Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 17

March 21, 2023

Cyclic codes

Observation

$\rightarrow$ For every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in F_q^n$, the polynomial is

$$\mathbf{c}(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

Cyclic codes

Observation

$\rightarrow$ For every codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in F_q^n$, the polynomial is

$$\mathbf{c}(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

$\rightarrow$ The codeword polynomial corresponding to the shifted codeword $\widetilde{\mathbf{c}}$ is

$$\widetilde{\mathbf{c}}(x) = c_{n-1} + c_0 x + c_1 x^2 + \dots + c_{n-2} x^{n-1} = x\mathbf{c}(x) - c_{n-1}(x^n - 1)$$

Cyclic codes

Observation

→ For every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in F_q^n$, the polynomial is

$$\mathbf{c}(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

→ The codeword polynomial corresponding to the shifted codeword $\widetilde{\mathbf{c}}$ is

$$\widetilde{\mathbf{c}}(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2}x^{n-1} = x\mathbf{c}(x) - c_{n-1}(x^n - 1)$$

→ Then

$$\widetilde{\mathbf{c}}(x) = x\mathbf{c}(x) \bmod (x^n - 1)$$

Cyclic codes

Observation

→ For every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in F_q^n$, the polynomial is

$$\mathbf{c}(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$$

→ The codeword polynomial corresponding to the shifted codeword $\widetilde{\mathbf{c}}$ is

$$\widetilde{\mathbf{c}}(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1} = x\mathbf{c}(x) - c_{n-1}(x^n - 1)$$

→ Then

$$\widetilde{\mathbf{c}}(x) = x\mathbf{c}(x) \bmod (x^n - 1)$$

→ If $f(x)$ is any polynomial of $F[x]$ whose remainder, upon division by $x^n - 1$, belongs to C then we may write

$$f(x) \in C \bmod (x^n - 1)$$

Cyclic codes

→ For any i, and the cyclic code C, we have

$$x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

Cyclic codes

→ For any i, and the cyclic code C, we have

$$x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

→ By linearity, for any $a_i \in F$,

$$a_i x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

and indeed

$$\sum_{i=0}^{d} a_i x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

Cyclic codes

→ For any i, and the cyclic code C, we have

$$x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

→ By linearity, for any $a_i \in F$,

$$a_i x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

and indeed

$$\sum_{i=0}^{d} a_i x^i \mathbf{c}(x) \in C \bmod (x^n - 1)$$

→ Thus for every polynomial $a(x) = \sum_{i=0}^{d} a_i x^i \in F[x]$, the product $a(x)\mathbf{c}(x)$ still belongs to C

Cyclic codes

Theorem Let $C \neq \{\mathbf{0}\}$ be a cyclic code of length n over F

1. Let $g(x)$ be a monic code polynomial of minimal degree in C. Then $g(x)$ is uniquely determined in C, and

$$C = \{q(x)g(x)\,|q(x) \in F[x]_{n-r}\}$$

where $r = deg((g(x)))$. In particular, C has dimension $n - r$

Cyclic codes

Theorem Let $C \neq \{\mathbf{0}\}$ be a cyclic code of length n over F

1. Let $g(x)$ be a monic code polynomial of minimal degree in C. Then $g(x)$ is uniquely determined in C, and
$$C = \{q(x)g(x)\,|q(x) \in F[x]_{n-r}\}$$
where $r = deg((g(x)))$. In particular, C has dimension $n - r$
2. The polynomial $g(x)$ divides $x^n - 1$ in $F[x]$

Cyclic codes

Proof

1. As $C \neq \{\mathbf{0}\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g(x)$ in C of minimal degree. Let this degree be r, unique even if $g(x)$ is not.

Cyclic codes

Proof

1. As $C \neq \{\mathbf{0}\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g(x)$ in C of minimal degree. Let this degree be r, unique even if $g(x)$ is not. Then the set of polynomials

$$C_0 = \{q(x)g(x) | q(x) \in F[x]_{n-r}\} \subseteq C.$$

Cyclic codes

Proof

1. As $C \neq \{\mathbf{0}\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g(x)$ in C of minimal degree. Let this degree be r, unique even if $g(x)$ is not. Then the set of polynomials

$$C_0 = \{q(x)g(x) | q(x) \in F[x]_{n-r}\} \subseteq C.$$

Under addition and scalar multiplication, C_0 is a vector space over F of dimension $n - r$.

Cyclic codes

Proof

1. As $C \neq \{\mathbf{0}\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g(x)$ in C of minimal degree. Let this degree be r, unique even if $g(x)$ is not. Then the set of polynomials

$$C_0 = \{q(x)g(x) | q(x) \in F[x]_{n-r}\} \subseteq C.$$

   Under addition and scalar multiplication, C_0 is a vector space over F of dimension $n - r$.
   To prove 1., we must show that every code polynomial $\mathbf{c}(x)$ is an $F[x]$-multiple of $g(x)$ and so is in C_0.

Cyclic codes

Proof

1. As $C \neq \{\mathbf{0}\}$, it contains nonzero code polynomials, each of which has a unique monic scalar multiple. Thus there is a monic polynomial $g(x)$ in C of minimal degree. Let this degree be r, unique even if $g(x)$ is not. Then the set of polynomials

$$C_0 = \{q(x)g(x) | q(x) \in F[x]_{n-r}\} \subseteq C.$$

Under addition and scalar multiplication, C_0 is a vector space over F of dimension $n - r$.

To prove 1., we must show that every code polynomial $\mathbf{c}(x)$ is an $F[x]$-multiple of $g(x)$ and so is in C_0.By division algorithm, we have

$$\mathbf{c}(x) = q(x)g(x) + r(x)$$

for some $q(x), r(x) \in F[x]$ with $deg((r(x))) < r = deg(g(x))$

Cyclic codes

Thus

$$r(x) = \mathbf{c}(x) - q(x)g(x).$$

Cyclic codes

Thus

$$r(x) = \mathbf{c}(x) - q(x)g(x).$$

By definition, $\mathbf{c}(x) \in C$ and $q(x)g(x) \in C_0$ (as $\mathbf{c}(x)$ has degree less than n)

Cyclic codes

Thus

$$r(x) = \mathbf{c}(x) - q(x)g(x).$$

By definition, $\mathbf{c}(x) \in C$ and $q(x)g(x) \in C_0$ (as $\mathbf{c}(x)$ has degree less than n) Thus by linearity $r(x) \in C$.

Cyclic codes

Thus
$$r(x) = \mathbf{c}(x) - q(x)g(x).$$
By definition, $\mathbf{c}(x) \in C$ and $q(x)g(x) \in C_0$ (as $\mathbf{c}(x)$ has degree less than n) Thus by linearity $r(x) \in C$. If $r(x)$ was nonzero, then it would have a monic scalar multiple belonging to C and of smaller degree than r. But this would contradict the original choice of $g(x)$.

Cyclic codes

Thus

$$r(x) = \mathbf{c}(x) - q(x)g(x).$$

By definition, $\mathbf{c}(x) \in C$ and $q(x)g(x) \in C_0$ (as $\mathbf{c}(x)$ has degree less than n) Thus by linearity $r(x) \in C$. If $r(x)$ was nonzero, then it would have a monic scalar multiple belonging to C and of smaller degree than r. But this would contradict the original choice of $g(x)$.
Thus $r(x) = 0$ and $\mathbf{c}(x) = q(x)g(x)$

Cyclic codes

Thus

$$r(x) = \mathbf{c}(x) - q(x)g(x).$$

By definition, $\mathbf{c}(x) \in C$ and $q(x)g(x) \in C_0$ (as $\mathbf{c}(x)$ has degree less than n) Thus by linearity $r(x) \in C$. If $r(x)$ was nonzero, then it would have a monic scalar multiple belonging to C and of smaller degree than r. But this would contradict the original choice of $g(x)$.
Thus $r(x) = 0$ and $\mathbf{c}(x) = q(x)g(x)$
Proof of 2. Next let $x^n - 1 = h(x)g(x) + s(x)$ for some $s(x)$ of degree less than $deg(g(x))$. Then as before

$$s(x) = (-h(x))g(x) \bmod (x^n - 1)$$

and $s(x) \in C$. Further, if $s(x)$ is nonzero then it has a monic scalar multiple belonging to C and of smaller degree than that of $g(x)$, contradiction. Thus $s(x) = 0$ and $g(x)h(x) = x^n - 1$

Cyclic codes

Generator polynomial and check polynomial The polynomial $g(x)$ is called the generator polynomial for the code C.

Cyclic codes

Generator polynomial and check polynomial The polynomial $g(x)$ is called the generator polynomial for the code C. The polynomial $h(x) \in F[x]$ determined by

$$g(x)h(x) = x^n - 1$$

is the check polynomial in C

Cyclic codes

Generator polynomial and check polynomial The polynomial $g(x)$ is called the generator polynomial for the code C. The polynomial $h(x) \in F[x]$ determined by

$$g(x)h(x) = x^n - 1$$

is the check polynomial in C

Under some circumstances it is convenient to consider $x^n - 1$ to be the generator polynomial of the cyclic code $\mathbf{0}$ of length n. Then by the above theorem, there is a one-to-one correspondence between cyclic codes of length n and monic divisors of $x^n - 1$ in $F[x]$.

Cyclic codes

Generator polynomial and check polynomial The polynomial $g(x)$ is called the generator polynomial for the code C. The polynomial $h(x) \in F[x]$ determined by

$$g(x)h(x) = x^n - 1$$

is the check polynomial in C

Under some circumstances it is convenient to consider $x^n - 1$ to be the generator polynomial of the cyclic code $\mathbf{0}$ of length n. Then by the above theorem, there is a one-to-one correspondence between cyclic codes of length n and monic divisors of $x^n - 1$ in $F[x]$.

Example Consider length 7 binary cyclic codes. The factorization of the irreducible polynomial

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Thus

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Cyclic codes

Proposition if C is a cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in F[x]_n | c(x)h(x) = 0 \bmod (x^n - 1)\}$

Cyclic codes

Proposition if C is a cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in F[x]_n | c(x)h(x) = 0 \bmod (x^n - 1)\}$
Proof if $c(x) \in C$ then there is $q(x)$ such that $c(x) = q(x)g(x)$. But then

$$c(x)h(x) = q(x)g(x)h(x) = q(x)(x^n - 1) = 0 \bmod (x^n - 1).$$

Cyclic codes

Proposition if C is a cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in F[x]_n | c(x)h(x) = 0 \bmod (x^n - 1)\}$
Proof if $c(x) \in C$ then there is $q(x)$ such that $c(x) = q(x)g(x)$. But then

$$c(x)h(x) = q(x)g(x)h(x) = q(x)(x^n - 1) = 0 \bmod (x^n - 1).$$

Now consider an arbitrary polynomial $c(x) \in F[x]_n$ with $c(x)h(x) = p(x)(x^n - 1)$, say. Then

$$c(x)h(x) = p(x)(x^n - 1) = p(x)g(x)h(x),$$

hence

$$(c(x) - p(x)g(x))h(x) = 0$$

Cyclic codes

Proposition if C is a cyclic code of length n with check polynomial $h(x)$, then $C = \{c(x) \in F[x]_n | c(x)h(x) = 0 \bmod (x^n - 1)\}$
Proof if $c(x) \in C$ then there is $q(x)$ such that $c(x) = q(x)g(x)$. But then

$$c(x)h(x) = q(x)g(x)h(x) = q(x)(x^n - 1) = 0 \bmod (x^n - 1).$$

Now consider an arbitrary polynomial $c(x) \in F[x]_n$ with $c(x)h(x) = p(x)(x^n - 1)$, say. Then

$$c(x)h(x) = p(x)(x^n - 1) = p(x)g(x)h(x),$$

hence

$$(c(x) - p(x)g(x))h(x) = 0$$

As $g(x)h(x) = x^n - 1$, we do not have $h(x) = 0$. Therefore $(c(x) - p(x)g(x))h(x) = 0$ and $c(x) = p(x)g(x)$ as desired

Cyclic codes

Generator matrix If $g(x) = \sum_{j=0}^{r} g_j x^j$ is a generator polynomial for the cyclic code C then the generator matrix is given by

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & 0 & \dots & & & & \dots & 0 \\ 0 & 0 & \dots & & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

Cyclic codes

Observation

$\rightarrow$ The matrix G has n columns and $k = n - r$ rows, so the first row, $\mathbf{g}_0$, finishes with a string of 0's of length $k - 1$

Cyclic codes

Observation

- $\rightarrow$ The matrix G has n columns and $k = n - r$ rows, so the first row, $\mathbf{g}_0$, finishes with a string of 0's of length $k - 1$
- $\rightarrow$ Each successive row is the cyclic shift of the previous row: $\mathbf{g}_i = \widetilde{\mathbf{g}}_{i-1}$, for $i = 1, \ldots, k - 1$

Cyclic codes

Observation

- $\rightarrow$ The matrix G has n columns and $k = n - r$ rows, so the first row, $\mathbf{g}_0$, finishes with a string of 0's of length $k - 1$
- $\rightarrow$ Each successive row is the cyclic shift of the previous row: $\mathbf{g}_i = \widetilde{\mathbf{g}}_{i-1}$, for $i = 1, \ldots, k - 1$
- $\rightarrow$ As $g(x)h(x) = x^n - 1$, we have $g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0$. In particular $g_0 \neq 0$ and $h_0 \neq 0$

Cyclic codes

Observation

- $\rightarrow$ The matrix G has n columns and $k = n - r$ rows, so the first row, $\mathbf{g}_0$, finishes with a string of 0's of length $k - 1$
- $\rightarrow$ Each successive row is the cyclic shift of the previous row: $\mathbf{g}_i = \widetilde{\mathbf{g}}_{i-1}$, for $i = 1, \ldots, k - 1$
- $\rightarrow$ As $g(x)h(x) = x^n - 1$, we have $g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0$. In particular $g_0 \neq 0$ and $h_0 \neq 0$
- $\rightarrow$ Therefore G is in echelon form (although likely not reduced). In particular the $k = dim(C)$ rows of G are linearly independent

Cyclic codes

Observation

- $\rightarrow$ The matrix G has n columns and $k = n - r$ rows, so the first row, $\mathbf{g}_0$, finishes with a string of 0's of length $k - 1$
- $\rightarrow$ Each successive row is the cyclic shift of the previous row: $\mathbf{g}_i = \widetilde{\mathbf{g}}_{i-1}$, for $i = 1, \ldots, k - 1$
- $\rightarrow$ As $g(x)h(x) = x^n - 1$, we have $g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0$. In particular $g_0 \neq 0$ and $h_0 \neq 0$
- $\rightarrow$ Therefore G is in echelon form (although likely not reduced). In particular the $k = dim(C)$ rows of G are linearly independent

G is also called the cyclic generator matrix of C

Cyclic codes

Example For the $[7, 4]$ binary cyclic code with generator polynomial $1 + x + x^3$, the generator matrix is

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

Cyclic codes

Example For the $[7, 4]$ binary cyclic code with generator polynomial $1 + x + x^3$, the generator matrix is

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

For encoding the information or message k-tuple $\mathbf{m} = (m_0, \ldots, m_{k-1})$, the encoded message is given by $\mathbf{c} = \mathbf{m}G$. In terms of polynomials, $m(x) = \sum_{i=0}^{k-1} m_i x^i$ and $\mathbf{c}(x) = \mathbf{m}(x)g(x)$.

Cyclic codes

Example For the $[7, 4]$ binary cyclic code with generator polynomial $1 + x + x^3$, the generator matrix is

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

For encoding the information or message k-tuple $\mathbf{m} = (m_0, \ldots, m_{k-1})$, the encoded message is given by $\mathbf{c} = \mathbf{m}G$. In terms of polynomials, $m(x) = \sum_{i=0}^{k-1} m_i x^i$ and $\mathbf{c}(x) = \mathbf{m}(x)g(x)$.
Observation Since the cyclic generator G is in echelon form, although G is not in standard/systematic form

Cyclic codes

Standard generator matrix We aim to have the encoding method such that

$$\mathbf{m} = (m_0, \ldots, m_{k-1}) \mapsto \mathbf{c} = (m_0, \ldots, m_{k-1}, -s_0, -s_1, \ldots, -s_{r-1})$$

where $s(x) = \sum_{j=0}^{r-1} s_j x^j$ is the remainder upon dividing $x^r m(x)$ by $g(x)$ i.e.

$$x^r m(x) = q(x)g(x) + s(x)$$

with $deg(s(x)) < deg(g(x)) = r$.

Cyclic codes

Standard generator matrix We aim to have the encoding method such that

$$\mathbf{m} = (m_0, \ldots, m_{k-1}) \mapsto \mathbf{c} = (m_0, \ldots, m_{k-1}, -s_0, -s_1, \ldots, -s_{r-1})$$

where $s(x) = \sum_{j=0}^{r-1} s_j x^j$ is the remainder upon dividing $x^r m(x)$ by $g(x)$ i.e.

$$x^r m(x) = q(x)g(x) + s(x)$$

with $deg(s(x)) < deg(g(x)) = r$.
To see that this is the correct standard encoding, first note that

$$x^r m(x) - s(x) = q(x)g(x) = b(x) \in C$$

with the corresponding codeword

$$\mathbf{b} = (-s_0, -s_1, \ldots, -s_{r-1}, m_0, \ldots, m_{k-1}).$$

Cyclic codes

Standard generator matrix We aim to have the encoding method such that

$$\mathbf{m} = (m_0, \ldots, m_{k-1}) \mapsto \mathbf{c} = (m_0, \ldots, m_{k-1}, -s_0, -s_1, \ldots, -s_{r-1})$$

where $s(x) = \sum_{j=0}^{r-1} s_j x^j$ is the remainder upon dividing $x^r m(x)$ by $g(x)$ i.e.

$$x^r m(x) = q(x)g(x) + s(x)$$

with $deg(s(x)) < deg(g(x)) = r$.
To see that this is the correct standard encoding, first note that

$$x^r m(x) - s(x) = q(x)g(x) = b(x) \in C$$

with the corresponding codeword

$$\mathbf{b} = (-s_0, -s_1, \ldots, -s_{r-1}, m_0, \ldots, m_{k-1}).$$

Since this is a codeword of cyclic C, every cyclic shift of it is also a codeword

Cyclic codes

In particular the c given above is found after k right shifts.

Thus c is a codeword of C.

Cyclic codes

In particular the c given above is found after k right shifts.

Thus c is a codeword of C.

Since C is systematic on the first k positions, this codeword is the only one with m on those positions and so is the result of standard encoding.

Cyclic codes

In particular the c given above is found after k right shifts.

Thus c is a codeword of C.

Since C is systematic on the first k positions, this codeword is the only one with m on those positions and so is the result of standard encoding.

To construct the standard generator matrix itself, we encode the k different k-tuple messages $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ of weight 1 corresponding to message polynomials x^i, for $0 \leq i \leq k-1$. These are the rows of the standard generator matrix.

Cyclic codes

Example Consider the $[7,4]$ binary cyclic code with generator x^3+x+1 (so $r=t-4=3$,) we find that, for instance,

$$x^3x^2 = (x^2+1)(x^3+x+1) + (x^2+x+1)$$

so that the third row of the standard generator matrix, corresponding to message polynomial x^2, is

$$(m_0, m_1, m_2, m_3, -s_0, -s_1, -s_2) = (0,0,1,0,1,1,1).$$

Cyclic codes

Example Consider the $[7, 4]$ binary cyclic code with generator $x^3 + x + 1$ (so $r = t - 4 = 3$,) we find that, for instance,

$$x^3 x^2 = (x^2 + 1)(x^3 + x + 1) + (x^2 + x + 1)$$

so that the third row of the standard generator matrix, corresponding to message polynomial x^2, is

$$(m_0, m_1, m_2, m_3, -s_0, -s_1, -s_2) = (0, 0, 1, 0, 1, 1, 1).$$

Proceeding in this way, we find that the standard generator matrix is

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