Solutions to Problem Set 5.

Mathematics 342, Term 2, 2018. Instructor: Reichstein.

(1) Let $q = 7$ and C be a q-ary code of length 6 with parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Assuming that at most one error occurred in transmission, decode the following received words, if possible: (a) $(1, 1, 1, 1, 1, 0)$, (b) $(0, 0, 0, 0, 1, 1)$, (c) $(3, 5, 0, 2, 4, 6)$.

Hint: Use a decoding scheme similar to the one in Example 7.12 in the book.

Solution: Denote the received word by $\mathbf{y} = (y_1, \dots y_6)$ and the syndrome $S(\mathbf{y}) = \mathbf{y} \cdot H^T$ by (s_1, s_2). The decoding algorithm is as follows.

Case 1. If $(s_1, s_2) = (0, 0)$, we assume that no error occured.

Case 2: If $s_1 \neq 0$ and $s_2 \neq 0$, we assume that one error occured. Denote the error magnitude by a, the error position by i, and the resulting error vector by

$$\mathbf{e} = (0, \dots, 0, a, 0, \dots, 0).$$

Then $S(\mathbf{e}) = (a, ia)$. Matching $S(\mathbf{e})$ to $S(\mathbf{y})$, we see that $a = s_1$ and $i = s_2/s_1$.

Case 3: If $(s_1, s_2) \neq (0, 0)$ but $s_1 = 0$ or $s_2 = 0$, then at least two errors occured.

Note that this is an incomplete decoding scheme. We can correct the received word in Cases 1 and 2. In Case 3, we just note that at least two errors occurred. This exceeds the error-correcting capability of our code: the received word is too corrupted to be correctable.

We now apply this algorithm to the received words $\mathbf{y}$ in parts (a), (b) and (c).

In part (a), $S(\mathbf{y}) = (5, 1)$, so we are in Case 2. Assume one error of magnitude 5 in position $1/5 = 3$. (Here the division is carried out in F_7: $5^{-1} = 3$ because $3 \cdot 5 = 15 = 1$ in F_7.) Thus $\mathbf{e} = (0, 0, 5, 0, 0, 0)$, and we decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (1, 1, 1, 1, 1, 0) - (0, 0, 5, 0, 0, 0) = (1, 1, 3, 1, 1, 0).$$

In part (b), $S(\mathbf{y}) = (2, 4)$, so we are again in Case 2. We assume one error of magnitude 2 in position $4/2 = 2$ and decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (0, 0, 0, 0, 1, 1) - (0, 2, 0, 0, 0, 0) = (0, 5, 0, 0, 1, 1).$$

In part (c), $S(\mathbf{y}) = (6, 0)$, so we are in Case 3. At least two errors occurred.

(2) Problem 7.11.

Solution: Assume H is a $r \times n$ matrix, so that $\dim(C) = n - r$. The extended code $\hat{C}$ has the same number of words as C and hence, the same dimension, $\dim(\hat{C}) = n - r$.

Let us begin by checking that the rows of $\hat{H}$ are linearly independent, i.e., $\hat{H}$ is a legitimate parity check matrix. Denote the rows of H by $R_1, \dots, R_r$. Appending zero to each of these rows on the right, we obtain the first r rows of $\hat{H}$, which we will denote by $(R_1, 0), \dots, (R_r, 0)$. Suppose some linear combination of the rows of $\hat{H}$ is the zero row,

$$a_1(R_1, 0) + a_2(R_2, 0) + \dots + a_r(R_r, 0) + a_{r+1}(1, 1, \dots 1) = (0, 0, \dots, 0).$$

Our goal is to show that $a_1 = a_2 = \dots = a_{r+1} = 0$. Equating the last component on both sides, we obtain $a_{r+1} = 0$. Equating the first n components, we obtain

$$a_1 R_1 + a_2 R_2 + \dots + a_r R_r = (0, \dots, 0).$$

Since the rows of H are linearly independent, we conclude that $a_1 = \cdots = a_r = 0$ as well, as desired.

Now we know that $\hat{H}$ is a partiy check matrix for some code D, where

$$\dim(D) = (n+1) - (r+1) = n - r = \dim(\hat{C}).$$

Moreover, by the definition of $\hat{C}$, every word in $\hat{C}$ is orthogonal to every row of $\hat{H}$. Thus $\hat{C} \subset D$. Since $\dim(\hat{C}) = \dim(D)$, we conclude that $\hat{C} = D$. Thus H is a partiy check matrix for $\hat{C}$.

(3) Find the minimum distance of the ternary linear code C with generator matrix

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

Solution: First we construct a parity check matrix: $H = \begin{pmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}$. This matrix has three linearly dependent columns (e.g., column 1 + column 2 - column 6 is the zero column), no zero columns, no two columns that are scalar multiples of each other. Thus the minimum distance is 3.

(4) Construct a generator matrix and a parity check matrix for the ternary Hamming code $\mathrm{Ham}(2, 3)$.

Solution: Parity check matrix : $H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$. Generator matrix: $G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$. Note that other answers are possible here; see the discussion on pp. 86–87 in the text.

(5) Assume a codeword $\mathbf{x}$ from for the ternary Hamming code $\mathrm{Ham}(2, 3)$ was sent and the word $\mathbf{y}$ was received. Use the partiy check matrix you constructed in Problem 4 to decode $\mathbf{y}$ in each part using syndrome decoding:

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

(b) $\mathbf{y} = (2, 2, 2, 2)$,

(c) $\mathbf{y} = (1, 2, 1, 2)$.

Solution: The decoding algorithm here is the one described at the bottom of page 88 in the book. Denote the columns fof H by K_1, K_2, K_3 and K_4.

(a) $S(\mathbf{y}) = (0, 0)$. Assume no error. Decode $\mathbf{y}$ as $\mathbf{x} = \mathbf{y} = (1, 1, 1, 0)$.

(b) $S(\mathbf{y}) = (0, 2) = 2K_4$. Assume one error of magnitude 2 in position 4. Decode $\mathbf{y}$ as

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

(c) $S(\mathbf{y}) = (1, 1) = K_1$. Assume one error of magnitude 1 in position 1. Decode $\mathbf{y}$ as

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

(6) Find the minimum distance of the binary linear code C with generator matrix

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

Show that $C \neq C^\perp$ but that C is equivalent to $C^\perp$.

Solution: Since G is in standard form we can easily find the parity check matrix:

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

Note that every row of G has even weight. Hence, every word in C has even weight, and $d(C)$ is thus even. The first column in H is equal to the sum of columns 6, 9 and 10 so there are four linearly dependent columns. This means that the minimum distance is at most 4. On the other hand, no two columns of H are equal, so $d(C) > 2$. Thus $d(C) = 4$.

To check that C is equivalent to $C^\perp$, note that the generator matrix H of $C^\perp$ can be obtained from the generator matrix G of C by permuting the columns.

To see that $C \neq C^\perp$ (i.e., C is not self-dual), note that rows 1 and 3 of G are not orthogonal.

(7) Recall that a linear code C is self-dual if $C = C^\perp$. Show that the extended binary Hamming code Hâm(3, 2) is self-dual.

Solution: We can take a generating matrix for $\text{Hâm}(3, 2)$ to be

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

Since every row of G is orthogonal to every other row, $\text{Hâm}(3, 2) \subset \text{Hâm}(3, 2)^\perp$. Since each has dimension 4, we actually have equality.

(8) Problem 8.10. Assume $q \geq 3$ is a prime.

Solution: First note that $A_q(n, 3) \leq q^{n-2}$ by the Singleton bound. To prove that $A_q(n, 3) \geq q^{n-2}$, we will construct a linear q-ary code C of length n, dimension $k = 2$ and minimal distance 3. This code will have q^{n-2} words, thus showing that $A_q(n, 3) \geq q^{n-2}$, as desired.

To define such a code, start with the parity check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & & q-1 \end{pmatrix}.$$

Note that H has two rows and $q+1$ columns. Let H' be the $2 \times n$ matrix obtained from H by keeping the first n columns and removing the rest. (Here we use the assumption that $n \leq q + 1$.) Since $n \geq 3$, the first three colums survive. In particular, H' is in standard form, its rows are linearly independent, its first three columns are linearly dependent,

and no two columns are linearly dependent. We conclude that the code C defined by H' has length n, dimension $n-2$, and minimal distance 3. These are precisely the properties we wanted.