Mathematics 342. Solutions to Midterm 2

Problem 1. Suppose a parity check matrix for a binary linear code C has 7 rows and 12 columns. How many words are there in C?

Solution: The dual code $C^{\perp}$ is a 7-dimensional subspace of $V(12,2) = (F_2)^{12}$. Hence, $\dim(C) = 12 - \dim(C^{\perp}) = 12 - 7 = 5$, and the number of words in C is $2^5 = 32$.

Problem 2. Let C be the span of $\mathbf{a} = (1,0,2,1,2)$, $\mathbf{b} = (2,2,1,2,2)$, and $\mathbf{c} = (2,1,1,2,0)$ in $V(5,3) = (F_3)^5$.

(a) Find a basis and the minimal distance of C.

(b) Find a basis and the minimal distance of $C^{\perp}$.

Solution: (a) Let

$$A = \begin{bmatrix} 1 & 0 & 2 & 1 & 2 \\ 2 & 2 & 1 & 2 & 2 \\ 2 & 1 & 1 & 2 & 0 \end{bmatrix}$$

Apply elementary row operations to find an REF:

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

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

$$REF = \begin{bmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The first two rows form a basis for the span.

To get a generator matrix in standard form, delete the zero row and multiply Row 2 by 2.

$$G = \begin{bmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \end{bmatrix}$$

in the form $G = [I_2|A]$. Then we obtain the parity check matrix

$$H = [-B^T|I_3] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Since H has no zero columns, $d(C) \geq 2$. Since columns 2 and 5 are linearly dependent, $d(C) = 2$.

(b) The rows of H form a basis for $C^{\perp}$. To find $d(C^{\perp})$, use the fact that G is a parity check matrix for $C^{\perp}$. Since G has no zero columns, $d(C^{\perp}) \geq 2$. columns 1 and 4 of G are linearly dependent, $d(C^{\perp}) = 2$.

Problem 3. Suppose C is a ternary code of length 8 with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{pmatrix}$$

Recall that "ternary" means that $q = 3$, i.e., our alphabet is $F_3 = \{0, 1, 2\}$.

In each part determine whether or not the words $\mathbf{v}$ and $\mathbf{w}$ lie in the same coset of C.

(a) $\mathbf{v} = (1, 1, 1, 1, 1, 1, 1, 1)$ and $\mathbf{w} = (2, 1, 1, 1, 1, 1, 2, 1)$,

(b) $\mathbf{v} = (1, 1, 1, 1, 1, 1, 1, 1)$ and $\mathbf{w} = (2, 2, 2, 2, 2, 2, 2, 2)$.

Solution: We construct the parity check matrix

$$H = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 \end{pmatrix}$$

and use it to check whether or not the syndroms $S(\mathbf{v}) = \mathbf{v} \cdot H^T$ and $S(\mathbf{w}) = \mathbf{w} \cdot H^T$ are the same.

(a) $S(\mathbf{v}) = (1, 1)$ and $S(\mathbf{w}) = (1, 1)$. Thus $\mathbf{v}$ and $\mathbf{w}$ are in the same coset.

(b) $S(\mathbf{v}) = (1, 1)$ and $S(\mathbf{w}) = (2, 2)$. Thus $\mathbf{v}$ and $\mathbf{w}$ are not in the same coset.

Problem 4. Suppose $q = 7$ and C is the q-ary repetition code of length 5, i.e., the code consisting of words of the form (i, i, i, i, i), where i is an element of $\mathbb{F}_q$.

(a) Find a generator matrix and a parity check matrix for C.

(b) Find a coset leader for the coset $(0, 0, 1, 1, 1) + C$.

Solution: (a) C consists of multiples of $(1, 1, 1, 1, 1)$, so, a generator matrix is $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$. Using this generator matrix, we find a parity check matrix:

$$H = \begin{pmatrix} 6 & 1 & 0 & 0 & 0 \\ 6 & 0 & 1 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b) The coset $(0, 0, 1, 1, 1) + C$ has 7 words,

$(0, 0, 1, 1, 1)$,
$(1, 1, 2, 2, 2)$,
$(2, 2, 3, 3, 3)$,
$(3, 3, 4, 4, 4)$,
$(4, 4, 5, 5, 5)$,
$(5, 5, 6, 6, 6)$, and
$(6, 6, 0, 0, 0)$.

The coset leader is the word $(6, 6, 0, 0, 0)$ of weight 2.

Problem 5. A message $\mathbf{x}$ was sent using the ternary linear code C of length 4 with parity check matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

A message $\mathbf{y}$ was received. Use syndrome decoding to decode $\mathbf{y}$ if

(a) $\mathbf{y} = (2, 2, 1, 0)$, (b) $\mathbf{y} = (1, 1, 0, 0)$.

Once again, "ternary" means that $q = 3$, same as in Problems 2 and 3.

Solution: (a) The syndrome of $\mathbf{y} = (2, 2, 1, 0)$ is

$$S(\mathbf{y}) = \mathbf{y} \cdot H^T = (0, 0).$$

Hence, $\mathbf{y}$ is in C, and we decode $\mathbf{y}$ as $\mathbf{x} = \mathbf{y} = (2, 2, 1, 0)$.

(b) Here the syndrome of $\mathbf{y} = (1, 1, 0, 0)$ is

$$S(\mathbf{y}) = \mathbf{y} \cdot H^T = (1, 1).$$

Since $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is the third column of H, we see that $S(0, 0, 1, 0) = (1, 1) = S(\mathbf{y})$.

Since the minimal distance of C is 3 (this can be established by looking at the columns of H), there is at most one vector of weight 1 in each coset of C. In particular, $e = (0, 0, 1, 0)$ is the unique element o weight 1 in the coset $\mathbf{y} + C$; all other vectors in this coset have weight ≥ 2. Thus $\mathbf{e} = (0, 0, 1, 0)$ is the unique coset leader in $\mathbf{y} + C$. We decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (1, 1, 0, 0) - (0, 0, 1, 0) = (1, 1, 2, 0).$$