Problem 1. Consider the $[15, 7, 5]$ 2-error correcting BCH code, whose parity check matrix is expressed over $GF(2^4)$ by:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^i & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3i} & \cdots & \alpha^{12} \end{pmatrix}$$

- Write the columns of H in binry form

$$H = \left(\begin{array}{ccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

- A message y is received, the syndrome is computed and is found to be $S = (0, 1, 0, 0, 0, 1, 1, 1)^{tr}$. What can you say about any error(s) that have occured during transmission.

  $z_1 = (0100) = \alpha^2$ and $z_2 = (0111) = \alpha^{10} \neq z_1^3$. If we solve the equation

  $$x^2 + \alpha^2 x + (\frac{\alpha^{10}}{\alpha^2} + (\alpha^2)^2) = x^2 + \alpha^2 x + \alpha^{13} = 0$$

  and find that the quadratic has no roots. Therefore, at least three errors have occured

- Repeat with syndrome $S = (1, 0, 1, 1, 1, 1, 0, 0)^{tr}$

  $z_1 = (1011) = \alpha^7$ and $z_2 = (1100) = \alpha^6 = z_1^3$. And so there is a single error at $i = z_1 = 7$

- Repeat with syndrome $S = (0, 1, 1, 1, 0, 1, 1, 0)^{tr}$

  $z_1 = (0111) = \alpha^{10}$ and $z_2 = (0110) = \alpha^5 \neq z_1^3$. If we solve the equation

  $$x^2 + \alpha^{10} x + (\frac{\alpha^5}{\alpha^{10}} + (\alpha^{10})^2) = x^2 + \alpha^{10} x + 1 = 0$$

  The equation has two roots at $i = 3, 12$, and so there are two errors at those locatons.

Problem 2.

Problem 3. Suppose that $\mathbb{F}$ is a field of order p^m, α a primitive element of $\mathbb{F}$ and suppose that C_s is the cyclotomic coset of s modulo $p^m - 1$

- Prove that

  $$\prod_{j \in C_s} (x - a^j) \in \mathbb{Z}_p[x]$$

  Let C_s be the cyclotomic coset of s, and let $M^{(s)}(x)$ be the minimal polynmial of a^s. Then for any n, $sp^n \in C_s$. Additionally, since $\mathbb{F}$ has order p^m, it has characteristic p. That is, we can easily show that $(a+b)^p = a^p + b^p$ using the Binomial theorem. Hence, for any polynomial $f \in \mathbb{F}$, $f(\beta^p) = f(\beta)^p$. So

  $$M^{(s)}(a^{sp^n}) = M^{(s)}((a^s)^{p^n}) = M^{(s)}(a^s)^{p^n} = 0$$

  So we have shown that for any $i, j \in C_s$, $M^{(i)}(x) = M^{(j)}(x)$. Since each $j \in C_s$ satisfies $M^{(s)}(a^j) = 0$, we have

  $$\prod_{j \in C_s} (x - a^j) \text{ divides } M^{(s)}(x)$$

- Illustrate the above result with $p^m = 16$, and $s = 3$.

  We will use $\mathbb{F} = GF(16)$. We have $C_s = \{3, 6, 12, 9\}$. Then

  $$\prod_{j \in C_s} (x - a^j) = (x - a^3)(x - a^6)(x - a^{12})(x - a^9) = x^4 + x^3 + x^2 + x + 1 \in Z_2[x]$$

  (the above was computed using Julia's Nemo Library)

Problem 4. Prove that

- $A_q(n, 1) = q^n$ Consider all the q-ary words of length n. There are exactly q^n of them. Additionally, distinct words always have a distance of at least one. Hence the code C containing all the q-ary words of length n is a (n, q^n, q) code. Since there are no more words to add, we have $A_q(n, 1) = q^n$.

- Assume we have a (n, M, n) code such that $M > q$. Then, by the pigeonhole principle, there must be two words, s_1, s_2 that have the same first digit. Then $d(s_1, s_2) \leq n-1$, and so we have a contradiction. Hence $A_q(n, n) \leq q$. Additionally, the repetiton code of length n is a (n, q, n) code, and so $A_q(n, n) = q$.

Problem 5. Construct, if possible binary (n, M, d) codes with the following parameters:

- (6,2,6)

  As discussed in the previous problem, this is the binary repetition code of length 6. That is , the two code words are (000000), and (111111).

- (3,8,1)

  As discussed in the previous problem, this is the code containing all binary words of length 3.

- (4,8,2)

  Consider the code $C = \{(0000), (1111), (1100), (0011), (1010), (0101), (1001), (0110)\}$

- (5,3,4)

  These parameters fail the Plotkin bound, since $3 > 2\lfloor \frac{4}{3} \rfloor = 2$

- (8,30,3)

Problem 6. Let C be a binary (n, M, d) code. Now consider that there are N words in C that have a 1 in the first column. Then there are $M - N$ words with 0, and one of either N or $M - N$ is $\geq M/2$. Now, let us delete only the words with a 1, or 0 in the first column (whichever one is fewer). We are left with a (n, M', d) code, where $M' \geq M/2$. Now we can simply puncture the first column, and the distance between the words will not change, since all the words remaining agree in the first column.

Now let $M = A_2(n, d)$. Then there exists $M' \geq M/2$. Hence $A_2(n, d) = M \leq 2M' \leq 2A_2(n-1, d)$.