Information and Coding Theory MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 18 March 27, 2023

3

<日

<</p>

Question Does the reverse shifting give a cyclic code?

э

イロト イボト イヨト イヨト

Question Does the reverse shifting give a cyclic code?

The reverse code $C^{[-1]}$ of a cyclic code C, reversing each codeword, is still cyclic:

 $(c_0,\ldots,c_i,\ldots,c_{n-1})\in C\longleftrightarrow (c_{n-1},\ldots,c_{n-1-i},\ldots,c_1,c_0)\in C^{[-1]}$

イロト イポト イヨト イヨト 二日

Question Does the reverse shifting give a cyclic code?

The reverse code $C^{[-1]}$ of a cyclic code C, reversing each codeword, is still cyclic:

$$(c_0,\ldots,c_i,\ldots,c_{n-1})\in C\longleftrightarrow (c_{n-1},\ldots,c_{n-1-i},\ldots,c_1,c_0)\in C^{[-1]}$$

In polynomial notation, this becomes

$$c(x) \in C \longleftrightarrow x^{n-1}c(x^{-1}) \in C^{[-1]}$$

2/8

Question Does the reverse shifting give a cyclic code?

The reverse code $C^{[-1]}$ of a cyclic code C, reversing each codeword, is still cyclic:

$$(c_0,\ldots,c_i,\ldots,c_{n-1})\in C\longleftrightarrow (c_{n-1},\ldots,c_{n-1-i},\ldots,c_1,c_0)\in C^{[-1]}$$

In polynomial notation, this becomes

$$c(x) \in C \longleftrightarrow x^{n-1}c(x^{-1}) \in C^{[-1]}$$

Reciprocal polynomial For a polynomial p(x) of degree d, the reciprocal of p(x) is given by

$$p^{[-1]}(x) = \sum_{i=0}^{d} p_{d-i} x^{i} = x^{d} p(x^{-1})$$

3

Proposition If g(x) generates a cyclic code C then $g_0^{-1}g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of G

3

글 제 제 글 제

Proposition If g(x) generates a cyclic code C then $g_0^{-1}g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of G

Observation

→ Let C be a cyclic code of length n with generator polynomial g(x) of degree r and check polynomial h(x) of degree k = n - r = dim(C).

医医尿管下 医

Proposition If g(x) generates a cyclic code C then $g_0^{-1}g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of G

Observation

- → Let C be a cyclic code of length n with generator polynomial g(x) of degree r and check polynomial h(x) of degree k = n r = dim(C).
- → Since h(x) is a divisor of $x^n 1$, it is a generator polynomial for a cyclic code *D* of length *n* and dimension n k = n (n r) = r

3/8

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Proposition If g(x) generates a cyclic code C then $g_0^{-1}g^{[-1]}(x)$ generates $C^{[-1]}$, the reverse code of G

Observation

- → Let C be a cyclic code of length n with generator polynomial g(x) of degree r and check polynomial h(x) of degree k = n r = dim(C).
- → Since h(x) is a divisor of $x^n 1$, it is a generator polynomial for a cyclic code *D* of length *n* and dimension n k = n (n r) = r

 $\rightarrow\,$ We have

$$C = \{q(x)g(x)|q(x) \in F[x]_k\}, \ D = \{p(x)h(x)|p(x) \in F[x]_r\}$$

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Let $c(x) = q(x)g(x) \in C$ so that $deg(q(x)) \leq k - 1$, and let $d(x) = p(x)h(x) \in D$, so that $deg(p(x)) \leq r - 1$.

イロト 不得 トイヨト イヨト 二日

Let $c(x) = q(x)g(x) \in C$ so that $deg(q(x)) \leq k - 1$, and let $d(x) = p(x)h(x) \in D$, so that $deg(p(x)) \leq r - 1$. Then

$$c(x)d(x) = q(x)g(x)p(x)h(x) = q(x)p(x)(x^{n}-1) = s(x)(x^{n}-1)$$

= $s(x)x^{n} - s(x)$,

where s(x) = q(x)p(x) with

$$deg(s(x)) \le (k-1) + (r-1) = r + k - 2 = n - 2 < n - 1.$$

イロト イポト イヨト イヨト 二日

Let $c(x) = q(x)g(x) \in C$ so that $deg(q(x)) \leq k - 1$, and let $d(x) = p(x)h(x) \in D$, so that $deg(p(x)) \leq r - 1$. Then

$$c(x)d(x) = q(x)g(x)p(x)h(x) = q(x)p(x)(x^{n}-1) = s(x)(x^{n}-1)$$

= $s(x)x^{n} - s(x)$,

where s(x) = q(x)p(x) with

$$deg(s(x)) \le (k-1) + (r-1) = r + k - 2 = n - 2 < n - 1.$$

Therefore, the coefficient of x^{n-1} in c(x)d(x) is 0.

イロト イポト イヨト イヨト 二日

Cyclic codes If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ and $d(x) = \sum_{j=0}^{n-1} d_j x^j$ then in general the coefficient of x^m in c(x)d(x) is $\sum_{i+j=m} c_i d_j$

3

・ 同 ト ・ ヨ ト ・ ヨ ト

If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ and $d(x) = \sum_{j=0}^{n-1} d_j x^j$ then in general the coefficient of x^m in c(x)d(x) is $\sum_{i+j=m} c_i d_j$

In particular, the coefficients corresponding to x^{n-1} in c(x)d(x) gives us

$$0 = \sum_{i+j=n-1}^{n} c_i d_j = \sum_{i=0}^{n} c_i d_{n-1-i}$$

= $c_0 d_{n-1} + c_1 d_{n-2} + \dots + c_i d_{n-i} + \dots + c_{n-1} d_0$
= $\mathbf{c} \cdot \mathbf{d}^*$

where

$$\mathbf{c} = (c_0, c_1, \dots, c_i, \dots, c_{n-1}), \ \mathbf{d}^* = (d_{n-1}, d_{n-2}, \dots, d_{n-i}, \dots, d_0)$$

If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ and $d(x) = \sum_{j=0}^{n-1} d_j x^j$ then in general the coefficient of x^m in c(x)d(x) is $\sum_{i+j=m} c_i d_j$

In particular, the coefficients corresponding to x^{n-1} in c(x)d(x) gives us

$$0 = \sum_{i+j=n-1}^{n} c_i d_j = \sum_{i=0}^{n} c_i d_{n-1-i}$$

= $c_0 d_{n-1} + c_1 d_{n-2} + \dots + c_i d_{n-i} + \dots + c_{n-1} d_0$
= $\mathbf{c} \cdot \mathbf{d}^*$

where

$$\mathbf{c} = (c_0, c_1, \dots, c_i, \dots, c_{n-1}), \ \mathbf{d}^* = (d_{n-1}, d_{n-2}, \dots, d_{n-i}, \dots, d_0)$$

Thus each codeword **c** in *C* has dot product 0 with the reverse of each codeword **d** of *D*, which further implies $C^{\perp} \subseteq D^{[-1]}$.

If $c(x) = \sum_{i=0}^{n-1} c_i x^i$ and $d(x) = \sum_{j=0}^{n-1} d_j x^j$ then in general the coefficient of x^m in c(x)d(x) is $\sum_{i+j=m} c_i d_j$

In particular, the coefficients corresponding to x^{n-1} in c(x)d(x) gives us

$$0 = \sum_{i+j=n-1}^{n} c_i d_j = \sum_{i=0}^{n} c_i d_{n-1-i}$$

= $c_0 d_{n-1} + c_1 d_{n-2} + \dots + c_i d_{n-i} + \dots + c_{n-1} d_0$
= $\mathbf{c} \cdot \mathbf{d}^*$

where

$$\mathbf{c} = (c_0, c_1, \dots, c_i, \dots, c_{n-1}), \ \mathbf{d}^* = (d_{n-1}, d_{n-2}, \dots, d_{n-i}, \dots, d_0)$$

Thus each codeword **c** in *C* has dot product 0 with the reverse of each codeword **d** of *D*, which further implies $C^{\perp} \subseteq D^{[-1]}$. Also

$$dim(C^{\perp}) = n - dim(C) = n - k = r = n - deg(h^{[-1]}(x)) = dim(D^{[-1]})$$

5/8

Conclusion If C is the cyclic code of length n with check polynomial h(x), then C^{\perp} is cyclic with generator polynomial $h_0^{-1}h^{[-1]}(x)$

イロト 不得 トイラト イラト 一日

Conclusion If C is the cyclic code of length n with check polynomial h(x), then C^{\perp} is cyclic with generator polynomial $h_0^{-1}h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let C be a cyclic code. Then there is a unique codeword c(x) which is an identity element for C

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Conclusion If C is the cyclic code of length n with check polynomial h(x), then C^{\perp} is cyclic with generator polynomial $h_0^{-1}h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let C be a cyclic code. Then there is a unique codeword c(x) which is an identity element for CProof

Let g(x) be the generator polynomial of C, and h(x) the check polynomial i.e. $g(x)h(x) = x^n - 1$

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

6/8

Conclusion If C is the cyclic code of length n with check polynomial h(x), then C^{\perp} is cyclic with generator polynomial $h_0^{-1}h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let C be a cyclic code. Then there is a unique codeword c(x) which is an identity element for CProof

Let g(x) be the generator polynomial of C, and h(x) the check polynomial i.e. $g(x)h(x) = x^n - 1$

Since $x^n - 1$ has no multiple zeros, we have gcd(g(x), h(x)) = 1 and hence there exist polynomials a(x) and b(x) such that

$$a(x)g(x)+b(x)h(x)=1$$

イロト 不得 トイヨト イヨト 二日

Conclusion If C is the cyclic code of length n with check polynomial h(x), then C^{\perp} is cyclic with generator polynomial $h_0^{-1}h^{[-1]}(x)$

Idempotent of a cyclic code Theorem Let C be a cyclic code. Then there is a unique codeword c(x) which is an identity element for CProof

Let g(x) be the generator polynomial of C, and h(x) the check polynomial i.e. $g(x)h(x) = x^n - 1$

Since $x^n - 1$ has no multiple zeros, we have gcd(g(x), h(x)) = 1 and hence there exist polynomials a(x) and b(x) such that

$$a(x)g(x) + b(x)h(x) = 1$$

Define c(x) = a(x)g(x) = 1 - b(x)h(x), which is a codeword in C

イロト 不得 トイヨト イヨト 二日

If p(x)g(x) is any codeword in C then

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

= $p(x)g(x) \mod (x^n - 1)$

э

(日) (四) (日) (日) (日)

If p(x)g(x) is any codeword in C then

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

= $p(x)g(x) \mod (x^n - 1)$

So c(x) is an identity element for C, and hence it is unique

3

If p(x)g(x) is any codeword in C then

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

= $p(x)g(x) \mod (x^n - 1)$

So c(x) is an identity element for *C*, and hence it is unique Since $c^2(x) = c(x)$, this codeword is called the idempotent. Since every codeword v(x) can be written as v(x)c(x), i.e. as a multiple of c(x), we see that c(x) generates the ideal *C*

Maximal and minimal cyclic code Let $x^n - 1 = f_1(x)f_2(x) \dots f_t(x)$ be the decomposition of $x^n - 1$ into irreducible factors.

The cyclic code generated by $f_i(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by M_i^+

Maximal and minimal cyclic code Let $x^n - 1 = f_1(x)f_2(x) \dots f_t(x)$ be the decomposition of $x^n - 1$ into irreducible factors.

The cyclic code generated by $f_i(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by M_i^+

The code generated by $(x^n - 1)/f_i(x)$ is called the minimal cyclic code, denoted by M_i^-

< 回 > < 回 > < 回 >

Maximal and minimal cyclic code Let $x^n - 1 = f_1(x)f_2(x) \dots f_t(x)$ be the decomposition of $x^n - 1$ into irreducible factors.

The cyclic code generated by $f_i(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by M_i^+

The code generated by $(x^n - 1)/f_i(x)$ is called the minimal cyclic code, denoted by M_i^-

Observation(Homework)

- → Let $g(x) = (x^n 1)/f_i(x)$, where $deg(f_i(x)) = k$ be a generator of the minimal code M_i^-
- \rightarrow If a(x) and b(x) are two codewords in M_i^- such that a(x)b(x) = 0, then one of them must be divisible by $f_i(x)$ and it is therefore 0

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Maximal and minimal cyclic code Let $x^n - 1 = f_1(x)f_2(x) \dots f_t(x)$ be the decomposition of $x^n - 1$ into irreducible factors.

The cyclic code generated by $f_i(x)$ is called a maximal cyclic code (since it is a maximal ideal), and denoted by M_i^+

The code generated by $(x^n - 1)/f_i(x)$ is called the minimal cyclic code, denoted by M_i^-

Observation(Homework)

- → Let $g(x) = (x^n 1)/f_i(x)$, where $deg(f_i(x)) = k$ be a generator of the minimal code M_i^-
- \rightarrow If a(x) and b(x) are two codewords in M_i^- such that a(x)b(x) = 0, then one of them must be divisible by $f_i(x)$ and it is therefore 0
- \rightarrow Since M_i^- has no zero divisors, it is a field

A B A B A B A B A B A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A
 B
 A