
1. Let \( d \geq 2t + 1 \) be the minimum distance of a linear code of length \( n \). Prove that every vector of weight \( t \) is a coset leader and is the unique coset leader of the coset containing it.

   Let \( x \) be a vector of weight 2, and consider the coset \( x + C \) of the code \( C \) that contains \( x \). Let \( y = x + c \) be any vector different from \( x \) in this coset where \( 0 \neq c \in C \). If the weight of \( y \) is \( t \) or less, then \( c = y - x \) is a nonzero codeword of weight at most the weight of \( y \) plus the weight of \( x \), that is \( 2t \). This contradicts \( d \geq 2t + 1 \). Hence the weight of \( y \) is at least \( t + 1 \) verifying that \( x \) is the unique coset leader of its coset.

2. Let \( C \) be an \((n, k, d)\) linear code over a finite field \( F \), and let \( H \) be a \( n - k \) by \( n \) parity check matrix for \( C \). Let \( x \) an \( n \)-tuple over \( F \).
   (i) In terms of \( H \) when is \( x \) a codeword of \( C \)?

   Exactly when \( Hx^T = 0 \).

   (ii) Prove that \( d \leq n - k + 1 \)

   The matrix \( H \) has rank equal to \( n - k \). Hence every set of \( n - k + 1 \) columns of \( H \) is linearly dependent. Thus every set of \( n - k + 1 \) columns produces a codeword of weight \( n - k + 1 \) at most, and \( d \leq n - k + 1 \). Note that in order for \( d = n - k + 1 \) to occur, every set of \( n - k \) columns of \( H \) would have to be linearly independent.

   (iii) Apply the upperbound in (ii) to the binary repetition code of length \( n \) and its dual. What do you get?

   For the binary repetition code, we get \( k = 1 \) and \( d = n \) and so we have equality in \( d = n - k + 1 \). For the dual (the even weight code) we have \( k = n - 1 \) and \( d = 2 \) and we also have equality in \( d = n - k + 1 \)

3. Find, with verification, the minimum distance of the binary code with generator matrix \( G \) where

\[
G^T = \begin{bmatrix}
1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1
\end{bmatrix}
\]

\[I_7 = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}\]

The minimum distance equals the minimum weight of a nonzero codeword. Since we have codewords in the generator matrix of weight 3, \( d \leq 3 \). If we add any three or more rows of \( G^T \) we get weight at least 3 (because of the \( I_7 \)). If we add any two rows of \( G^T \), we get weight at least 3, since no two rows to the right of the \( I_7 \) are identical. So \( d = 3 \).
4. Let $C$ be a binary code with generator matrix

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

Decode the following received words (using nearest-neighbor decoding):

A parity check matrix is

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

(a) $x = (1, 1, 0, 1, 0, 1, 1)$

We have $Hx^T = 0$ and so $x$ is a codeword and thus should be decoded as $x$.

(b) $x = (0, 1, 1, 0, 1, 1, 1)$

We have $Hx^T = \begin{bmatrix} 1 \\
0 \\
1 \end{bmatrix}$ so that $x$ is not a codeword. Since this syndrome is the last column of $H$, $(0, 1, 1, 0, 1, 1, 0)$ is a codeword at distance 1 from $x$.

(c) $x = (0, 1, 1, 1, 0, 0, 0)$

We have $Hx^T = \begin{bmatrix} 1 \\
0 \\
1 \end{bmatrix}$ so that $x$ is not a codeword. Since this syndrome is both the first and second column of $H$, both $(1, 1, 1, 1, 0, 0, 0)$ and $x = (0, 0, 1, 1, 0, 0, 0)$ are codewords at distance 1 from $x$. 