1,0,1,1,0) \).