Error-Correcting Codes over Rings

Lecture 2: Cyclic Codes

W. Cary Huffman

Department of Mathematics and Statistics
Loyola University Chicago
whuffma@luc.edu

Noncommutative Rings and Their Applications
Université d'Atois
Lens, France
June 25, 2019

Cyclic Codes - the Beginning

People

Eugene Prange (Air Force Cambridge Research Laboratory, Bedford, Massachusetts) and W. Wesley Peterson (IBM, MIT, U. of Florida, U. of Hawaii).

Cyclic Codes - the Beginning

People

Eugene Prange (Air Force Cambridge Research Laboratory, Bedford, Massachusetts) and W. Wesley Peterson (IBM, MIT, U. of Florida, U. of Hawaii).

References

- E. Prange, Technical Notes AFCRL
  - "Cyclic error-correcting codes in two symbols", TN-57-103 (September, 1957)
  - "Some cyclic error-correcting codes with simple decoding algorithms", TN-58-156 (April, 1958)
  - "The use of coset equivalence in the analysis and decoding of group codes," TN-59-164 (1959)
  - "An algorithm for factoring $x^n - 1$ over a finite field", TN-59-175 (October, 1959)

Cyclic Codes - the Beginning

People

Eugene Prange (Air Force Cambridge Research Laboratory, Bedford, Massachusetts) and W. Wesley Peterson (IBM, MIT, U. of Florida, U. of Hawaii).

References

- E. Prange, Technical Notes AFCRL
  - "Cyclic error-correcting codes in two symbols", TN-57-103 (September, 1957)
  - "Some cyclic error-correcting codes with simple decoding algorithms", TN-58-156 (April, 1958)
  - "The use of coset equivalence in the analysis and decoding of group codes," TN-59-164 (1959)
  - "An algorithm for factoring $x^n - 1$ over a finite field", TN-59-175 (October, 1959)
- W. W. Peterson, *Error-Correcting Codes*, MIT Press, Cambridge, MA, 1961.

Definition of a Cyclic Code

Notation

Subscript change: $\mathbf{v} = v_0 v_1 \cdots v_{n-1} \in \mathbb{A}^n$.

Definition of a Cyclic Code

Notation

Subscript change: $\mathbf{v} = v_0 v_1 \cdots v_{n-1} \in \mathbb{A}^n$.

Definition

Let $\mathcal{C} \subseteq \mathbb{A}^n$. $\mathcal{C}$ is cyclic provided for all $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in \mathcal{C}$, the cyclic shift $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2} \in \mathcal{C}$.

Definition of a Cyclic Code

Notation

Subscript change: $\mathbf{v} = v_0 v_1 \cdots v_{n-1} \in \mathbb{A}^n$.

Definition

Let $\mathcal{C} \subseteq \mathbb{A}^n$. $\mathcal{C}$ is cyclic provided for all $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in \mathcal{C}$, the cyclic shift $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2} \in \mathcal{C}$.

Remark

A cyclic code is closed under cyclic shifts, with wrap-around, of any amount in either direction.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

- $\mathfrak{R}[x]$ is the ring of polynomials in x with coefficients in $\mathfrak{R}$.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

- $\mathfrak{R}[x]$ is the ring of polynomials in x with coefficients in $\mathfrak{R}$.
- Let $\langle x^n - 1 \rangle$ denote the two-sided principal ideal of $\mathfrak{R}[x]$ generated by $x^n - 1$. Let $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1 \rangle$.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

- $\mathfrak{R}[x]$ is the ring of polynomials in x with coefficients in $\mathfrak{R}$.
- Let $\langle x^n - 1 \rangle$ denote the two-sided principal ideal of $\mathfrak{R}[x]$ generated by $x^n - 1$. Let $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1 \rangle$.
- Define $\iota : \mathfrak{R}^n \to \mathcal{P}_{\mathfrak{R},n}$ as follows: If $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in \mathfrak{R}^n$, let $\iota(\mathbf{c}) = \mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + \langle x^n - 1 \rangle$.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

- $\mathfrak{R}[x]$ is the ring of polynomials in x with coefficients in $\mathfrak{R}$.
- Let $\langle x^n - 1 \rangle$ denote the two-sided principal ideal of $\mathfrak{R}[x]$ generated by $x^n - 1$. Let $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1 \rangle$.
- Define $\iota : \mathfrak{R}^n \to \mathcal{P}_{\mathfrak{R},n}$ as follows: If $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in \mathfrak{R}^n$, let $\iota(\mathbf{c}) = \mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + \langle x^n - 1 \rangle$.

Remarks

- Both $\mathfrak{R}^n$ and $\mathcal{P}_{\mathfrak{R},n}$ are left (or right) $\mathfrak{R}$-modules under addition and left (or right) scalar multiplication by elements of $\mathfrak{R}$. The map ι is an $\mathfrak{R}$-module isomorphism of $\mathfrak{R}^n$ onto $\mathcal{P}_{\mathfrak{R},n}$.

Polynomial Setting

Notation

Let $\mathfrak{R}$ be a finite ring with unity. Let x be an indeterminate over $\mathfrak{R}$ and n a positive integer.

- $\mathfrak{R}[x]$ is the ring of polynomials in x with coefficients in $\mathfrak{R}$.
- Let $\langle x^n - 1 \rangle$ denote the two-sided principal ideal of $\mathfrak{R}[x]$ generated by $x^n - 1$. Let $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1 \rangle$.
- Define $\iota : \mathfrak{R}^n \to \mathcal{P}_{\mathfrak{R},n}$ as follows: If $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in \mathfrak{R}^n$, let $\iota(\mathbf{c}) = \mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + \langle x^n - 1 \rangle$.

Remarks

- Both $\mathfrak{R}^n$ and $\mathcal{P}_{\mathfrak{R},n}$ are left (or right) $\mathfrak{R}$-modules under addition and left (or right) scalar multiplication by elements of $\mathfrak{R}$. The map ι is an $\mathfrak{R}$-module isomorphism of $\mathfrak{R}^n$ onto $\mathcal{P}_{\mathfrak{R},n}$.
- Images under ι of left-linear (or right-linear) codes in $\mathfrak{R}^n$ are left (or right) $\mathfrak{R}$-submodules of $\mathcal{P}_{\mathfrak{R},n}$.

Polynomial Setting (cont.)

Remarks

- For $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$, let $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2}$. Then in $\mathcal{P}_{\mathfrak{R},n}$, $\iota(\mathbf{c}') = x\iota(\mathbf{c}) = \iota(\mathbf{c})x$.

Polynomial Setting (cont.)

Remarks

- For $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$, let $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2}$. Then in $\mathcal{P}_{\mathfrak{R},n}$, $\iota(\mathbf{c}') = x\iota(\mathbf{c}) = \iota(\mathbf{c})x$.
- So images under ι of left-linear (or right-linear) cyclic codes in $\mathfrak{R}^n$ are left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$.

Polynomial Setting (cont.)

Remarks

- For $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$, let $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2}$. Then in $\mathcal{P}_{\mathfrak{R},n}$, $\iota(\mathbf{c}') = x\iota(\mathbf{c}) = \iota(\mathbf{c})x$.
- So images under ι of left-linear (or right-linear) cyclic codes in $\mathfrak{R}^n$ are left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$.
- We will view left-linear (or right-linear) cyclic codes in either the $\mathfrak{R}^n$ setting or as left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$, whichever is convenient.

Polynomial Setting (cont.)

Remarks

- For $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$, let $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2}$. Then in $\mathcal{P}_{\mathfrak{R},n}$, $\iota(\mathbf{c}') = x\iota(\mathbf{c}) = \iota(\mathbf{c})x$.
- So images under ι of left-linear (or right-linear) cyclic codes in $\mathfrak{R}^n$ are left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$.
- We will view left-linear (or right-linear) cyclic codes in either the $\mathfrak{R}^n$ setting or as left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$, whichever is convenient.
- Polynomials $c(x) = c_0 + c_1 x + \cdots \in \mathfrak{R}[x]$ will be written without bold face font; $\mathbf{c}(x) = c(x) + \langle x^n - 1 \rangle \in \mathcal{P}_{\mathfrak{R},n}$. We will say $c(x)$ and $\mathbf{c}(x)$ correspond.

Polynomial Setting (cont.)

Remarks

- For $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$, let $\mathbf{c}' = c_{n-1} c_0 \cdots c_{n-2}$. Then in $\mathcal{P}_{\mathfrak{R},n}$, $\iota(\mathbf{c}') = x\iota(\mathbf{c}) = \iota(\mathbf{c})x$.
- So images under ι of left-linear (or right-linear) cyclic codes in $\mathfrak{R}^n$ are left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$.
- We will view left-linear (or right-linear) cyclic codes in either the $\mathfrak{R}^n$ setting or as left (or right) ideals of $\mathcal{P}_{\mathfrak{R},n}$, whichever is convenient.
- Polynomials $c(x) = c_0 + c_1 x + \cdots \in \mathfrak{R}[x]$ will be written without bold face font; $\mathbf{c}(x) = c(x) + \langle x^n - 1 \rangle \in \mathcal{P}_{\mathfrak{R},n}$. We will say $c(x)$ and $\mathbf{c}(x)$ correspond.
- Simplification: We write cosets $\mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ of $\mathcal{P}_{\mathfrak{R},n}$ without $\langle x^n - 1 \rangle$; so $\mathbf{a}(x)\mathbf{b}(x) = \mathbf{c}(x) \in \mathcal{P}_{\mathfrak{R},n}$ will be written as a polynomial of degree at most $n-1$ with the understanding that we really mean $(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle)(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + \langle x^n - 1 \rangle) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle x^n - 1 \rangle$.

Linear Cyclic Codes over $\mathbb{F}_q$

Theorem

$\mathbb{F}_q[x]$ is a unique factorization domain (and therefore a principal ideal domain) and $\mathcal{P}_{\mathbb{F}_q,n}$ is a principal ideal ring. Furthermore, the following are equivalent.

(a) $gcd(n, q) = 1$.

(b) $\mathcal{P}_{\mathbb{F}_q,n}$ *is semi-simple.*

(c) $x^n - 1$ *has distinct roots in an extension field of* $\mathbb{F}_q$.

Linear Cyclic Codes over $\mathbb{F}_q$

Theorem

$\mathbb{F}_q[x]$ is a unique factorization domain (and therefore a principal ideal domain) and $\mathcal{P}_{\mathbb{F}_q,n}$ is a principal ideal ring. Furthermore, the following are equivalent.

(a) $gcd(n, q) = 1$.

(b) $\mathcal{P}_{\mathbb{F}_q,n}$ *is semi-simple.*

(c) $x^n - 1$ *has distinct roots in an extension field of* $\mathbb{F}_q$.

Notation

The principal ideal generated by $a(x)$ (or $\mathbf{a}(x)$) in $\mathbb{F}_q[x]$ (or $\mathcal{P}_{\mathbb{F}_q,n}$) will be denoted $\langle a(x)\rangle$ (or $\langle \mathbf{a}(x)\rangle$).

Linear Cyclic Codes over $\mathbb{F}_q$ (cont.)

Theorem

Let $\mathcal{C} \subseteq \mathcal{P}_{\mathbb{F}_q,n}$ be a nonzero linear cyclic code of dimension k. There exists a polynomial $\mathbf{g}(x) \in \mathcal{C}$, corresponding to $g(x) \in \mathbb{F}_q[x]$, with the following properties.

(a) $\mathbf{g}(x)$ *is the unique monic polynomial of minimum degree in $\mathcal{C}$.*

(b) $\mathcal{C} = \langle \mathbf{g}(x) \rangle$.

(c) $g(x) \mid (x^n - 1)$ *in* $\mathbb{F}_q[x]$ *and* $\deg g(x) = n - k$.

(d) $\{\mathbf{g}(x), x\mathbf{g}(x), \ldots, x^{k-1}\mathbf{g}(x)\}$ *is a basis of $\mathcal{C}$.*

(e) *Every element of $\mathcal{C}$ is expressed uniquely as a product* $\mathbf{f}(x)\mathbf{g}(x)$ *where* $f(x) = 0$ *or* $\deg f(x) < k$.

Linear Cyclic Codes over $\mathbb{F}_q$ (cont.)

(f) *A generator matrix G of $\mathcal{C}$ is*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & 0 & 0 & g_0 & \cdots & \cdots & \cdots & g_{n-k} \end{bmatrix}$$

$$\leftrightarrow \begin{bmatrix} \mathbf{g}(x) & & & \\ & x\mathbf{g}(x) & & \\ & & \ddots & \\ & & & x^{k-1}\mathbf{g}(x) \end{bmatrix}$$

where $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$.

Linear Cyclic Codes over $\mathbb{F}_q$ (cont.)

(f) *A generator matrix G of $\mathcal{C}$ is*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & 0 & 0 & g_0 & \cdots & \cdots & \cdots & g_{n-k} \end{bmatrix}$$

$$\leftrightarrow \begin{bmatrix} \mathbf{g}(x) & & & \\ & x\mathbf{g}(x) & & \\ & & \ddots & \\ & & & x^{k-1}\mathbf{g}(x) \end{bmatrix}$$

where $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$.

Remark

$g(x)$ is the generator polynomial of $\mathcal{C}$. The zero cyclic code has generator polynomial $g(x) = x^n - 1$.

Linear Cyclic Codes over $\mathbb{F}_q$ (cont.)

Two Cases

- $\gcd(n, q) = 1$
- $\gcd(n, q) \neq 1$

Linear Cyclic Codes over $\mathbb{F}_q$ (cont.)

Two Cases

- $\gcd(n, q) = 1$
- $\gcd(n, q) \neq 1$

Remark

In both cases, the factorization of $x^n - 1$ over $\mathbb{F}_q$ is key.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$

Notation and Terminology

- Let $t = \mathrm{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$

Notation and Terminology

- Let $t = \mathrm{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.
- $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$

Notation and Terminology

- Let $t = \text{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.
- $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$.
- If γ is a primitive element of $\mathbb{F}_{q^t}$, then $\alpha = \gamma^{(q^t-1)/n}$ is a primitive n^{th} root of unity; i.e. $\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are the n distinct roots of $x^n - 1$ in $\mathbb{F}_{q^t}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$

Notation and Terminology

- Let $t = \mathrm{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.
- $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$.
- If γ is a primitive element of $\mathbb{F}_{q^t}$, then $\alpha = \gamma^{(q^t-1)/n}$ is a primitive n^{th} root of unity; i.e. $\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are the n distinct roots of $x^n - 1$ in $\mathbb{F}_{q^t}$.
- For $s \in \mathbb{Z}$ with $0 \leq s < n$, the q-cyclotomic coset of s modulo n is

$$C_{s,q,n} = \{s, sq, \ldots, sq^{r-1}\} \pmod{n}$$

  where r is the smallest positive integer such that $sq^r \equiv s \pmod{n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n,q)=1$

Notation and Terminology

- Let $t = \mathrm{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.
- $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$.
- If γ is a primitive element of $\mathbb{F}_{q^t}$, then $\alpha = \gamma^{(q^t-1)/n}$ is a primitive n^{th} root of unity; i.e. $\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are the n distinct roots of $x^n - 1$ in $\mathbb{F}_{q^t}$.
- For $s \in \mathbb{Z}$ with $0 \le s < n$, the q-cyclotomic coset of s modulo n is
$$C_{s,q,n} = \{s, sq, \ldots, sq^{r-1}\} \pmod{n}$$
where r is the smallest positive integer such that $sq^r \equiv s \pmod{n}$. Note: $r \mid t$ and $t = |C_{1,q,n}|$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$

Notation and Terminology

- Let $t = \mathrm{ord}_n(q)$ be the smallest positive integer where $n \mid (q^t - 1)$; t is the order of q modulo n.
- $\mathbb{F}_{q^t}$ is the splitting field of $x^n - 1$ over $\mathbb{F}_q$.
- If γ is a primitive element of $\mathbb{F}_{q^t}$, then $\alpha = \gamma^{(q^t-1)/n}$ is a primitive n^{th} root of unity; i.e. $\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are the n distinct roots of $x^n - 1$ in $\mathbb{F}_{q^t}$.
- For $s \in \mathbb{Z}$ with $0 \leq s < n$, the q-cyclotomic coset of s modulo n is

$$C_{s,q,n} = \{s, sq, \ldots, sq^{r-1}\} \pmod{n}$$

  where r is the smallest positive integer such that $sq^r \equiv s \pmod{n}$. Note: $r \mid t$ and $t = |C_{1,q,n}|$.
- Define $M_{\alpha^s}(x) = \prod_{i \in C_{s,q,n}} (x - \alpha^i)$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

The following hold.

(a) *The distinct q-cyclotomic cosets modulo n partition* $\{0, 1, \ldots, n-1\}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

The following hold.

(a) *The distinct q-cyclotomic cosets modulo n partition* $\{0, 1, \ldots, n-1\}$.

(b) $M_{\alpha^s}(x)$ *is irreducible over* $\mathbb{F}_q$, *and* $x^n - 1 = \prod_s M_{\alpha^s}(x)$ *where s runs through a set of representatives of* **all** *distinct q-cyclotomic cosets modulo n.*

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

The following hold.

(a) *The distinct q-cyclotomic cosets modulo n partition* $\{0, 1, \ldots, n-1\}$.

(b) $M_{\alpha^s}(x)$ *is irreducible over* $\mathbb{F}_q$, *and* $x^n - 1 = \prod_s M_{\alpha^s}(x)$ *where s runs through a set of representatives of* **all** *distinct q-cyclotomic cosets modulo n.*

(c) *If* $g(x)$ *is the generator polynomial of a linear cyclic code of length n, then* $g(x) = \prod_{s \in S} M_{\alpha^s}(x)$ *where s runs through* **some** *subset S of representatives of distinct q-cyclotomic cosets modulo n.*

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

The following hold.

(a) *The distinct q-cyclotomic cosets modulo n partition* $\{0, 1, \ldots, n-1\}$.

(b) $M_{\alpha^s}(x)$ *is irreducible over* $\mathbb{F}_q$*, and* $x^n - 1 = \prod_s M_{\alpha^s}(x)$ *where s runs through a set of representatives of* **all** *distinct q-cyclotomic cosets modulo n.*

(c) *If* $g(x)$ *is the generator polynomial of a linear cyclic code of length n, then* $g(x) = \prod_{s \in S} M_{\alpha^s}(x)$ *where s runs through* **some** *subset S of representatives of distinct q-cyclotomic cosets modulo n.*

(d) *There are* 2^m *linear cyclic codes of length n where m is the number of distinct q-cyclotomic cosets modulo n.*

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

The following hold.

(a) *The distinct q-cyclotomic cosets modulo n partition* $\{0, 1, \ldots, n-1\}$.

(b) $M_{\alpha^s}(x)$ *is irreducible over* $\mathbb{F}_q$, *and* $x^n - 1 = \prod_s M_{\alpha^s}(x)$ *where s runs through a set of representatives of* **all** *distinct q-cyclotomic cosets modulo n.*

(c) *If* $g(x)$ *is the generator polynomial of a linear cyclic code of length n, then* $g(x) = \prod_{s \in S} M_{\alpha^s}(x)$ *where s runs through* **some** *subset S of representatives of distinct q-cyclotomic cosets modulo n.*

(d) *There are* 2^m *linear cyclic codes of length n where m is the number of distinct q-cyclotomic cosets modulo n.*

Definition

Let $g(x) = \prod_{s \in S} M_{\alpha^s}(x)$ be the generator polynomial of $\mathcal{C}$. Let $T = \bigcup_{s \in S} C_{s,q,n}$; T is the defining set of $\mathcal{C}$ relative to α.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

An element e in a ring $\mathfrak{R}$ is an idempotent provided $e^2 = e$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n,q)=1$ (cont.)

Definition

An element e in a ring $\mathfrak{R}$ is an idempotent provided $e^2 = e$.

Theorem

Let $\mathcal{C}$ be an $[n,k]_q$ linear cyclic code over $\mathbb{F}_q$ with generator polynomial $g(x)$. The following hold.

(a) *There exists a unique idempotent $\mathbf{e}(x) \in \mathcal{P}_{\mathbb{F}_q,n}$ such that $\mathcal{C} = \langle \mathbf{e}(x) \rangle$.*

(b) *Let $h(x) = (x^n - 1)/g(x)$. If $1 = a(x)g(x) + b(x)h(x)$ in $\mathbb{F}_q[x]$, then $\mathbf{e}(x) = \mathbf{a}(x)\mathbf{g}(x)$.*

(c) *$g(x) = gcd(e(x), x^n - 1)$.*

(d) *$\{\mathbf{e}(x), x\mathbf{e}(x), \ldots, x^{k-1}\mathbf{e}(x)\}$ is a basis of $\mathcal{C}$.*

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

An element e in a ring $\mathfrak{R}$ is an idempotent provided $e^2 = e$.

Theorem

Let $\mathcal{C}$ be an $[n, k]_q$ linear cyclic code over $\mathbb{F}_q$ with generator polynomial $g(x)$. The following hold.

(a) *There exists a unique idempotent $\mathbf{e}(x) \in \mathcal{P}_{\mathbb{F}_q,n}$ such that $\mathcal{C} = \langle \mathbf{e}(x) \rangle$.*

(b) *Let $h(x) = (x^n - 1)/g(x)$. If $1 = a(x)g(x) + b(x)h(x)$ in $\mathbb{F}_q[x]$, then $\mathbf{e}(x) = \mathbf{a}(x)\mathbf{g}(x)$.*

(c) *$g(x) = gcd(e(x), x^n - 1)$.*

(d) *$\{\mathbf{e}(x), x\mathbf{e}(x), \ldots, x^{k-1}\mathbf{e}(x)\}$ is a basis of $\mathcal{C}$.*

Definition

$\mathbf{e}(x)$ is the generating idempotent of $\mathcal{C}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $a \in \mathbb{Z}$ with $\gcd(n, a) = 1$. Define the map $\mu_{a,n} : \mathcal{P}_{\mathbb{F}_q,n} \to \mathcal{P}_{\mathbb{F}_q,n}$ by $\mu_{a,n}(\mathbf{f}(x)) = \mathbf{f}(x^a)$. $\mu_{a,n}$ is a multiplier on $\mathcal{P}_{\mathbb{F}_q,n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $a \in \mathbb{Z}$ with $\gcd(n, a) = 1$. Define the map $\mu_{a,n} : \mathcal{P}_{\mathbb{F}_q,n} \to \mathcal{P}_{\mathbb{F}_q,n}$ by $\mu_{a,n}(\mathbf{f}(x)) = \mathbf{f}(x^a)$. $\mu_{a,n}$ is a multiplier on $\mathcal{P}_{\mathbb{F}_q,n}$.

Example

If $\mathbf{f}(x) = x + x^2 + x^4 \in \mathcal{P}_{\mathbb{F}_2,7}$, then $\mu_{-4,7}(\mathbf{f}(x)) = x^3 + x^5 + x^6$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $a \in \mathbb{Z}$ with $\gcd(n, a) = 1$. Define the map $\mu_{a,n} : \mathcal{P}_{\mathbb{F}_q,n} \to \mathcal{P}_{\mathbb{F}_q,n}$ by $\mu_{a,n}(\mathbf{f}(x)) = \mathbf{f}(x^a)$. $\mu_{a,n}$ is a multiplier on $\mathcal{P}_{\mathbb{F}_q,n}$.

Example

If $\mathbf{f}(x) = x + x^2 + x^4 \in \mathcal{P}_{\mathbb{F}_2,7}$, then $\mu_{-4,7}(\mathbf{f}(x)) = x^3 + x^5 + x^6$.
$x + x^2 + x^4 = x^1 + x^2 + x^4 \to x^{-4} + x^{-8} + x^{-16} \to x^3 + x^6 + x^5$

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $a \in \mathbb{Z}$ with $\gcd(n, a) = 1$. Define the map $\mu_{a,n} : \mathcal{P}_{\mathbb{F}_q,n} \to \mathcal{P}_{\mathbb{F}_q,n}$ by $\mu_{a,n}(\mathbf{f}(x)) = \mathbf{f}(x^a)$. $\mu_{a,n}$ is a multiplier on $\mathcal{P}_{\mathbb{F}_q,n}$.

Example

If $\mathbf{f}(x) = x + x^2 + x^4 \in \mathcal{P}_{\mathbb{F}_2,7}$, then $\mu_{-4,7}(\mathbf{f}(x)) = x^3 + x^5 + x^6$.
$x + x^2 + x^4 = x^1 + x^2 + x^4 \to x^{-4} + x^{-8} + x^{-16} \to x^3 + x^6 + x^5$

Theorem

Let $a \in \mathbb{Z}$ with $\gcd(n, a) = 1$. The following hold.

(a) *$\mu_{a,n}$ is a ring automorphism of $\mathcal{P}_{\mathbb{F}_q,n}$.*

(b) *If $\mathbf{e}(x)$ is an idempotent of $\mathcal{P}_{\mathbb{F}_q,n}$, so is $\mu_{a,n}(\mathbf{e}(x))$.*

(c) *Let $\mathcal{C}$ be a linear cyclic code of length n over $\mathbb{F}_q$ with generating idempotent $\mathbf{e}(x)$ and defining set T with respect to α. Then $\mu_{a,n}(\mathcal{C})$ is a linear cyclic code with generating idempotent $\mu_{a,n}(\mathbf{e}(x))$ and defining set $a^{-1}T \bmod n$ where $aa^{-1} \equiv 1 \pmod{n}$.*

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

Let $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2$ be linear cyclic codes of length n over $\mathbb{F}_q$ with generator polynomials $g(x), g_1(x), g_2(x)$, defining sets T, T_1, T_2, and generating idempotents $\mathbf{e}(x), \mathbf{e}_1(x), \mathbf{e}_2(x)$. The following hold.

(a) $\mathcal{C}_1 \subseteq \mathcal{C}_2$ *if and only if* $g_2(x) \mid g_1(x)$ *in* $\mathbb{F}_q[x]$ *if and only if* $T_2 \subseteq T_1$.

(b) $\mathcal{C}_1 + \mathcal{C}_2$ *is a cyclic code with generator polynomial* $\gcd(g_1(x), g_2(x))$, *defining set* $T_1 \cap T_2$, *and generating idempotent* $\mathbf{e}_1(x) + \mathbf{e}_2(x) - \mathbf{e}_1(x)\mathbf{e}_2(x)$.

(c) $\mathcal{C}_1 \cap \mathcal{C}_2$ *is a cyclic code with generator polynomial* $\mathrm{lcm}(g_1(x), g_2(x))$, *defining set* $T_1 \cup T_2$, *and generating idempotent* $\mathbf{e}_1(x)\mathbf{e}_2(x)$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Theorem

Let $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2$ be linear cyclic codes of length n over $\mathbb{F}_q$ with generator polynomials $g(x), g_1(x), g_2(x)$, defining sets T, T_1, T_2, and generating idempotents $\mathbf{e}(x), \mathbf{e}_1(x), \mathbf{e}_2(x)$. The following hold.

(a) $\mathcal{C}_1 \subseteq \mathcal{C}_2$ *if and only if* $g_2(x) \mid g_1(x)$ *in* $\mathbb{F}_q[x]$ *if and only if* $T_2 \subseteq T_1$.

(b) $\mathcal{C}_1 + \mathcal{C}_2$ *is a cyclic code with generator polynomial* $\gcd(g_1(x), g_2(x))$*, defining set* $T_1 \cap T_2$*, and generating idempotent* $\mathbf{e}_1(x) + \mathbf{e}_2(x) - \mathbf{e}_1(x)\mathbf{e}_2(x)$.

(c) $\mathcal{C}_1 \cap \mathcal{C}_2$ *is a cyclic code with generator polynomial* $\mathrm{lcm}(g_1(x), g_2(x))$*, defining set* $T_1 \cup T_2$*, and generating idempotent* $\mathbf{e}_1(x)\mathbf{e}_2(x)$.

(d) $\mathcal{C}^{\perp_E}$ *is a cyclic code with generating idempotent* $1 - \mu_{-1,n}(\mathbf{e}(x))$*, defining set* $\{0, 1, \ldots, n-1\} \setminus (-1)T \bmod n$*, and generator polynomial*

$$\frac{x^k}{h(0)} h(x^{-1})$$

where $k = \dim_{\mathbb{F}_q}(\mathcal{C})$ *and* $h(x) = (x^n - 1)/g(x)$.

Binary Linear Cyclic Codes of Length 7

- $C_{0,2,7} = \{0\}$, $C_{1,2,7} = \{1, 2, 4\}$, $C_{3,2,7} = \{3, 6, 5\}$.

Binary Linear Cyclic Codes of Length 7

- $C_{0,2,7} = \{0\}$, $C_{1,2,7} = \{1, 2, 4\}$, $C_{3,2,7} = \{3, 6, 5\}$.
- $x^7 - 1 = x^7 + 1$ splits in $\mathbb{F}_8$, which has a primitive element γ satisfying $\gamma^3 = 1 + \gamma$. $\alpha = \gamma$ is a primitive 7^{th} root of unity.

Binary Linear Cyclic Codes of Length 7

- $C_{0,2,7} = \{0\}$, $C_{1,2,7} = \{1, 2, 4\}$, $C_{3,2,7} = \{3, 6, 5\}$.
- $x^7 - 1 = x^7 + 1$ splits in $\mathbb{F}_8$, which has a primitive element γ satisfying $\gamma^3 = 1 + \gamma$. $\alpha = \gamma$ is a primitive 7^{th} root of unity.
- $M_{\alpha^0}(x) = 1 + x$, $M_{\alpha^1}(x) = 1 + x + x^3$, $M_{\alpha^3}(x) = 1 + x^2 + x^3$.

Binary Linear Cyclic Codes of Length 7 (cont.)

i	dim	d_H	$g_i(x)$ $e_i(x)$	defining set
0	0	$-$	$1+x^7$ 0	$\{0,1,\dots,6\}$
1	1	7	$1+x+\cdots+x^6$ $1+x+\cdots+x^6$	$\{1,2,\dots,6\}$
2	3	4	$1+x^2+x^3+x^4$ $1+x^3+x^5+x^6$	$\{0,1,2,4\}$
3	3	4	$1+x+x^2+x^4$ $1+x+x^2+x^4$	$\{0,3,5,6\}$
4	4	3	$1+x+x^3$ $x+x^2+x^4$	$\{1,2,4\}$
5	4	3	$1+x^2+x^3$ $x^3+x^5+x^6$	$\{3,5,6\}$
6	6	2	$1+x$ $x+x^2+\cdots+x^6$	$\{0\}$
7	7	1	1 1	$\emptyset$

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $\mathcal{N} = \{0, 1, \ldots, n-1\}$. $T \subseteq \mathcal{N}$ contains a set of $s \leq n$ consecutive elements provided there exists $b \in \mathcal{N}$ such that such that $\{b, b+1, \ldots, b+s-1\} \bmod n \subseteq T$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $\mathcal{N} = \{0, 1, \ldots, n-1\}$. $T \subseteq \mathcal{N}$ contains a set of $s \leq n$ consecutive elements provided there exists $b \in \mathcal{N}$ such that such that $\{b, b+1, \ldots, b+s-1\} \bmod n \subseteq T$.

Theorem (BCH Bound)

Let $\mathcal{C}$ be a linear cyclic code of length n over $\mathbb{F}_q$ and minimum distance $d_H(\mathcal{C})$ with defining set T relative to α. Assume T contains $\delta - 1$ consecutive elements for some integer $\delta \geq 2$. Then

$$d_H(\mathcal{C}) \geq \delta.$$

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $b, \delta \in \mathbb{Z}$ with $0 \leq b \leq n-1$, $2 \leq \delta \leq n$. The BCH code over $\mathbb{F}_q$ of length n and designed distance δ is the linear cyclic code with defining set

$$T = C_{b,q,n} \cup C_{b+1,q,n} \cup \cdots \cup C_{b+\delta-2,q,n}$$

relative to α. If $b = 1$, the code is narrow-sense. If $n = q^t - 1$ for some t, the code is primitive. A BCH code can have more than one designed distance; the largest designed distance is called the Bose distance.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Definition

Let $b, \delta \in \mathbb{Z}$ with $0 \leq b \leq n-1$, $2 \leq \delta \leq n$. The BCH code over $\mathbb{F}_q$ of length n and designed distance δ is the linear cyclic code with defining set

$$T = C_{b,q,n} \cup C_{b+1,q,n} \cup \cdots \cup C_{b+\delta-2,q,n}$$

relative to α. If $b = 1$, the code is narrow-sense. If $n = q^t - 1$ for some t, the code is primitive. A BCH code can have more than one designed distance; the largest designed distance is called the Bose distance.

Remark

The BCH code with defining set T is an $[n, n - |T|, d_H]_q$ code with $d_H \geq \delta$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Origins of BCH Codes

The binary BCH codes were discovered by A. Hocquenghem[1] and independently by R. C. Bose and D. K. Ray-Chaudhuri[2] [3] and were generalized to all finite fields by D. C. Gorenstein and N. Zierler.[4]

[1] A. Hocquenghem, “Codes correcteurs d'erreurs”, *Chiffres (Paris)* **2** (1959), 147–156.

[2] R. C. Bose and D. K. Ray-Chaudhuri, “On a class of error correcting binary group codes”, *Inform. and Control* **3** (1960), 68–79.

[3] R. C. Bose and D. K. Ray-Chaudhuri, “Further results on error correcting binary group codes”, *Inform. and Control* **3** (1960), 279–290.

[4] D. C. Gorenstein and N. Zierler, “A class of error-correcting codes in p^m symbols”, *J. SIAM* **9** (1961), 207–214.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 7)

All seven nonzero binary cyclic codes of length 7 are BCH with d_H equalling the Bose designed distance.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 7)

All seven nonzero binary cyclic codes of length 7 are BCH with d_H equalling the Bose designed distance.

- The code $\mathcal{C}_4$ has defining set $\{1, 2, 4\} = C_{1,2,7} = C_{1,2,7} \cup C_{2,2,7}$ is a BCH code with $b = 1$ and designed distance either 2 or 3. $\mathcal{C}_4$ is a $[7, 4, 3]_2$ code.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 7)

All seven nonzero binary cyclic codes of length 7 are BCH with d_H equalling the Bose designed distance.

- The code $\mathcal{C}_4$ has defining set $\{1, 2, 4\} = C_{1,2,7} = C_{1,2,7} \cup C_{2,2,7}$ is a BCH code with $b = 1$ and designed distance either 2 or 3. $\mathcal{C}_4$ is a $[7, 4, 3]_2$ code.
- The code $\mathcal{C}_3$ has defining set $\{0, 3, 5, 6\} = C_{0,2,7} \cup C_{3,2,7} = C_{6,2,7} \cup C_{0,2,7} = C_{5,2,7} \cup C_{6,2,7} \cup C_{0,2,7}$ is a BCH code with $b = 6$ and designed distance 3 or $b = 5$ and designed distance 4. $\mathcal{C}_4$ is a $[7, 3, 4]_2$ code.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 23)

The $[23, 12, 7]_2$ binary Golay code[5] has a cyclic formulation as a narrow-sense BCH code.

[5] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 23)

The $[23, 12, 7]_2$ binary Golay code[5] has a cyclic formulation as a narrow-sense BCH code.

- Defining set: $\{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\} = C_{1,2,23} = C_{1,2,23} \cup C_{2,2,23} \cup C_{3,2,23} \cup C_{4,2,23}$.
- Bose designed distance: $\delta = 5$.
- Relative to some α: $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ and $\mathbf{e}(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}$.

[5] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Binary Length 23)

The $[23, 12, 7]_2$ binary Golay code[5] has a cyclic formulation as a narrow-sense BCH code.

- Defining set: $\{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\} = C_{1,2,23} = C_{1,2,23} \cup C_{2,2,23} \cup C_{3,2,23} \cup C_{4,2,23}$.
- Bose designed distance: $\delta = 5$.
- Relative to some α: $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ and $\mathbf{e}(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}$.

Remark

Voyager 1 and *Voyager 2* were launched in 1979 to explore Jupiter, Saturn, and their moons. The General Science and Engineering (GSE) data was transmitted using a concatenated code whose outer encoder was the $[24, 12, 8]_2$ Golay code.

---

[5] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Ternary Length 11)

The $[11, 6, 5]_3$ ternary Golay code[6] has a cyclic formulation as both a narrow-sense and a non-narrow-sense BCH code.

[6] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Ternary Length 11)

The $[11, 6, 5]_3$ ternary Golay code[6] has a cyclic formulation as both a narrow-sense and a non-narrow-sense BCH code.

- Defining set:
  $\{1, 3, 9, 5, 4\} = C_{1,3,11} = C_{3,3,11} \cup C_{4,3,11} \cup C_{5,3,11}$.
- Bose designed distance: $\delta = 4$.
- Relative to some α: $g(x) = -1 + x^2 - x^3 + x^4 + x^5$ and $\mathbf{e}(x) = -(x^2 + x^6 + x^7 + x^8 + x^{10})$.

[6] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Hamming Codes)

Let $r \in \mathbb{Z}$ with $r \geq 2$ and $n = (q^r - 1)/(q - 1)$. Let $H_{r,q} \in \mathrm{Mat}_{r \times n}(\mathbb{F}_q)$ have columns consisting of a nonzero vector from each 1-dimensional subspace of $\mathbb{F}_q^r$. The $[n, n - r, 3]_q$ linear code $\mathcal{H}_{r,q}$ with parity check matrix $H_{r,q}$ is called a Hamming code. Not every Hamming code has a cyclic formulation (e.g. $\mathcal{H}_{2,3}$).

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

Example (Hamming Codes)

Let $r \in \mathbb{Z}$ with $r \geq 2$ and $n = (q^r - 1)/(q - 1)$. Let $H_{r,q} \in \mathrm{Mat}_{r \times n}(\mathbb{F}_q)$ have columns consisting of a nonzero vector from each 1-dimensional subspace of $\mathbb{F}_q^r$. The $[n, n-r, 3]_q$ linear code $\mathcal{H}_{r,q}$ with parity check matrix $H_{r,q}$ is called a Hamming code. Not every Hamming code has a cyclic formulation (e.g. $\mathcal{H}_{2,3}$).

Theorem

If $\gcd(r, q-1) = 1$, then a code monomially equivalent to $\mathcal{H}_{r,q}$ is a narrow-sense BCH code with defining set $C_{1,q,n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) = 1$ (cont.)

The $[7, 4, 3]_2$ code $\mathcal{H}_{3,2}$ was discovered in 1947 by R. W. Hamming.[7] This code also appeared in C. E. Shannon's 1948 seminal paper.[8] It was generalized to codes over fields of prime order by M. J. E. Golay.[9]

[7] R. W. Hamming, "Error detecting and error correcting codes", *Bell System Tech. J.* **29** (1950), 10–23.

[8] C. Shannon, "A mathematical theory of communication", *Bell System Tech. J.*, **27** (1948), 379–423 and 623–656.

[9] M. J. E. Golay, "Notes on digital coding", *Proc. IRE* **37** (1949), 657.

An Equivalence Result

The following is a consequence of a theorem due to P. P. Pálfy.[10]

Theorem

For $i \in \{1, 2\}$, let $\mathcal{C}_i$ be a linear cyclic code of length n over $\mathbb{F}_q$ ($\gcd(n, q) = 1$) with generating idempotent $\mathbf{e}_i(x)$ and defining set T_i. Suppose $\gcd(n, \phi(n)) = 1$ or $n = 4$ (with q odd in this case) where ϕ is the Euler totient. The following are equivalent.

(a) *$\mathcal{C}_1$ and $\mathcal{C}_2$ are permutation equivalent.*

(b) *$\mathcal{C}_2 = \mu_{a,n}(\mathcal{C}_1)$ for some $1 \leq a < n$ with $\gcd(a, n) = 1$.*

(c) *$\mathbf{e}_2(x) = \mu_{a,n}(\mathbf{e}_1(x))$ for some $1 \leq a < n$ with $\gcd(a, n) = 1$.*

(d) *$T_2 = bT_1 \bmod n$ for some $1 \leq b < n$ with $\gcd(b, n) = 1$.*

[10] P. P. Pálfy, "Isomorphism problem for relational structures with a cyclic automorphism", *European J. Combin.* **8** (1987), 35–43.

An Equivalence Result

The following is a consequence of a theorem due to P. P. Pálfy.[10]

Theorem

For $i \in \{1, 2\}$, let $\mathcal{C}_i$ be a linear cyclic code of length n over $\mathbb{F}_q$ ($\gcd(n, q) = 1$) with generating idempotent $\mathbf{e}_i(x)$ and defining set T_i. Suppose $\gcd(n, \phi(n)) = 1$ or $n = 4$ (with q odd in this case) where ϕ is the Euler totient. The following are equivalent.

(a) *$\mathcal{C}_1$ and $\mathcal{C}_2$ are permutation equivalent.*

(b) *$\mathcal{C}_2 = \mu_{a,n}(\mathcal{C}_1)$ for some $1 \le a < n$ with $\gcd(a, n) = 1$.*

(c) *$\mathbf{e}_2(x) = \mu_{a,n}(\mathbf{e}_1(x))$ for some $1 \le a < n$ with $\gcd(a, n) = 1$.*

(d) *$T_2 = bT_1 \bmod n$ for some $1 \le b < n$ with $\gcd(b, n) = 1$.*

Implication

Rather than checking $n!$ permutations in Sym_n, you need to check no more than $\phi(n)$ multipliers.

---

[10] P. P. Pálfy, "Isomorphism problem for relational structures with a cyclic automorphism", *European J. Combin.* **8** (1987), 35–43.

An Equivalence Result (cont.)

Actually!

If T is a union of q-cyclotomic cosets modulo n, then $T = qT \bmod n$. You only need to check one representative b from each q-cyclotomic coset that has elements relatively prime to n, excluding $C_{1,q,n}$.

An Equivalence Result (cont.)

Actually!

If T is a union of q-cyclotomic cosets modulo n, then $T = qT \bmod n$. You only need to check one representative b from each q-cyclotomic coset that has elements relatively prime to n, excluding $C_{1,q,n}$.

Example (Binary Length 7)

The most general equivalence of binary linear codes is permutation equivalence. To check equivalence of $[7, k]_2$ cyclic codes, you only need to check $b = 3$. $\mathcal{C}_2$ and $\mathcal{C}_3$ have defining set $T_2 = \{0, 1, 2, 4\}$ and $T_3 = \{0, 3, 5, 6\}$. Since $T_3 = 3T_2 \bmod 7$, $\mathcal{C}_2$ and $\mathcal{C}_3$ are equivalent.

An Equivalence Result (cont.)

Actually!

If T is a union of q-cyclotomic cosets modulo n, then $T = qT \bmod n$. You only need to check one representative b from each q-cyclotomic coset that has elements relatively prime to n, excluding $C_{1,q,n}$.

Example (Binary Length 7)

The most general equivalence of binary linear codes is permutation equivalence. To check equivalence of $[7, k]_2$ cyclic codes, you only need to check $b = 3$. $\mathcal{C}_2$ and $\mathcal{C}_3$ have defining set $T_2 = \{0, 1, 2, 4\}$ and $T_3 = \{0, 3, 5, 6\}$. Since $T_3 = 3T_2 \bmod 7$, $\mathcal{C}_2$ and $\mathcal{C}_3$ are equivalent.

Example (Binary Length 31)

$q = 2$, $n = 31$. Check $b = 3, 5, 7, 11, 15$.

- There are 6 $[31, 26]_2$ cyclic codes. All are equivalent.
- There are 15 $[31, 21]_2$ cyclic codes that split into 3 equivalence classes.
- There are 20 $[31, 16]_2$ cyclic codes that split into 4 equivalence classes.

An Equivalence Result (cont.)

Definition

Suppose you have a class of combinatorial objects on $\{0, 1, \ldots, n-1\}$ where equivalence between two objects is defined by permutations of Sym_n. A cyclic combinatorial object is one fixed by the permutation $i \mapsto i + 1 \bmod n$.

An Equivalence Result (cont.)

Definition

Suppose you have a class of combinatorial objects on $\{0, 1, \ldots, n-1\}$ where equivalence between two objects is defined by permutations of Sym_n. A cyclic combinatorial object is one fixed by the permutation $i \mapsto i + 1 \bmod n$.

Theorem

Suppose r, s are distinct primes with $\gcd(rs, \phi(rs)) \neq 1$. If $n = r^2$ [11] or $n = rs$ [12], then two cyclic combinatorial objects on n elements are equivalent if and only if they are equivalent by elements chosen from a specified list of at most $\phi(n)$ permutations.

---

[11] W. C. Huffman, V. Job, V. S. Pless, "Multipliers and generalized multipliers of cyclic objects and cyclic codes", *J. Combin. Theory Ser. A* **62** (1993), 183–215.

[12] W. C. Huffman, "The equivalence of two cyclic objects on *pq* elements," *Discrete Math.* **154** (1996), 103–127.

An Equivalence Result (cont.)

Definition

Suppose you have a class of combinatorial objects on $\{0, 1, \ldots, n-1\}$ where equivalence between two objects is defined by permutations of Sym_n. A cyclic combinatorial object is one fixed by the permutation $i \mapsto i + 1 \bmod n$.

Theorem

Suppose r, s are distinct primes with $\gcd(rs, \phi(rs)) \neq 1$. If $n = r^2$ [11] or $n = rs$ [12], then two cyclic combinatorial objects on n elements are equivalent if and only if they are equivalent by elements chosen from a specified list of at most $\phi(n)$ permutations.

Open Question

Does a similar result hold for other values of n with $\gcd(n, \phi(n)) \neq 1$?

---

[11] W. C. Huffman, V. Job, V. S. Pless, "Multipliers and generalized multipliers of cyclic objects and cyclic codes", *J. Combin. Theory Ser. A* **62** (1993), 183–215.

[12] W. C. Huffman, "The equivalence of two cyclic objects on *pq* elements," *Discrete Math.* **154** (1996), 103–127.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$

What Changes

The ring $\mathcal{P}_{\mathbb{F}_q,n}$ is no longer semi-simple and $x^n - 1$ has repeated roots.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$

What Changes

The ring $\mathcal{P}_{\mathbb{F}_q,n}$ is no longer semi-simple and $x^n - 1$ has repeated roots.

Notation

- Let p be the characteristic of $\mathbb{F}_q$ and $n = p^a\overline{n}$ where $a \geq 1$ and $p \nmid \overline{n}$.
- Let α be a primitive $\overline{n}^{\text{th}}$ root of unity and define $M_{\alpha^s}(x) = \prod_{i \in C_{s,q,\overline{n}}}(x - \alpha^i)$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

What Happens

- $x^n - 1 = (x^{\overline{n}} - 1)^{p^a} = \prod_s (M_{\alpha^s}(x))^{p^a}$ where s runs through a set of representatives of **all** distinct q-cyclotomic cosets modulo $\overline{n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

What Happens

- $x^n - 1 = (x^{\overline{n}} - 1)^{p^a} = \prod_s (M_{\alpha^s}(x))^{p^a}$ where s runs through a set of representatives of **all** distinct q-cyclotomic cosets modulo $\overline{n}$.
- If $g(x)$ is the generator polynomial of a linear cyclic code of length n, then

$$g(x) = \prod_{s \in S} (M_{\alpha^s}(x))^{i_s}$$

where $1 \leq i_s \leq p^a$ and s runs through **some** subset S of representatives of distinct q-cyclotomic cosets modulo $\overline{n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

What Happens

- $x^n - 1 = (x^{\overline{n}} - 1)^{p^a} = \prod_s (M_{\alpha^s}(x))^{p^a}$ where s runs through a set of representatives of **all** distinct q-cyclotomic cosets modulo $\overline{n}$.
- If $g(x)$ is the generator polynomial of a linear cyclic code of length n, then

$$g(x) = \prod_{s \in S} (M_{\alpha^s}(x))^{i_s}$$

  where $1 \leq i_s \leq p^a$ and s runs through **some** subset S of representatives of distinct q-cyclotomic cosets modulo $\overline{n}$.
- There are $(p^a + 1)^m$ linear cyclic codes of length n where m is the number of distinct q-cyclotomic cosets modulo $\overline{n}$.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

What Happens

- $x^n - 1 = (x^{\overline{n}} - 1)^{p^a} = \prod_s (M_{\alpha^s}(x))^{p^a}$ where s runs through a set of representatives of **all** distinct q-cyclotomic cosets modulo $\overline{n}$.
- If $g(x)$ is the generator polynomial of a linear cyclic code of length n, then

$$g(x) = \prod_{s \in S} (M_{\alpha^s}(x))^{i_s}$$

  where $1 \leq i_s \leq p^a$ and s runs through **some** subset S of representatives of distinct q-cyclotomic cosets modulo $\overline{n}$.
- There are $(p^a + 1)^m$ linear cyclic codes of length n where m is the number of distinct q-cyclotomic cosets modulo $\overline{n}$.
- Defining sets are unions of q-cyclotomic cosets modulo $\overline{n}$ but must include multiplicity.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

What Happens

- $x^n - 1 = (x^{\overline{n}} - 1)^{p^a} = \prod_s (M_{\alpha^s}(x))^{p^a}$ where s runs through a set of representatives of **all** distinct q-cyclotomic cosets modulo $\overline{n}$.
- If $g(x)$ is the generator polynomial of a linear cyclic code of length n, then
$$g(x) = \prod_{s \in S} (M_{\alpha^s}(x))^{i_s}$$
where $1 \leq i_s \leq p^a$ and s runs through **some** subset S of representatives of distinct q-cyclotomic cosets modulo $\overline{n}$.
- There are $(p^a + 1)^m$ linear cyclic codes of length n where m is the number of distinct q-cyclotomic cosets modulo $\overline{n}$.
- Defining sets are unions of q-cyclotomic cosets modulo $\overline{n}$ but must include multiplicity.
- The BCH Bound still holds when consecutive sets are defined modulo $\overline{n}$; the multiplicity does not improve the bound.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

History

- These cyclic codes are called repeated-root cyclic codes.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

History

- These cyclic codes are called repeated-root cyclic codes.
- Repeated-root cyclic codes were first studied in 1991 by J. H. van Lint[13] and Guy Castagnoli et al.[14]

[13] J. H. van Lint, "Repeated-root cyclic codes", *IEEE Trans. Inform. Theory* **37** (1991), 343–345.

[14] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seeman, "On repeated-root cyclic codes", *IEEE Trans. Inform. Theory* **37** (1991), 337–342.

Linear Cyclic Codes over $\mathbb{F}_q$, $\gcd(n, q) \neq 1$ (cont.)

History

- These cyclic codes are called repeated-root cyclic codes.
- Repeated-root cyclic codes were first studied in 1991 by J. H. van Lint[13] and Guy Castagnoli et al.[14]

Theorem (Castagnoli et al.)

Let $\mathcal{C}$ be an $[n, k, d_H(\mathcal{C})]_q$ linear repeated-root cyclic code. There exists a linear (single-root) cyclic code $\mathcal{C}_1$ with parameters $[\overline{n}, k_1, d_H(\mathcal{C}_1)]_q$ such that

$$\frac{k_1}{\overline{n}} \geq \frac{k}{n} \quad \textit{and} \quad \frac{d_H(\mathcal{C}_1)}{\overline{n}} \geq \frac{d_H(\mathcal{C})}{n}.$$

[13] J. H. van Lint, "Repeated-root cyclic codes", *IEEE Trans. Inform. Theory* **37** (1991), 343–345.

[14] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seeman, "On repeated-root cyclic codes", *IEEE Trans. Inform. Theory* **37** (1991), 337–342.

Linear Cyclic Codes over $\mathbb{Z}_4$

How Does $\mathbb{Z}_4[x]$ Differ From $\mathbb{F}_q[x]$?

- In $\mathbb{Z}_4[x]$, the degree of a product may be less than the sum of the degrees.
- In $\mathbb{Z}_4[x]$, units are not necessarily constant polynomials (e.g. $1 + 2f(x)$).
- $\mathbb{Z}_4[x]$ has divisors of zero, is not a unique factorization ring, and is not a principal ideal ring.

Linear Cyclic Codes over $\mathbb{Z}_4$

How Does $\mathbb{Z}_4[x]$ Differ From $\mathbb{F}_q[x]$?

- In $\mathbb{Z}_4[x]$, the degree of a product may be less than the sum of the degrees.
- In $\mathbb{Z}_4[x]$, units are not necessarily constant polynomials (e.g. $1 + 2f(x)$).
- $\mathbb{Z}_4[x]$ has divisors of zero, is not a unique factorization ring, and is not a principal ideal ring.

Definition

$f(x) \in \mathbb{Z}_4[x]$ is irreducible over $\mathbb{Z}_4$ if $f(x)$ is not a unit and whenever $f(x) = g(x)h(x)$ with $f(x), g(x) \in \mathbb{Z}_4[x]$, one of $f(x), g(x)$ is a unit.

Linear Cyclic Codes over $\mathbb{Z}_4$

How Does $\mathbb{Z}_4[x]$ Differ From $\mathbb{F}_q[x]$?

- In $\mathbb{Z}_4[x]$, the degree of a product may be less than the sum of the degrees.
- In $\mathbb{Z}_4[x]$, units are not necessarily constant polynomials (e.g. $1 + 2f(x)$).
- $\mathbb{Z}_4[x]$ has divisors of zero, is not a unique factorization ring, and is not a principal ideal ring.

Definition

$f(x) \in \mathbb{Z}_4[x]$ is irreducible over $\mathbb{Z}_4$ if $f(x)$ is not a unit and whenever $f(x) = g(x)h(x)$ with $f(x), g(x) \in \mathbb{Z}_4[x]$, one of $f(x), g(x)$ is a unit.

Example (Factoring $x^4 - 1$ over $\mathbb{Z}_4$)

Two factorizations of $x^4 - 1$ into irreducibles:

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

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

The map $\nu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ is the reduction homomorphism where

$$\nu(f(x)) = f(x) \bmod 2$$

(i.e. $\nu(0) = \nu(2) = 0$, $\nu(1) = \nu(3) = 1$, $\nu(x^i) = x^i$).

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

The map $\nu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ is the reduction homomorphism where

$$\nu(f(x)) = f(x) \bmod 2$$

(i.e. $\nu(0) = \nu(2) = 0$, $\nu(1) = \nu(3) = 1$, $\nu(x^i) = x^i$).

Remark

ν is a surjective ring homomorphism with kernel

$$\langle 2 \rangle = \{2s(x) \mid s(x) \in \mathbb{Z}_4[x]\}.$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

The map $\nu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ is the reduction homomorphism where

$$\nu(f(x)) = f(x) \bmod 2$$

(i.e. $\nu(0) = \nu(2) = 0$, $\nu(1) = \nu(3) = 1$, $\nu(x^i) = x^i$).

Remark

ν is a surjective ring homomorphism with kernel

$$\langle 2 \rangle = \{2s(x) \mid s(x) \in \mathbb{Z}_4[x]\}.$$

Definition

For $\mathfrak{R} = \mathbb{Z}_4[x]$ or $\mathbb{F}_2[x]$, two polynomials $f(x), g(x) \in \mathfrak{R}$ are coprime provided $\mathfrak{R} = \langle f(x) \rangle + \langle g(x) \rangle$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

The map $\nu : \mathbb{Z}_4[x] \to \mathbb{F}_2[x]$ is the reduction homomorphism where

$$\nu(f(x)) = f(x) \bmod 2$$

(i.e. $\nu(0) = \nu(2) = 0$, $\nu(1) = \nu(3) = 1$, $\nu(x^i) = x^i$).

Remark

ν is a surjective ring homomorphism with kernel

$$\langle 2 \rangle = \{2s(x) \mid s(x) \in \mathbb{Z}_4[x]\}.$$

Definition

For $\mathfrak{R} = \mathbb{Z}_4[x]$ or $\mathbb{F}_2[x]$, two polynomials $f(x), g(x) \in \mathfrak{R}$ are coprime provided $\mathfrak{R} = \langle f(x) \rangle + \langle g(x) \rangle$.

Two Tools

- A special case of Hensel's Lemma.
- A special case of Graeffe's Method.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Theorem (Hensel's Lemma)

Let $f(x) \in \mathbb{Z}_4[x]$. Suppose $\nu(f(x)) = h_1(x)h_2(x)\cdots h_k(x)$ where $h_i(x) \in \mathbb{F}_2[x]$ are pairwise coprime. Then there exist $g_1(x), g_2(x), \ldots, g_k(x) \in \mathbb{Z}_4[x]$ such that

(a) $\nu(g_i(x)) = h_i(x)$ *for* $1 \leq i \leq k$,

(b) *the* $g_i(x)$ *are pairwise coprime, and*

(c) $f(x) = g_1(x)g_2(x)\cdots g_k(x)$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Theorem (Hensel's Lemma)

Let $f(x) \in \mathbb{Z}_4[x]$. Suppose $\nu(f(x)) = h_1(x)h_2(x)\cdots h_k(x)$ where $h_i(x) \in \mathbb{F}_2[x]$ are pairwise coprime. Then there exist $g_1(x), g_2(x), \ldots, g_k(x) \in \mathbb{Z}_4[x]$ such that

(a) $\nu(g_i(x)) = h_i(x)$ *for* $1 \leq i \leq k$,

(b) *the* $g_i(x)$ *are pairwise coprime, and*

(c) $f(x) = g_1(x)g_2(x)\cdots g_k(x)$.

Theorem

Let n be odd. Then $x^n - 1 = g_1(x)g_2(x)\cdots g_k(x)$ where $g_i(x)$ are unique monic irreducible pairwise coprime polynomials in $\mathbb{Z}_4[x]$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Graeffe's Method

Step I For n odd, factor $x^n - 1 = h_1(x)h_2(x)\cdots h_k(x)$ where $h_i(x) \in \mathbb{F}_2[x]$ are irreducible over $\mathbb{F}_2$.

Step II Write $h_i(x) = e_i(x) + o_i(x)$ where $e_i(x)$, respectively $o_i(x)$, is the sum of the terms of $h_i(x)$ of even, respectively odd, exponent.

Step III Let $g_i(x^2) = \pm(e(x)^2 - o(x)^2) \in \mathbb{Z}_4[x]$ (sign chosen so $g_i(x^2)$ is monic). Then $\nu(g_i(x)) = h_i(x)$, $g_i(x)$ are monic irreducible pairwise coprime polynomials, and

$$x^n - 1 = g_1(x)g_2(x)\cdots g_k(x) \in \mathbb{Z}_4[x].$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example (Factoring $x^7 - 1$ over $\mathbb{Z}_4$)

- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3) \in \mathbb{F}_2[x]$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example (Factoring $x^7 - 1$ over $\mathbb{Z}_4$)

- $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3) \in \mathbb{F}_2[x]$.
- $h_1(x) = 1 + x$; $e_1(x) = 1$, $o_1(x) = x$; $g_1(x^2) = \pm(1 - x^2)$
  $\Rightarrow g_1(x) = -1 + x$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example (Factoring $x^7 - 1$ over $\mathbb{Z}_4$)

- $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3) \in \mathbb{F}_2[x]$.
- $h_1(x) = 1 + x$; $e_1(x) = 1$, $o_1(x) = x$; $g_1(x^2) = \pm(1 - x^2)$
  $\Rightarrow g_1(x) = -1 + x$
- $h_2(x) = 1 + x + x^3$; $e_2(x) = 1$, $o_2(x) = x + x^3$;
  $g_2(x^2) = \pm(1 - (x + x^3)^2) = \pm(1 - x^2 - 2x^4 - x^6)$
  $\Rightarrow g_2(x) = -1 + x + 2x^2 + x^3$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example (Factoring $x^7 - 1$ over $\mathbb{Z}_4$)

- $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3) \in \mathbb{F}_2[x]$.
- $h_1(x) = 1+x$; $e_1(x) = 1$, $o_1(x) = x$; $g_1(x^2) = \pm(1-x^2)$
  $\Rightarrow g_1(x) = -1+x$
- $h_2(x) = 1+x+x^3$; $e_2(x) = 1$, $o_2(x) = x+x^3$;
  $g_2(x^2) = \pm(1-(x+x^3)^2) = \pm(1-x^2-2x^4-x^6)$
  $\Rightarrow g_2(x) = -1+x+2x^2+x^3$
- $h_3(x) = 1+x^2+x^3$; $e_3(x) = 1+x^2$, $o_3(x) = x^3$;
  $g_3(x^2) = \pm((1+x^2)^2-(x^3)^2) = \pm(1+2x^2+x^4-x^6)$
  $\Rightarrow g_3(x) = -1-2x-x^2+x^3$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Theorem

For n odd, let $x^n - 1 = g_1(x)g_2(x)\cdots g_k(x)$ where $g_i(x)$ are monic irreducible pairwise coprime polynomials of degree d_i in $\mathbb{Z}_4[x]$. Let $\widehat{g}_i(x) = \prod_{j\neq i} g_j(x)$. The following hold.

(a) *If $g(x)$ is a monic divisor of $x^n - 1$, it is a product of $g_i(x)$'s.*

(b) $\mathcal{P}_{\mathbb{Z}_4,n} = \langle \widehat{\mathbf{g}}_1(x)\rangle \oplus \langle \widehat{\mathbf{g}}_2(x)\rangle \oplus \cdots \oplus \langle \widehat{\mathbf{g}}_k(x)\rangle$.

(c) *If $1 \leq i \leq k$, $\langle \widehat{\mathbf{g}}_i(x)\rangle = \langle \widehat{\mathbf{e}}_i(x)\rangle$ where $\{\widehat{\mathbf{e}}_i(x) \mid 1 \leq i \leq k\}$ are idempotents of $\mathcal{P}_{\mathbb{Z}_4,n}$ with $\widehat{\mathbf{e}}_i(x)\widehat{\mathbf{e}}_j(x) = 0$ for $i \neq j$ and $\sum_{i=1}^{k} \widehat{\mathbf{e}}_i(x) = 1$.*

(d) *If $1 \leq i \leq k$, $\langle \widehat{\mathbf{g}}_i(x)\rangle \simeq \mathbb{Z}_4[x]/\langle g_i(x)\rangle$ and $\langle \widehat{\mathbf{g}}_i(x)\rangle$ is a Galois ring of order 4^{d_i}.*

(e) *Every ideal of $\mathcal{P}_{\mathbb{Z}_4,n}$ is a direct sum of $\langle \widehat{\mathbf{g}}_i(x)\rangle$'s and $\langle 2\widehat{\mathbf{g}}_j(x)\rangle$'s.*

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Theorem (Qian[15])

For n odd, let $\mathcal{C}$ be a linear cyclic code over $\mathbb{Z}_4$ of length n, considered as an ideal of $\mathcal{P}_{\mathbb{Z}_4,n}$. The following hold.

(a) *There exist unique monic polynomials $f(x), g(x), h(x) \in \mathbb{Z}_4[x]$ with $x^n - 1 = f(x)g(x)h(x)$ such that*

$$\mathcal{C} = \langle \mathbf{f}(x)\mathbf{g}(x) \rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x) \rangle.$$

(b) *There exist unique idempotents $\mathbf{e}(x), \mathbf{E}(x) \in \mathcal{P}_{\mathbb{Z}_4,n}$ such that $\langle \mathbf{f}(x)\mathbf{g}(x) \rangle = \langle \mathbf{e}(x) \rangle$, $\langle \mathbf{f}(x)\mathbf{h}(x) \rangle = \langle \mathbf{E}(x) \rangle$, and*

$$\mathcal{C} = \langle \mathbf{e}(x) \rangle \oplus \langle 2\mathbf{E}(x) \rangle = \langle \mathbf{e}(x) + 2\mathbf{E}(x) \rangle.$$

[15] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory* **42** (1996), 1594–1600.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Theorem (Qian[15])

For n odd, let $\mathcal{C}$ be a linear cyclic code over $\mathbb{Z}_4$ of length n, considered as an ideal of $\mathcal{P}_{\mathbb{Z}_4,n}$. The following hold.

(a) *There exist unique monic polynomials $f(x), g(x), h(x) \in \mathbb{Z}_4[x]$ with $x^n - 1 = f(x)g(x)h(x)$ such that*

$$\mathcal{C} = \langle \mathbf{f}(x)\mathbf{g}(x) \rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x) \rangle.$$

(b) *There exist unique idempotents $\mathbf{e}(x), \mathbf{E}(x) \in \mathcal{P}_{\mathbb{Z}_4,n}$ such that $\langle \mathbf{f}(x)\mathbf{g}(x) \rangle = \langle \mathbf{e}(x) \rangle$, $\langle \mathbf{f}(x)\mathbf{h}(x) \rangle = \langle \mathbf{E}(x) \rangle$, and*

$$\mathcal{C} = \langle \mathbf{e}(x) \rangle \oplus \langle 2\mathbf{E}(x) \rangle = \langle \mathbf{e}(x) + 2\mathbf{E}(x) \rangle.$$

Corollary

There are 3^k linear cyclic codes over $\mathbb{Z}_4$ of odd length n where k is the number of irreducible factors of $x^n - 1 \in \mathbb{Z}_4[x]$.

[15] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory* **42** (1996), 1594–1600.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Idempotents in $\mathcal{P}_{\mathbb{Z}_4,n}$

Theorem

For n odd, let $f(x)$ be a factor of $x^n - 1$ in $\mathbb{Z}_4[x]$. Let $b(x) \in \mathbb{F}_2[x]$ such that $\mathbf{b}(x)$ is a binary idempotent in $\mathcal{P}_{\mathbb{F}_2,n}$ and $\langle \mathbf{b}(x) \rangle = \langle \nu(\mathbf{f}(\mathbf{x})) \rangle$. Let $e(x) = (b(x)^2)$ computed in $\mathbb{Z}_4[x]$. Then $\mathbf{e}(x)$ is the generating idempotent for $\langle \mathbf{f}(x) \rangle$ in $\mathcal{P}_{\mathbb{Z}_4,n}$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$)

- $x^7 - 1 = g_1(x)g_2(x)g_3(x) = (-1 + x)(-1 + x + 2x^2 + x^3)(-1 - 2x - x^2 + x^3)$.
- $\widehat{g}_2(x) = g_1(x)g_3(x)$.
  $\nu(\widehat{g}_2(x)) = \nu(g_1(x))\nu(g_3(x)) = 1 + x + x^2 + x^4$. In $\mathcal{P}_{\mathbb{F}_2,7}$, the binary idempotent generator for $\langle 1 + x + x^2 + x^4 \rangle$ is
  $b_2(x) = 1 + x + x^2 + x^4$.
  $\widehat{e}_2(x) = 1 + 2x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2x^6 + x^8$.
  $\widehat{\mathbf{e}}_2(x) = 1 + 3x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2x^6$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$)

- $x^7 - 1 = g_1(x)g_2(x)g_3(x) =$
  $(-1 + x)(-1 + x + 2x^2 + x^3)(-1 - 2x - x^2 + x^3)$.
- $\widehat{g}_2(x) = g_1(x)g_3(x)$.
  $\nu(\widehat{g}_2(x)) = \nu(g_1(x))\nu(g_3(x)) = 1 + x + x^2 + x^4$. In $\mathcal{P}_{\mathbb{F}_2,7}$, the binary idempotent generator for $\langle 1 + x + x^2 + x^4 \rangle$ is
  $b_2(x) = 1 + x + x^2 + x^4$.
  $\widehat{e}_2(x) = 1 + 2x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2x^6 + x^8$.
  $\widehat{\mathbf{e}}_2(x) = 1 + 3x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2x^6$.
- $\widehat{\mathbf{e}}_1(x) = 3 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6$.
- $\widehat{\mathbf{e}}_3(x) = 1 + 2x + 2x^2 + 3x^3 + 2x^4 + 3x^5 + 3x^6$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

- $g(x) = 1 + x + 3x^2 + 2x^3 + x^4$, $h(x) = -1 + x + 2x^2 + x^3$.
- $\mathcal{C} = \langle \mathbf{f}(x)\mathbf{g}(x) \rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x) \rangle =$
  $\langle 1 + x + 3x^2 + 2x^3 + x^4 \rangle \oplus \langle 2 + 2x + 2x^3 \rangle$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

- $g(x) = 1 + x + 3x^2 + 2x^3 + x^4$, $h(x) = -1 + x + 2x^2 + x^3$.
- $\mathcal{C} = \langle \mathbf{f}(x)\mathbf{g}(x) \rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x) \rangle =$ $\langle 1 + x + 3x^2 + 2x^3 + x^4 \rangle \oplus \langle 2 + 2x + 2x^3 \rangle$.
- $\mathcal{C}$ has size $4^3 2^4$ with generator matrix:

$$\left[\begin{array}{ccccccc} 1 & 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 3 & 2 & 1 \\ \hline 2 & 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 2 \end{array}\right].$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$$\begin{aligned}
\mathcal{C} &= \langle \mathbf{g}_1(x)\mathbf{g}_3(x)\rangle \oplus \langle 2\mathbf{g}_2(x)\rangle \\
&= \langle \widehat{\mathbf{g}}_2(x)\rangle \oplus \langle 2\widehat{\mathbf{g}}_1(x)\rangle \oplus \langle 2\widehat{\mathbf{g}}_3(x)\rangle \\
&= \langle \widehat{\mathbf{e}}_2(x)\rangle \oplus \langle 2\widehat{\mathbf{e}}_1(x)\rangle \oplus \langle 2\widehat{\mathbf{e}}_3(x)\rangle \\
&= \langle \widehat{\mathbf{e}}_2(x) + 2\widehat{\mathbf{e}}_1(x) + 2\widehat{\mathbf{e}}_3(x)\rangle \\
&= \langle 1 + x + x^2 + 2x^3 + x^4 + 2x^5 + 2x^6\rangle
\end{aligned}$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}_4[x]$ with $a_d \neq 0$. Let $f^*(x) = \pm x^d (f(x^{-1})) = \pm(a_d + a_{d-1} x + \cdots + a_0 x^d)$ with $\pm$ chosen so that the leading coefficient of $f^*(x)$ is 1 or 2. $f^*(x)$ is the reciprocal polynomial of $f(x)$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Definition

Let $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbb{Z}_4[x]$ with $a_d \neq 0$. Let $f^*(x) = \pm x^d(f(x^{-1})) = \pm(a_d + a_{d-1}x + \cdots + a_0x^d)$ with $\pm$ chosen so that the leading coefficient of $f^*(x)$ is 1 or 2. $f^*(x)$ is the reciprocal polynomial of $f(x)$.

Theorem

If $\mathcal{C} = \langle \mathbf{f}(x)\mathbf{g}(x)\rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x)\rangle$ is a cyclic code of odd length n in $\mathcal{P}_{\mathbb{Z}_4,n}$ with $f(x)g(x)h(x) = x^n - 1$, then $x^n - 1 = h^*(x)g^*(x)f^*(x)$ and $\mathcal{C}^{\perp_E} = \langle \mathbf{h}^*(x)\mathbf{g}^*(x)\rangle \oplus \langle 2\mathbf{h}^*(x)\mathbf{f}^*(x)\rangle$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$)

- $g_1(x) = -1 + x \to g_1^*(x) = -1 + x$
- $g_2(x) = -1+x+2x^2+x^3 \to g_2^*(x) = -1-2x-x^2+x^3 = g_3(x)$
- $g_3(x) = -1-2x-x^2+x^3 \to g_3^*(x) = -1+x+2x^2+x^3 = g_2(x)$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$f^*(x) = 1$, $g^*(x) = g_1(x)g_2(x)$, $h^*(x) = g_3(x)$.

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$f^*(x) = 1$, $g^*(x) = g_1(x)g_2(x)$, $h^*(x) = g_3(x)$.

$$\mathcal{C} \;=\; \langle \mathbf{f}(x)\mathbf{g}(x)\rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x)\rangle = \langle \mathbf{g}_1(x)\mathbf{g}_3(x)\rangle \oplus \langle 2\mathbf{g}_2(x)\rangle$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$f^*(x) = 1$, $g^*(x) = g_1(x)g_2(x)$, $h^*(x) = g_3(x)$.

$$\begin{aligned}
\mathcal{C} &= \langle \mathbf{f}(x)\mathbf{g}(x)\rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x)\rangle = \langle \mathbf{g}_1(x)\mathbf{g}_3(x)\rangle \oplus \langle 2\mathbf{g}_2(x)\rangle \\
\mathcal{C}^{\perp_E} &= \langle \mathbf{h}^*(x)\mathbf{g}^*(x)\rangle \oplus \langle 2\mathbf{h}^*(x)\mathbf{f}^*(x)\rangle \\
&= \langle \mathbf{g}_3(x)\mathbf{g}_1(x)\mathbf{g}_2(x)\rangle \oplus \langle 2\mathbf{g}_3(x)\rangle \\
&= \langle 2\mathbf{g}_3(x)\rangle
\end{aligned}$$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$f^*(x) = 1$, $g^*(x) = g_1(x)g_2(x)$, $h^*(x) = g_3(x)$.

$$\begin{aligned}
\mathcal{C} &= \langle \mathbf{f}(x)\mathbf{g}(x)\rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x)\rangle = \langle \mathbf{g}_1(x)\mathbf{g}_3(x)\rangle \oplus \langle 2\mathbf{g}_2(x)\rangle \\
\mathcal{C}^{\perp_E} &= \langle \mathbf{h}^*(x)\mathbf{g}^*(x)\rangle \oplus \langle 2\mathbf{h}^*(x)\mathbf{f}^*(x)\rangle \\
&= \langle \mathbf{g}_3(x)\mathbf{g}_1(x)\mathbf{g}_2(x)\rangle \oplus \langle 2\mathbf{g}_3(x)\rangle \\
&= \langle 2\mathbf{g}_3(x)\rangle
\end{aligned}$$

$\mathcal{C}^{\perp_E}$ has size 2^4 with generator matrix:

$$\begin{bmatrix} 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 2 & 2 \end{bmatrix}.$$

$|\mathcal{C}| \cdot |\mathcal{C}^{\perp_E}| = 4^3 2^4 \cdot 2^4 = 4^7$

Linear Cyclic Codes over $\mathbb{Z}_4$ (cont.)

Example ($n = 7$, $f(x) = 1$, $g(x) = g_1(x)g_3(x)$, $h(x) = g_2(x)$)

$f^*(x) = 1$, $g^*(x) = g_1(x)g_2(x)$, $h^*(x) = g_3(x)$.

$$\begin{aligned}
\mathcal{C} &= \langle \mathbf{f}(x)\mathbf{g}(x)\rangle \oplus \langle 2\mathbf{f}(x)\mathbf{h}(x)\rangle = \langle \mathbf{g}_1(x)\mathbf{g}_3(x)\rangle \oplus \langle 2\mathbf{g}_2(x)\rangle \\
\mathcal{C}^{\perp_E} &= \langle \mathbf{h}^*(x)\mathbf{g}^*(x)\rangle \oplus \langle 2\mathbf{h}^*(x)\mathbf{f}^*(x)\rangle \\
&= \langle \mathbf{g}_3(x)\mathbf{g}_1(x)\mathbf{g}_2(x)\rangle \oplus \langle 2\mathbf{g}_3(x)\rangle \\
&= \langle 2\mathbf{g}_3(x)\rangle
\end{aligned}$$

$\mathcal{C}^{\perp_E}$ has size 2^4 with generator matrix:

$$\begin{bmatrix} 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 2 & 2 \end{bmatrix}.$$

$|\mathcal{C}| \cdot |\mathcal{C}^{\perp_E}| = 4^3 2^4 \cdot 2^4 = 4^7$

$$\begin{aligned}
\mathcal{C}^{\perp_E} &= \langle 2\mathbf{g}_3(x)\rangle = \langle 2\widehat{\mathbf{g}}_1(x)\rangle \oplus \langle 2\widehat{\mathbf{g}}_2(x)\rangle = \langle 2\widehat{\mathbf{e}}_1(x)\rangle \oplus \langle 2\widehat{\mathbf{e}}_2(x)\rangle \\
&= \langle 2\widehat{\mathbf{e}}_1(x) + 2\widehat{\mathbf{e}}_2(x)\rangle = \langle 2x^3 + 2x^5 + 2x^6\rangle
\end{aligned}$$

Linear Cyclic Codes over $\mathbb{Z}_{p^m}$

The results on linear cyclic codes over $\mathbb{Z}_4[x]$ were generalized to linear cyclic codes of length n over $\mathbb{Z}_{p^m}$ where $p \nmid n$ with p a prime.[16]

[16] P. Kanwar and S. R. López-Permouth, "Cyclic codes over the integers modulo p^m", *Finite Fields Appl.* **3** (1997), 334–352.

Linear Cyclic Codes over $\mathbb{Z}_{p^m}$

The results on linear cyclic codes over $\mathbb{Z}_4[x]$ were generalized to linear cyclic codes of length n over $\mathbb{Z}_{p^m}$ where $p \nmid n$ with p a prime.[16]

Theorem

Let $p \nmid n$. The following hold.

(a) $x^n - 1 = g_1(x)g_2(x)\cdots g_k(x)$ *where* $g_i(x)$ *are monic irreducible pairwise coprime polynomials in* $\mathbb{Z}_{p^m}[x]$.

(b) *Let* $\widehat{g}_i(x) = \prod_{j\neq i} g_j(x)$. *Then every ideal (i. e. linear cyclic code over* $\mathbb{Z}_{p^m}$*) of* $\mathcal{P}_{\mathbb{Z}_{p^m},n}$ *is a direct sum of* $\langle \widehat{\mathbf{g}}_i(x)\rangle$*'s,* $\langle p\widehat{\mathbf{g}}_j(x)\rangle$*'s,...,*$\langle p^{m-1}\widehat{\mathbf{g}}_\ell(x)\rangle$*'s.*

(c) *There are* $(m+1)^k$ *linear cyclic codes over* $\mathbb{Z}_{p^m}$.

(d) *For* $1 \leq i \leq k$*, there exist* $e_i(x) \in \mathbb{Z}_{p^m}[x]$ *such that* $\mathbf{e}_i(x)$ *is an idempotent in* $\mathcal{P}_{\mathbb{Z}_{p^m},n}$, $\sum_{i=1}^k \mathbf{e}_i(x) = 1$, *and* $\mathbf{e}_i(x)\mathbf{e}_j(x) = 0$.

(e) $\mathcal{P}_{\mathbb{Z}_{p^m},n}$ *is a principal ideal ring.*

---

[16] P. Kanwar and S. R. López-Permouth, "Cyclic codes over the integers modulo p^m", *Finite Fields Appl.* **3** (1997), 334–352.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) = 1$

Let r be composite with prime factorization $p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$. By the Chinese Remainder Theorem, $\mathbb{Z}_r \simeq \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_s^{m_s}}$. This can be exploited to describe linear cyclic codes over $\mathbb{Z}_r$ of length n with $\gcd(n, r) = 1$ by reducing to the case of these codes over $\mathbb{Z}_{p^m}$.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) = 1$

Let r be composite with prime factorization $p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$. By the Chinese Remainder Theorem, $\mathbb{Z}_r \simeq \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_s^{m_s}}$. This can be exploited to describe linear cyclic codes over $\mathbb{Z}_r$ of length n with $\gcd(n, r) = 1$ by reducing to the case of these codes over $\mathbb{Z}_{p^m}$.

Some References

- I. F. Blake, "Codes over certain rings", *Inform. and Control* **20** (1972), 396–404.
- I. F. Blake, "Codes over integer residue rings", *Inform. and Control* **29** (1975), 295–300.
- E. Spiegel, "Codes over $\mathbb{Z}_m$", *Inform. and Control* **35** (1977), 48–51.
- E. Spiegel, "Codes over $\mathbb{Z}_m$, revisited", *Inform. and Control* **37** (1978), 100–104.
- B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of cyclic codes over $\mathbb{Z}_m$", *Appl. Algebra Engrg. Comm. Comput.* **5** (1994), 261–275.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) \neq 1$

When $\gcd(n, r) = 1$, the roots of $x^n - 1$ in some extension ring of $\mathbb{Z}_r$ are distinct, but not when $\gcd(n, r) \neq 1$.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) \neq 1$

When $\gcd(n, r) = 1$, the roots of $x^n - 1$ in some extension ring of $\mathbb{Z}_r$ are distinct, but not when $\gcd(n, r) \neq 1$.

Some References

- T. Blackford, "Cyclic codes over $\mathbb{Z}_4$ of oddly even length", *Discrete Appl. Math.* **128** (2003), 27–46.
- T. Abualrub and R. Oehmke, "On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e", *IEEE Trans. Inform. Theory* **49** (2003), 2126–2133.
- S. T. Dougherty and S. Ling, "Cyclic codes over $\mathbb{Z}_4$ of even length", *Des. Codes Cryptogr.* **39** (2006), 127–153.
- A. Sălăgean, "Repeated-root cyclic and negacyclic codes over a finite chain ring", *Discrete Appl. Math.* **154** (2006), 413–419.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) \neq 1$ (cont.)

Theorem (Sălăgean)

Let $\mathfrak{R}$ be a finite (commutative) chain ring and p the characteristic of its residue field. If $p \mid n$, then $\mathcal{P}_{\mathfrak{R},n}$ is not a principal ideal ring.

Linear Cyclic Codes over $\mathbb{Z}_r$, $\gcd(n, r) \neq 1$ (cont.)

Theorem (Sălăgean)

Let $\mathfrak{R}$ be a finite (commutative) chain ring and p the characteristic of its residue field. If $p \mid n$, then $\mathcal{P}_{\mathfrak{R},n}$ is not a principal ideal ring.

Corollary

If n is even, $\mathcal{P}_{\mathbb{Z}_4,n}$ is not a principal ideal ring.

Linear Cyclic Codes over Noncommutative Rings

There has been a great deal of research on linear cyclic codes over many different commutative rings where topics such as generating polynomials, generating idempotents, size (type), minimum distance, dual codes, decoding, etc. are considered. That is less so for noncommutative rings.

Linear Cyclic Codes over Noncommutative Rings

There has been a great deal of research on linear cyclic codes over many different commutative rings where topics such as generating polynomials, generating idempotents, size (type), minimum distance, dual codes, decoding, etc. are considered. That is less so for noncommutative rings.

Reference

M. Greferath, "Cyclic codes over finite rings", *Discrete Math.* **177** (1997), 273–277.

Linear Cyclic Codes over Noncommutative Rings

There has been a great deal of research on linear cyclic codes over many different commutative rings where topics such as generating polynomials, generating idempotents, size (type), minimum distance, dual codes, decoding, etc. are considered. That is less so for noncommutative rings.

Reference

M. Greferath, "Cyclic codes over finite rings", *Discrete Math.* **177** (1997), 273–277.

Remark

If $\mathfrak{R}$ is a ring with unity, $x^n - 1 \in \mathfrak{R}[x]$ commutes with all polynomials in $\mathfrak{R}[x]$. Thus $(x^n - 1)\mathfrak{R}[x] = \mathfrak{R}[x](x^n - 1)$, which we still denote $\langle x^n - 1 \rangle$.

Linear Cyclic Codes over Noncommutative Rings

There has been a great deal of research on linear cyclic codes over many different commutative rings where topics such as generating polynomials, generating idempotents, size (type), minimum distance, dual codes, decoding, etc. are considered. That is less so for noncommutative rings.

Reference

M. Greferath, "Cyclic codes over finite rings", *Discrete Math.* **177** (1997), 273–277.

Remark

If $\mathfrak{R}$ is a ring with unity, $x^n - 1 \in \mathfrak{R}[x]$ commutes with all polynomials in $\mathfrak{R}[x]$. Thus $(x^n - 1)\mathfrak{R}[x] = \mathfrak{R}[x](x^n - 1)$, which we still denote $\langle x^n - 1 \rangle$.

Definition

Let $\mathfrak{R}$ be a finite (associative) ring with unity. A left-linear (right-linear) code $\mathcal{C}$ of length n over $\mathfrak{R}$ is a submodule of ${}_{\mathfrak{R}}\mathfrak{R}^n$ $(\mathfrak{R}^n{}_{\mathfrak{R}})$.

Linear Cyclic Codes over Noncommutative Rings (cont.)

Remark

In what follows, $\mathfrak{R}$ will be a finite (associative) ring with unity; there is a right analogue to results stated for left modules.

Linear Cyclic Codes over Noncommutative Rings (cont.)

Remark

In what follows, $\mathfrak{R}$ will be a finite (associative) ring with unity; there is a right analogue to results stated for left modules.

Definition

A left linear cyclic code $\mathcal{C}$ of length n over $\mathfrak{R}$ is a left ideal of $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1\rangle$. $\mathcal{C}$ is a left splitting if it is a direct summand of ${}_{\mathfrak{R}}\mathcal{P}_{\mathfrak{R},n}$.

Linear Cyclic Codes over Noncommutative Rings (cont.)

Remark

In what follows, $\mathfrak{R}$ will be a finite (associative) ring with unity; there is a right analogue to results stated for left modules.

Definition

A left linear cyclic code $\mathcal{C}$ of length n over $\mathfrak{R}$ is a left ideal of $\mathcal{P}_{\mathfrak{R},n} = \mathfrak{R}[x]/\langle x^n - 1\rangle$. $\mathcal{C}$ is a left splitting if it is a direct summand of ${}_{\mathfrak{R}}\mathcal{P}_{\mathfrak{R},n}$.

Lemma

Let $g(x)h(x) = x^n - 1$ for some $g(x), h(x) \in \mathfrak{R}[x]$. The following hold.

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

(b) ${}_{\mathfrak{R}}(\mathfrak{R}[x]g(x))$ *is a free module.*

(c) $\mathfrak{R}[x]g(x)$ *is a direct summand of* ${}_{\mathfrak{R}}\mathfrak{R}[x]$.

Linear Cyclic Codes over Noncommutative Rings (cont.)

Corollary

If $g(x)$ is a factor of $x^n - 1$ in $\mathfrak{R}[x]$, then ${}_{\mathfrak{R}}(\mathcal{P}_{\mathfrak{R},n}g(x))$ is a left-linear cyclic code and a left splitting of ${}_{\mathfrak{R}}\mathcal{P}_{\mathfrak{R},n}$.

Linear Cyclic Codes over Noncommutative Rings (cont.)

Corollary

If $g(x)$ is a factor of $x^n - 1$ in $\mathfrak{R}[x]$, then ${}_{\mathfrak{R}}(\mathcal{P}_{\mathfrak{R},n}g(x))$ is a left-linear cyclic code and a left splitting of ${}_{\mathfrak{R}}\mathcal{P}_{\mathfrak{R},n}$.

Theorem

For a left linear cyclic code $\mathcal{C}$ of length n over $\mathfrak{R}$, the following are equivalent:

(a) *$\mathcal{C}$ is a left splitting code.*

(b) *There exists a divisor $g(x)$ of $x^n - 1$ in $\mathfrak{R}[x]$ such that $\mathcal{C} = {}_{\mathfrak{R}}(\mathcal{P}_{\mathfrak{R},n}g(x))$.*

Linear Cyclic Codes over Noncommutative Rings (cont.)

Corollary

If $g(x)$ is a factor of $x^n - 1$ in $\mathfrak{R}[x]$, then ${}_{\mathfrak{R}}(\mathcal{P}_{\mathfrak{R},n}g(x))$ is a left-linear cyclic code and a left splitting of ${}_{\mathfrak{R}}\mathcal{P}_{\mathfrak{R},n}$.

Theorem

For a left linear cyclic code $\mathcal{C}$ of length n over $\mathfrak{R}$, the following are equivalent:

(a) *$\mathcal{C}$ is a left splitting code.*

(b) *There exists a divisor $g(x)$ of $x^n - 1$ in $\mathfrak{R}[x]$ such that $\mathcal{C} = {}_{\mathfrak{R}}(\mathcal{P}_{\mathfrak{R},n}g(x))$.*

Remark

There are left linear cyclic codes that are not a left splitting.

Generalizations of Cyclic Codes

Definition

If $\mathfrak{R}$ is a commutative ring and $\lambda \in \mathfrak{R}$, $\mathcal{C} \subseteq \mathfrak{R}^n$ is λ-constacyclic or λ-twisted if whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then

$$(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

If $\lambda = -1$, $\mathcal{C}$ is negacyclic.

Generalizations of Cyclic Codes

Definition

If $\mathfrak{R}$ is a commutative ring and $\lambda \in \mathfrak{R}$, $\mathcal{C} \subseteq \mathfrak{R}^n$ is λ-constacyclic or λ-twisted if whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then

$$(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

If $\lambda = -1$, $\mathcal{C}$ is negacyclic.

Remark

Linear λ-constacyclic codes of length n can be viewed as ideals of $\mathfrak{R}[x]/\langle x^n - \lambda \rangle$.

Generalizations of Cyclic Codes

Definition

If $\mathfrak{R}$ is a commutative ring and $\lambda \in \mathfrak{R}$, $\mathcal{C} \subseteq \mathfrak{R}^n$ is λ-constacyclic or λ-twisted if whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then

$$(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

If $\lambda = -1$, $\mathcal{C}$ is negacyclic.

Remark

Linear λ-constacyclic codes of length n can be viewed as ideals of $\mathfrak{R}[x]/\langle x^n - \lambda \rangle$.

Definition

Let $\mathcal{C} \subseteq \mathfrak{R}^n$ and ℓ a positive integer with $\ell \mid n$. $\mathcal{C}$ is ℓ-quasi-cyclic if whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ then

$$(c_{n-\ell}, c_{n-\ell+1}, \ldots, c_{n-1}, c_0, \ldots, c_{n-\ell-2} c_{n-\ell-1}) \in \mathcal{C}.$$

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?
- Is there anything like BCH codes?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?
- Is there anything like BCH codes?
- Is there an ‘easy’ way to decide equivalence?

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?
- Is there anything like BCH codes?
- Is there an 'easy' way to decide equivalence?
- Classification.

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?
- Is there anything like BCH codes?
- Is there an 'easy' way to decide equivalence?
- Classification.
- Encoding and decoding.

Considerations for Cyclic Codes over Rings

Suggestions

- Define cyclic codes.
- What is the setting to study these codes?
- How do you generate the cyclic codes?
- Is there anything like defining sets?
- Can you get dual codes easily?
- Are there bounds on the minimum distance?
- Is there anything like BCH codes?
- Is there an 'easy' way to decide equivalence?
- Classification.
- Encoding and decoding.
- What light do your cyclic codes shed on old cyclic codes?