

1. How many cyclic codes of length 4 are there over $GF(3)$? Write down the generator polynomial for each of these cyclic codes.

Solution : (a) The cyclotomic cosets depending on $n = 4$ and $q = 3$ are

$$\{0\} , \{1, 3\} \text{ and } \{2\}$$

So $x^4 - 1$ has three irreducible factors over $GF(3)$. Over \mathbb{Z} , we easily get that

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$$

So this is also the factorization of $x^4 - 1$ into irreducible factors over $GF(3)$. If β is an element of order 4 in some field extension of $GF(3)$ (namely $GF(9)$) then

$$x - 1 = x - \beta^0 , x + 1 = x - \beta^2 \text{ and } x^2 + 1 = (x - \beta^1)(x - \beta^3)$$

Since there are three factors, there are $2^3 = 8$ cyclic codes of length 4 over $GF(3)$. The generator polynomials for these eight codes are

Cosets Used	Generator Polynomial
none	1
{0}	$x - 1$
{2}	$x + 1$
{1, 3}	$x^2 + 1$
{0}, {2}	$(x - 1)(x + 1) = x^2 - 1$
{0}, {1, 3}	$(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$
{2}, {1, 3}	$(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1$
{0}, {2}, {1, 3}	$(x - 1)(x + 1)(x^2 + 1) = x^4 - 1 = 0$

2. Let C be a binary cyclic code of length n (note that n is odd). Prove that exactly one of the following holds:

- Every codeword in C has even weight.
- The word $11 \dots 11$ is a codeword.

Proof : Note that the word $11 \dots 11$ has weight n and n is odd. So at most one of the above holds. We show that one of the above does hold.

Let $g(x)$ be the generator polynomial of C .

Suppose that not every codeword has even weight. Then $1 + x$ does not divide $g(x)$ by HW 5 # 3. So $\gcd(1 + x, g(x)) = 1$. Since $g(x)$ divides $x^n - 1$ and

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x^2 + x + 1)$$

we get that $g(x)$ divides $1 + x + x^2 + \dots + x^{n-2} + x^{n-1}$. So $1 + x + x^2 + \dots + x^{n-2} + x^{n-1}$ is a codeword polynomial. Hence the corresponding word $11 \dots 11$ is a codeword. \square

3. In this exercise, you are asked to construct BCH-codes of length 15 and designed distance 5 over certain fields. Try to find an example with maximal dimension. For each code, you must identify b and the dimension.

- (a) over $GF(4)$.
- (b) over $GF(16)$.

Solution : (a) The cyclotomic cosets depending on $n = 15$ and $q = 4$ are

$$\{0\} , \{1, 4\} , \{2, 8\} , \{3, 12\} , \{5\} , \{6, 9\} , \{7, 13\} , \{10\} \text{ and } \{11, 14\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) = x - \beta^0 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^4}(x) = (x - \beta^1)(x - \beta^4) \\ g_2(x) &:= m_{\beta^2}(x) = m_{\beta^8}(x) = (x - \beta^2)(x - \beta^8) \\ g_3(x) &:= m_{\beta^3}(x) = m_{\beta^{12}}(x) = (x - \beta^3)(x - \beta^{12}) \\ g_4(x) &:= m_{\beta^5}(x) = x - \beta^5 \\ g_5(x) &:= m_{\beta^6}(x) = m_{\beta^9}(x) = (x - \beta^6)(x - \beta^9) \\ g_6(x) &:= m_{\beta^7}(x) = m_{\beta^{13}}(x) = (x - \beta^7)(x - \beta^{13}) \\ g_7(x) &:= m_{\beta^{10}}(x) = x - \beta^{10} \\ g_8(x) &:= m_{\beta^{11}}(x) = m_{\beta^{14}}(x) = (x - \beta^{11})(x - \beta^{14}) \end{aligned}$$

Since $\delta = 5$ we need $\delta - 1 = 4$ consecutive roots. So

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x))$$

for some b . We want to choose b such that $\deg(g(x))$ is minimal. By going over all possibilities for b , we get that

$$\deg(g(x)) = \begin{cases} 6 & \text{if } b \in \{1, 6, 11\} \\ 7 & \text{if } b \in \{0, 2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14\} \end{cases}$$

For example, if $b = 1$ then

$$g(x) = \text{lcm}(m_{\beta^1}(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x)) = \text{lcm}(g_1(x), g_2(x), g_3(x), g_1(x)) = g_1(x)g_2(x)g_3(x)$$

So

$$\deg(g(x)) = \deg(g_1(x)g_2(x)g_3(x)) = \deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)) = 2 + 2 + 2 = 6$$

Hence

$$\dim(C) = n - \deg(g(x)) = 15 - 6 = 9$$

(b) This exercise is actually about Reed-Solomon codes.

Let β be an element of order 15 in some field extension of $GF(16)$. Then we have that $\beta \in GF(16)$. So $\beta^i \in GF(16)$ for all i . Hence the minimal polynomial $m_{\beta^i}(x)$ of β^i over $GF(16)$ is

$$m_{\beta^i}(x) = x - \beta^i$$

Or put another way: all the cyclotomic cosets are singletons.

Since $\delta = 5$, we need to pick $\delta - 1 = 4$ consecutive roots. So no matter what value of b we choose, we always have that

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x)) = (x - \beta^b)(x - \beta^{b+1})(x - \beta^{b+2})(x - \beta^{b+3})$$

So $\deg(g(x)) = 4$ and $\dim(C) = 15 - 4 = 11$. □

4. Construct a BCH-code of length 17 and dimension 9 over $GF(4)$ that can correct at least three errors.

Solution : Since the code must be able to correct at least three errors, the minimum distance of the code must be at least $2 \cdot 3 + 1 = 7$. So we choose $\delta = 7$. Since the dimension of the code is 9, the degree of the generator polynomial must be $17 - 9 = 8$.

The cyclotomic cosets depending on $n = 17$ and $q = 4$ are

$$\{0\} , \{1, 4, 16, 13\} , \{2, 8, 15, 9\} , \{3, 12, 14, 5\} , \text{ and } \{6, 7, 11, 10\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) = x - \beta^0 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^4}(x) = m_{\beta^{16}}(x) = m_{\beta^{13}}(x) = (x - \beta^1)(x - \beta^4)(x - \beta^{16})(x - \beta^{13}) \\ g_2(x) &:= m_{\beta^2}(x) = m_{\beta^8}(x) = m_{\beta^{15}}(x) = m_{\beta^9}(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{15})(x - \beta^9) \\ g_3(x) &:= m_{\beta^3}(x) = m_{\beta^{12}}(x) = m_{\beta^{14}}(x) = m_{\beta^5}(x) = (x - \beta^3)(x - \beta^{12})(x - \beta^{14})(x - \beta^5) \\ g_4(x) &:= m_{\beta^6}(x) = m_{\beta^7}(x) = m_{\beta^{11}}(x) = m_{\beta^{10}}(x) = (x - \beta^6)(x - \beta^7)(x - \beta^{11})(x - \beta^{10}) \end{aligned}$$

Since $\delta = 7$, we need to pick $\delta - 1 = 6$ consecutive roots. So

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x), m_{\beta^{b+4}}(x), m_{\beta^{b+5}}(x))$$

It turns out that

$$\deg(g(x)) = \begin{cases} 13 & \text{if } b \in \{0, 12, 13, 14, 15, 16\} \\ 12 & \text{if } b \in \{1, 5, 7\} \\ 16 & \text{if } b \in \{2, 3, 4, 8, 9, 10, 11\} \\ 8 & \text{if } b = 6 \end{cases}$$

We choose $b = 6$. Then

$$\begin{aligned} g(x) &= \text{lcm}(m_{\beta^6}(x), m_{\beta^7}(x), m_{\beta^8}(x), m_{\beta^9}(x), m_{\beta^{10}}(x), m_{\beta^{11}}(x)) \\ &= \text{lcm}(g_4(x), g_4(x), g_2(x), g_2(x), g_4(x), g_4(x)) \\ &= g_2(x)g_4(x) \end{aligned}$$

So

$$\deg(g(x)) = \deg(g_2(x)g_4(x)) = \deg(g_2(x)) + \deg(g_4(x)) = 4 + 4 = 8$$

and so

$$\dim(C) = n - \deg(g(x)) = 17 - 8 = 9 \quad \square$$

5. Construct a binary BCH-code of length 31 of designed distance 5 with minimum distance at least 11.

Solution : The cyclotomic cosets depending on $n = 31$ and $q = 2$ are

$$\{0\} , \{1, 2, 4, 8, 16\} , \{3, 6, 12, 24, 17\} , \{5, 10, 20, 9, 18\} , \{7, 14, 28, 25, 19\} , \{11, 22, 13, 26, 21\} \text{ and } \{15, 30, 29, 27, 23\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) && \text{and } \deg(g_0(x)) = 1 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^2}(x) = m_{\beta^4}(x) = m_{\beta^8}(x) = m_{\beta^{16}}(x) && \text{and } \deg(g_1(x)) = 5 \\ g_2(x) &:= m_{\beta^3}(x) = m_{\beta^6}(x) = m_{\beta^{12}}(x) = m_{\beta^{24}}(x) = m_{\beta^{17}}(x) && \text{and } \deg(g_2(x)) = 5 \\ g_3(x) &:= m_{\beta^5}(x) = m_{\beta^{10}}(x) = m_{\beta^{20}}(x) = m_{\beta^9}(x) = m_{\beta^{18}}(x) && \text{and } \deg(g_3(x)) = 5 \\ g_4(x) &:= m_{\beta^7}(x) = m_{\beta^{14}}(x) = m_{\beta^{28}}(x) = m_{\beta^{25}}(x) = m_{\beta^{19}}(x) && \text{and } \deg(g_4(x)) = 5 \\ g_5(x) &:= m_{\beta^{11}}(x) = m_{\beta^{22}}(x) = m_{\beta^{13}}(x) = m_{\beta^{26}}(x) = m_{\beta^{21}}(x) && \text{and } \deg(g_5(x)) = 5 \\ g_6(x) &:= m_{\beta^{15}}(x) = m_{\beta^{30}}(x) = m_{\beta^{29}}(x) = m_{\beta^{27}}(x) = m_{\beta^{23}}(x) && \text{and } \deg(g_6(x)) = 5 \end{aligned}$$

We choose $b = 4$ and $\delta = 5$. So we need $\delta - 1 = 4$ consecutive roots. Hence

$$g(x) = \text{lcm}(m_{\beta^4}(x), m_{\beta^5}(x), m_{\beta^6}(x), m_{\beta^7}(x)) = \text{lcm}(g_1(x), g_3(x), g_2(x), g_4(x)) = g_1(x)g_2(x)g_3(x)g_4(x)$$

However, this generator polynomial has actually ten consecutive roots:

$$\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7, \beta^8, \beta^9 \text{ and } \beta^{10}$$

So the minimum distance is at least $10 + 1 = 11$ (because if we choose $b = 1$ and $\delta = 11$, we end up with exactly the same generator polynomial as when we choose $b = 4$ and $\delta = 5$). \square

6. This exercise is about the relation between certain Hamming codes and cyclic codes.

Let $r \geq 1$. Let α be a primitive element in $GF(2^r)$ (so α is an element of order $n := 2^r - 1$). Then every element of $GF(2^r)$ can be written as a polynomial over $GF(2)$ in α of degree less than r : $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{r-1}\alpha^{r-1}$ where $a_0, a_1, \dots, a_{r-1} \in GF(2)$.

Consider the matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \end{bmatrix}$$

where we write α^j in polynomial form and turn it into a column. Let C be the binary code with H as a parity check matrix.

- (a) H is parity check matrix if the rows of H are linearly independent. What are the dimensions of H ? Are the rows of H linearly independent?

Solution : We turned every α^j into a column of length r . So H is an $r \times n$ -matrix. Notice that the first r columns of H are form the identity matrix (since $\alpha^j = 1 \cdot \alpha^j$ for $0 \leq j \leq r - 1$). So H is indeed of rank r .

- (b) Show that C is a binary Hamming code.

Solution : Since

$$\{\alpha^j : 0 \leq j \leq n - 1\} = \{1, \alpha, \alpha^2, \dots, \alpha^{2^r-2}\} = GF(2^r) \setminus \{0\}$$

we see that the columns of H are all the non-zero columns of length r showing up exactly once. So by definition of Hamming codes, C is a Hamming code!

- (c) Let $\mathbf{w} = (w_0, w_1, \dots, w_{n-1}) \in GF(2)^n$. Prove that $\mathbf{w} \in C$ if and only if $\mathbf{w}(\alpha) = 0$.

Solution : We get that

$$\begin{aligned} \mathbf{w} \in C &\iff H\mathbf{w}^T = \mathbf{0} \\ &\iff \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \end{bmatrix} \begin{bmatrix} w_0 & w_1 & w_2 & \dots & w_{n-1} \end{bmatrix}^T = \mathbf{0} \\ &\iff w_0 \cdot 1 + w_1 \cdot \alpha + w_2 \cdot \alpha^2 + \dots + w_{n-1} \cdot \alpha^{n-1} = 0 \\ &\iff \mathbf{w}(\alpha) = 0 \end{aligned}$$

- (d) Deduce that C is a cyclic code. What is the generator polynomial of C ? What is the dimension of C ?

Solution : Let $\mathbf{c} \in C$. Then

$$\mathbf{c}'(x) \equiv x \mathbf{c}(x) \pmod{x^n - 1}$$

So

$$\mathbf{c}'(x) = x \mathbf{c}(x) + a(x)(x^n - 1)$$

for some polynomial $a(x) \in GF(2)[x]$. Hence

$$\mathbf{c}'(\alpha) = \alpha \mathbf{c}(\alpha) + a(\alpha)(\alpha^n - 1)$$

Since $\mathbf{c} \in C$, we have that $\mathbf{c}(\alpha) = 0$ by (c). Since α is an element of order n , we have that $\alpha^n = 1$ and so $\alpha^n - 1 = 0$. Thus $\mathbf{c}'(\alpha) = 0$. Hence $\mathbf{c}' \in C$ by (c). So C is cyclic.

Let $g(x)$ be the generator polynomial of C and $m(x)$ the minimal polynomial of α over $GF(2)$. Note that $\deg(m(x)) = r$ (recall how we set up a table for $GF(2^r)$).

Since $g(x)$ is a codeword polynomial, it follows from (c) that $g(\alpha) = 0$. Hence $m(x)$ divides $g(x)$ by properties of the minimal polynomial.

Since $\deg(m(x)) = r < n$, we see that $m(x)$ is a word polynomial. But $m(\alpha) = 0$. So $m(x)$ is a codeword polynomial by (c). Thus $g(x)$ divides $m(x)$ by properties of the generator polynomial.

So $m(x)$ divides $g(x)$ and $g(x)$ divides $m(x)$. Since $m(x)$ and $g(x)$ are both monic, we must have that $g(x) = m(x)$. So the generator polynomial of C is the minimal polynomial of α over $GF(2)$ and has degree r . Hence the dimension of C is $n - r = 2^r - 1 - r$.

(e) Prove that the following decoding algorithm is Nearest Neighbor Decoding:

- When receiving a word \vec{w} , evaluate $\vec{w}(\alpha)$.
- If $\vec{w}(\alpha) = 0$ then we decode \vec{w} as \vec{w} .
- If $\vec{w}(\alpha) \neq 0$ then $\vec{w}(\alpha) = \alpha^j$ for a unique $0 \leq j \leq n - 1$ (why?) and we decode \vec{w} as $\vec{w} + \vec{e}_j$ (the word corresponding to $\vec{w}(x) + x^j$).

Solution : Suppose first that $\mathbf{w}(\alpha) = 0$. Then \mathbf{w} is a codeword by (c). So we decode \mathbf{w} as \mathbf{w} (namely \mathbf{w} is the unique codeword closest to \mathbf{w}).

Suppose next that $\mathbf{w}(\alpha) \neq 0$. Since

$$GF(2^r) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

we see that there is a unique $0 \leq j \leq n - 1$ such that $\mathbf{w}(\alpha) = \alpha^j$. So $\mathbf{w}(\alpha) + \alpha^j = 0$. Hence $\mathbf{w}(x) + x^j$ is a codeword polynomial, say $\mathbf{w}(x) + x^j = \mathbf{c}(x)$ where $\mathbf{c} \in C$. Note that \mathbf{w} is not a codeword (by (c)) and $d(\mathbf{w}, \mathbf{c}) = 1$. Since the minimum distance of C is 3, \mathbf{c} is the unique codeword at distance 1 of \mathbf{w} (indeed, if $d(\mathbf{w}, \mathbf{c}') = 1$ for some $\mathbf{c}' \in C$ then $d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{c}, \mathbf{w}) + d(\mathbf{w}, \mathbf{c}') = 2 < d(C)$ and so $\mathbf{c} = \mathbf{c}'$). Hence we decode \mathbf{w} as \mathbf{c} . \square