Solutions to Problem Set 6.

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

Questions 1-3 concern a general q-ary BCH code C defined by a parity check matrix of the form

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \dots & \dots & \dots & \dots \\ a_1^{d-1} & a_2^{d-1} & \dots & a_n^{d-1} \end{pmatrix}.$$

Here $1 \leq d+1 \leq n \leq q$ and $a_1, \dots, a_n$ are distinct elements of F_q. We showed in class that $d(C) = d+1$.

Problem 1. Show that H can be row reduced to a matrix of the form $H' = \begin{pmatrix} B & I_d \end{pmatrix}$, where B is a $d \times (n-d)$ matrix and I_d is the $d \times d$ identity matrix. Conclude that C has a generator matrix in standard form.

Solution: Write $H = \begin{pmatrix} X & Y \end{pmatrix}$, where X is a $d \times (n-d)$ matrix and

$$Y = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_{n-d+1} & a_{n-d+1} & \dots & a_n \\ \dots & \dots & \dots & \dots \\ a_{n-d+1}^{d-1} & a_{n-d+2}^{d-1} & \dots & a_n^{d-1} \end{pmatrix}$$

is the $d \times d$ matrix. Let us apply row operations to H to reduce Y to reduced echelon form E. In this way we will reduce H to a matrix of the form

$$H' = \begin{pmatrix} B & E \end{pmatrix}.$$

Our goal is to show that E is the $d \times d$ identity matrix I_d, or equivalently, E has no zero rows. In other words, we want to show that the rows of E are linearly independent. Since E and Y have the same row space, this is equivalent to the rows of Y being linearly independent. But Y is a $d \times d$ Vandermonde matrix, and we showed in class that the rows of a Vandermonde matrix are linearly independent. This shows that $E = I_d$.

Finally, we can use H' to construct a generator matrix in standard from for C,

$$G = \begin{pmatrix} I_{n-d} & -B^T \end{pmatrix}.$$

Problem 2. Show that if $d = n-1$, then C is equivalent to the q-ary repetition code of length n. Recall that the repetition code is a q-ary linear code with generator matrix $G = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$.

Solution: C is a 1-dimensional linear q-ary code of length n and minimal distance n. Hence C has generator matrix $M = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix}$, where $a_1, \dots, a_n \neq 0$ in F_q.

Denote the q-ary repetiton code of length n with generator matrix $G = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$ by R. Since M can be obtained from G by multiplying column i by a_i, C and R are equivalent; see Theorem 5.4.

Problem 3. (a) How many binary BCH codes C are there? Find a generator matrix and the minimal distance for each C. (b) Same question for ternary codes.

Solution: Recall that $1 \leq d+1 \leq n \leq q$.

First assume that $d = 0$. Then the parity check matrix is empty, so $C = V(n,q) = F_q^n$ is the code consisting of all q-ary words of length n. A generaror matrix for this code is I_n, the $n \times n$ identity matrix, and the minimal distance is $d+1 = 1$. From now on, let us assume that $d \geqslant 1$.

(a) If $q = 2$ and $d \geq 1$, then $n = 2$ and $d = 1$. Arguing as in Problem 2, we see that C is a 1-dimensional code with $d = n = 2$ and generator matrix of the form $G = \begin{pmatrix} a_1 & a_2 \end{pmatrix}$, where $a_1, a_2 \neq 0$. Since $a_1, a_2 \in F_2$, this means that the generator matrix $G = \begin{pmatrix} 1 & 1 \end{pmatrix}$. This is the binary repetition code of length 2. The minimal distance of this code is $d+1 = 2$.

(b) Now assume $q = 3$ and $d \geq 1$. If $d = 2$, then $n = 3$, and the reasoning is the same as in part (a): C is a 1-dimensional code of minimal distance 3 with generator matrix

$$G = \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix},$$

where $a_1, a_2, a_3 \in \{1, 2\}$. There are 8 choices of a_1, a_2, a_3 but only 4 codes of this form, since (a_1, a_2, a_3) and $(2a_1, 2a_2, 2a_3)$ generate the same code. By Problem 2 all of these codes are equivalent to the ternary repetition code of length 3.

Now suppose $q = 3$ and $d = 1$. Here $n = 2$ and $H = \begin{pmatrix} 1 & 1 \end{pmatrix}$ or $n = 3$ and $H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. These are ternary parity check codes of length 2 and 3. The minimal distances are $d+1 = 2$ in both cases, and generator matrices are readily produced from H: for $n = 2$,

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

and for $n = 3$

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

Problem 4. Let $q > 2$ be a prime integer. Show that exactly half of the $q-1$ non-zero elements of F_q are squares, and the rest are non-squares. (For $q = 11$ the non-zero squares are 1, 3, 4, 5 and 9; see the table on p. 130.)

Solution: The non-zero elements of F_q come in pairs, $\{x, -x\}$, where $x = 1, \ldots, \dfrac{q-1}{2}$. x and $-x$ have the same square. Hence, there are at most $\dfrac{q-1}{2}$ squares,

$$1^2, 2^2, \ldots, (\frac{q-1}{2})^2.$$

It remains to show that these squares are all distinct. Indeed, if $x^2 = y^2$ in F_q, then $x^2 - y^2 = 0$ or equivalently, $(x-y)(x+y) = 0$. Since F_q is a field, this can only happen

if $x - y = 0$ or $x + y = 0$, i.e., $x = y$ or $x = -y$. This tells us that the $\frac{q-1}{2}$ squares we found,

$$1^2, 2^2, \ldots, (\frac{q-1}{2})^2,$$

are distinct.

Problems 5–8 below concern the specific code in Example 11.3, with $q = 11$, $n = 10$, $d = 4$, and $a_1 = 1$, $a_2 = 2, \ldots, a_{10} = 10$. In each problem use the decoding scheme in Example 11.3 to decode the received word $\mathbf{y}$, if possible. Recall that decoding is possible if at most two errors occurred in transmission and impossible if three or more errors occurred.

Problem 5. $\mathbf{y} = (0, 0, 0, 8, 0, 0, 1, 7, 0, 0)$.

Solution: We follow the decoding algorithm in Example 11.3. We begin by computing the syndrome $S(\mathbf{y}) = (s_1, s_2, s_3, s_4) = (5, 7, 9, 6)$. Next we compute the coefficients of the error-locator polynomial:

$P = s_2^2 - s_1 s_3 = 4$, $Q = s_1 s_4 - s_2 s_3 = 0$, $R = s_3^2 - s_2 s_4 = 6$.

Here all computations are done modulo 11. The resulting polynomial $4x^2 + 6$, has two roots, $x = 2$ and $x = -2 = 9$. These are the error positions. We now solve for error magnitudes, a (in position 2) and b (in position 9):

$a + b = s_1 = 5$

$2a - 2b = s_2 = 7$

Multiplying the first equation by 2 and adding to the second, we obtain $4a = 17$ or $a = 7$ in F_{11}. Now, from the first equation $b = -2 = 9$.

To check this answer, we substitute $a = 7$ and $b = -2$ into $4a + 4b = s_3 = -2$ and $8a - 8b = s_4 = 6$. These check out. Thus our error vector is

$$\mathbf{e} = (0, 7, 0, 0, 0, 0, 0, 0, 9, 0).$$

We decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (0, 4, 0, 8, 0, 0, 1, 7, 2, 0).$$

Problem 6. $\mathbf{y} = (1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$.

Solution: Once again, we follow the decoding algorithm in Example 11.3. First compute the syndrome: $S(\mathbf{y}) = (s_1, s_2, s_3, s_4) = (3, 6, 3, 3)$, then the coefficients of the error-locator polynomial:

$P = s_2^2 - s_1 s_3 = 5$, $Q = s_1 s_4 - s_2 s_3 = 2$, $R = s_3^2 - s_2 s_4 = 2$.

Here all computations are done modulo 11. The resulting polynomial $5x^2 + 2x + 2$, has no roots in F_{11}, because the discriminant $D = 2^2 - 4 \cdot 5 \cdot 2 = -36 = -3 = 8$ is not a square in F_{11}. Thus we are in case (iv) of the decoding algorithm: at least three errors occurred, and $\mathbf{y}$ is too corrupted to be decoded.

Problem 7. $\mathbf{y} = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$.

Solution: Once again, we compute the syndrome,

$$S(\mathbf{y}) = (s_1, s_2, s_3, s_4) = (4, 10, 8, 1),$$

and the coefficients of the error-locator polynomial:

$P = s_2^2 - s_1 s_3 = 2$, $Q = s_1 s_4 - s_2 s_3 = 1$, $R = s_3^2 - s_2 s_4 = -1$.

The resulting polynomial $2x^2 + x - 1$, has discriminant $D = 1^2 + 8 = 9$ and two roots, $x = -1 = 10$ and $x = 6$. These are the error positions. We now solve for error magnitudes, a (in position 6) and b (in position 10):

$a + b = s_1 = 4$

$6a - b = s_2 = 10$

Adding these two equations, we obtain $7a = 14$, so $a = 2$. Now from the first equation, $b = 2$.

To check this answer, we substitute $a = b = 2$ into $6^2 a + b = s_3 = 8$ and $6^3 a - b = s_4 = 1$. These check out. Thus our error vector is

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

We decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (1, 1, 1, 1, 0, 9, 0, 0, 0, 9).$$

Problem 8. $\mathbf{y} = (2, 2, 2, 2, 0, 0, 0, 0, 0, 7)$.

Solution: We begin by computing the syndrome: $S(\mathbf{y}) = (s_1, s_2, s_3, s_4) = (4, 2, 1, 6)$. Next we compute the coefficients of the error-locator polynomial:

$P = s_2^2 - s_1 s_3 = 0$, $Q = s_1 s_4 - s_2 s_3 = 0$, $R = s_3^2 - s_2 s_4 = 0$.

Thus we are in case (ii) of the decoding algorithm (see p. 130 in the book). We assume one error with error magnitude $s_1 = 4$ and error location $S_2/s_1 = 2/4 = 1/2 = 6$. Thus our error vector is

$$\mathbf{e} = (0, 0, 0, 0, 0, 4, 0, 0, 0, 0),$$

and we decode $\mathbf{y}$ as

$$\mathbf{x} = \mathbf{y} - \mathbf{e} = (2, 2, 2, 2, 0, 7, 0, 0, 0, 7).$$