

Quasi-Cyclic Codes over Rings

San Ling

School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore

lingsan@ntu.edu.sg

Contents

Rings

Quasi-Cyclic Codes over Rings

Codes over Rings

Quasi-Cyclic Codes

The Ring $R(A, m)$

Fourier Transform & Trace Formula

Applications

1-Generator Codes

Alternative Descriptions of Quasi-Cyclic Codes

1-Generator Quasi-Cyclic Codes

Rings

A : commutative ring with identity 1

A **local**: if it has a unique maximal ideal M .

$k := A/M$ is a field.

Rings

A : commutative ring with identity 1

A **local**: if it has a unique maximal ideal M .

$k := A/M$ is a field.

Hensel lifting: Factorizations fg of elements h of $k[X]$ can be “lifted” to factorizations FG of H in $A[X]$ in such a way that f, g, h correspond to F, G, H respectively under reduction modulo M .

Chain Rings

Chain ring: both local and principal.

A local ring is a chain ring



maximal ideal has a single generator t , say: $M = (t)$.

Chain Rings

Chain ring: both local and principal.

A local ring is a chain ring



maximal ideal has a single generator t , say: $M = (t)$.

$$A \supset (t) \supset (t^2) \supset \cdots \supset (t^{d-1}) \supset (t^d) = (0).$$

d : **depth** of A .

If k has q elements, then $A/(t^i)$ has q^i elements, so A has q^d elements.

Chain Rings

Example

1. Finite fields \mathbb{F}_q
2. Integer rings \mathbb{Z}_{p^r}
3. Galois rings $GR(p^r, m)$
4. $\mathbb{F}_q[u]/(u^k)$

Codes over Rings

Linear code C of length n over A : an A -submodule of A^n , i.e.,

- ▶ $x, y \in C \Rightarrow x + y \in C$;
- ▶ $\forall \lambda \in A, x \in C \Rightarrow \lambda x \in C$,

Codes over Rings

Linear code C of length n over A : an A -submodule of A^n , i.e.,

- ▶ $x, y \in C \Rightarrow x + y \in C$;
- ▶ $\forall \lambda \in A, x \in C \Rightarrow \lambda x \in C$,

T : standard shift operator on A^n

$$T(a_0, a_1, \dots, a_{n-1}) = (a_{n-1}, a_0, \dots, a_{n-2}).$$

C **quasi-cyclic** of index ℓ or ℓ -quasi-cyclic: invariant under T^ℓ .

Assume: ℓ divides n

$m := n/\ell$: co-index.

Codes over Rings

Example

- ▶ If $\ell = 2$ and first circulant block is identity matrix, code equivalent to a so-called pure **double circulant** code.
- ▶ Up to equivalence, generator matrix of such a code consists of $m \times m$ circulant matrices.

Quasi-Cyclic Codes

m : positive integer.

$$R := R(A, m) = A[Y]/(Y^m - 1).$$

C : quasi-cyclic code over A of length lm and index l .

$$\mathbf{c} = (c_{00}, c_{01}, \dots, c_{0,l-1}, c_{10}, \dots, c_{1,l-1}, \dots, c_{m-1,0}, \dots, c_{m-1,l-1}) \in C$$

Quasi-Cyclic Codes

m : positive integer.

$$R := R(A, m) = A[Y]/(Y^m - 1).$$

C : quasi-cyclic code over A of length ℓm and index ℓ .

$$\mathbf{c} = (c_{00}, c_{01}, \dots, c_{0,\ell-1}, c_{10}, \dots, c_{1,\ell-1}, \dots, c_{m-1,0}, \dots, c_{m-1,\ell-1}) \in C$$

Define $\phi : A^{\ell m} \rightarrow R^\ell$ by

$$\phi(\mathbf{c}) = (\mathbf{c}_0(Y), \mathbf{c}_1(Y), \dots, \mathbf{c}_{\ell-1}(Y)) \in R^\ell,$$

$$\text{where } \mathbf{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in R.$$

$\phi(C)$: image of C under ϕ .

Quasi-Cyclic Codes

Lemma

ϕ induces one-to-one correspondence

quasi-cyclic codes over A of index ℓ and length ℓm



linear codes over R of length ℓ

Proof

C linear $\Rightarrow \phi(C)$ closed under scalar multiplication by elements of A .

Since $Y^m = 1$ in R ,

$$Yc_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^{i+1} = \sum_{i=0}^{m-1} c_{i-1,j} Y^i,$$

subscripts taken modulo m .

Proof continued

$$(Yc_0(Y), Yc_1(Y), \dots, Yc_{\ell-1}(Y)) \in R^\ell$$

corresponds to

$$(c_{m-1,0}, c_{m-1,1}, \dots, c_{m-1,\ell-1}, c_{00}, c_{01}, \dots, c_{0,\ell-1}, \dots, c_{m-2,0}, \dots, c_{m-2,\ell-1}) \in A^{\ell m},$$

which is in C since C is quasi-cyclic of index ℓ .

Therefore, $\phi(C)$ closed under multiplication by Y .

Hence $\phi(C)$ is R -submodule of R^ℓ .

Proof continued

$$(Yc_0(Y), Yc_1(Y), \dots, Yc_{l-1}(Y)) \in R^\ell$$

corresponds to

$$(c_{m-1,0}, c_{m-1,1}, \dots, c_{m-1,l-1}, c_{00}, c_{01}, \dots, c_{0,l-1}, \dots, c_{m-2,0}, \dots, c_{m-2,l-1}) \in A^{\ell m},$$

which is in C since C is quasi-cyclic of index l .

Therefore, $\phi(C)$ closed under multiplication by Y .

Hence $\phi(C)$ is R -submodule of R^ℓ .

For converse, reverse above argument.

Quasi-Cyclic Codes

Euclidean inner product on $A^{\ell m}$: for

$$\mathbf{a} = (a_{00}, a_{01}, \dots, a_{0,\ell-1}, a_{10}, \dots, a_{1,\ell-1}, \dots, a_{m-1,0}, \dots, a_{m-1,\ell-1})$$

and

$$\mathbf{b} = (b_{00}, b_{01}, \dots, b_{0,\ell-1}, b_{10}, \dots, b_{1,\ell-1}, \dots, b_{m-1,0}, \dots, b_{m-1,\ell-1}),$$

define

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} a_{ij} b_{ij}.$$

Quasi-Cyclic Codes

Conjugation map $\bar{}$ on R : identity on the elements of A and sends Y to $Y^{-1} = Y^{m-1}$, and extended linearly.

Quasi-Cyclic Codes

Conjugation map $\bar{}$ on R : identity on the elements of A and sends Y to $Y^{-1} = Y^{m-1}$, and extended linearly.

Hermitian inner product on R^ℓ : for

$$\mathbf{x} = (x_0, \dots, x_{\ell-1}) \text{ and } \mathbf{y} = (y_0, \dots, y_{\ell-1}),$$

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=0}^{\ell-1} x_j \bar{y}_j.$$

Quasi-Cyclic Codes

Proposition

$\mathbf{a}, \mathbf{b} \in A^{\ell m}$. Then

$$(T^{\ell k}(\mathbf{a})) \cdot \mathbf{b} = 0 \text{ for all } 0 \leq k \leq m - 1$$

$$\begin{array}{c} \Updownarrow \\ \langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0. \end{array}$$

Proof

Condition $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$ equivalent to

$$0 = \sum_{j=0}^{\ell-1} a_j \overline{b_j} = \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{m-1} a_{ij} Y^i \right) \left(\sum_{k=0}^{m-1} b_{kj} Y^{-k} \right). \quad (1)$$

Proof

Condition $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$ equivalent to

$$0 = \sum_{j=0}^{\ell-1} a_j \bar{b}_j = \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{m-1} a_{ij} Y^i \right) \left(\sum_{k=0}^{m-1} b_{kj} Y^{-k} \right). \quad (1)$$

Comparing coefficients of Y^h , (1) equivalent to

$$\sum_{j=0}^{\ell-1} \sum_{i=0}^{m-1} a_{i+h,j} b_{ij} = 0, \quad \text{for all } 0 \leq h \leq m-1, \quad (2)$$

subscripts taken modulo m .

Proof

Condition $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$ equivalent to

$$0 = \sum_{j=0}^{\ell-1} a_j \bar{b}_j = \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{m-1} a_{ij} Y^i \right) \left(\sum_{k=0}^{m-1} b_{kj} Y^{-k} \right). \quad (1)$$

Comparing coefficients of Y^h , (1) equivalent to

$$\sum_{j=0}^{\ell-1} \sum_{i=0}^{m-1} a_{i+hj} b_{ij} = 0, \quad \text{for all } 0 \leq h \leq m-1, \quad (2)$$

subscripts taken modulo m .

(2) means $(T^{-\ell h}(\mathbf{a})) \cdot \mathbf{b} = 0$.

Proof

Since $T^{-\ell h} = T^{\ell(m-h)}$, it follows that (2), and hence $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$, is equivalent to $(T^{\ell k}(\mathbf{a})) \cdot \mathbf{b} = 0$ for all $0 \leq k \leq m-1$.

Quasi-Cyclic Codes

Corollary

C : quasi-cyclic code over A of length ℓm and of index ℓ

$\phi(C)$: its image in R^ℓ under ϕ .

Then $\phi(C)^\perp = \phi(C^\perp)$,

where dual in $A^{\ell m}$ is wrt Euclidean inner product,

while dual in R^ℓ is wrt Hermitian inner product.

In particular,

C over A self-dual wrt Euclidean inner product



$\phi(C)$ over R self-dual wrt Hermitian inner product.

The Ring $R(A, m)$

When $m > 1$,

$R(A, m) = A[Y]/(Y^m - 1)$ is **never** a local ring.

But always decomposes into **product of local rings**.

The Ring $R(A, m)$

When $m > 1$,

$R(A, m) = A[Y]/(Y^m - 1)$ is **never** a local ring.

But always decomposes into **product of local rings**.

Characteristic of A : p^n (p prime).

Write $m = p^a m'$, where $(m', p) = 1$.

$Y^{m'} - 1$ factors into distinct irreducible factors in $k[Y]$.

The Ring $R(A, m)$

When $m > 1$,

$R(A, m) = A[Y]/(Y^m - 1)$ is **never** a local ring.

But always decomposes into **product of local rings**.

Characteristic of A : p^n (p prime).

Write $m = p^a m'$, where $(m', p) = 1$.

$Y^{m'} - 1$ factors into distinct irreducible factors in $k[Y]$.

By Hensel lifting, may write

$$Y^{m'} - 1 = f_1 f_2 \cdots f_r \in A[Y],$$

f_j : distinct basic irreducible polynomials.

The Ring $R(A, m)$

Product unique:

if $Y^{m'} - 1 = f'_1 f'_2 \cdots f'_s$ is another decomposition into basic irreducible polynomials,

then $r = s$ and,

after suitable renumbering of the f'_j 's, f_j is associate of f'_j , for each $1 \leq j \leq r$.

The Ring $R(A, m)$

f : polynomial

f^* : its reciprocal polynomial

Note: $(f^*)^* = f$.

The Ring $R(A, m)$

f : polynomial

f^* : its reciprocal polynomial

Note: $(f^*)^* = f$.

$$Y^{m'} - 1 = -f_1^* f_2^* \cdots f_r^*.$$

f basic irreducible \Rightarrow so is f^* .

By uniqueness of decomposition

$$Y^{m'} - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*,$$

δ : unit in A ,

g_1, \dots, g_s : those f_j 's associate to their own reciprocals,

$h_1, h_1^*, \dots, h_t, h_t^*$: remaining f_j 's grouped in pairs.

The Ring $R(A, m)$

Suppose further:

if characteristic of A is p^n ($n > 1$), then $a = 0$,
i.e., $m = m'$ relatively prime to p .

When characteristic of A is p (e.g., finite field), m need not be relatively prime to p .

The Ring $R(A, m)$

Suppose further:

if characteristic of A is p^n ($n > 1$), then $a = 0$,
 i.e., $m = m'$ relatively prime to p .

When characteristic of A is p (e.g., finite field), m need not be
 relatively prime to p .

Then

$$\begin{aligned} Y^m - 1 &= Y^{p^a m'} - 1 = (Y^{m'} - 1)^{p^a} \\ &= \delta^{p^a} g_1^{p^a} \cdots g_s^{p^a} h_1^{p^a} (h_1^*)^{p^a} \cdots h_t^{p^a} (h_t^*)^{p^a} \in A[Y]. \end{aligned}$$

The Ring $R(A, m)$

Consequently,

$$R = \frac{A[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^s \frac{A[Y]}{(g_i)^{\rho^a}} \right) \oplus \left(\bigoplus_{j=1}^t \left(\frac{A[Y]}{(h_j)^{\rho^a}} \oplus \frac{A[Y]}{(h_j^*)^{\rho^a}} \right) \right), \quad (3)$$

(with coordinatewise addition and multiplication).

The Ring $R(A, m)$

Consequently,

$$R = \frac{A[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^s \frac{A[Y]}{(g_i)^{p^a}} \right) \oplus \left(\bigoplus_{j=1}^t \left(\frac{A[Y]}{(h_j)^{p^a}} \oplus \frac{A[Y]}{(h_j^*)^{p^a}} \right) \right), \quad (3)$$

(with coordinatewise addition and multiplication).

$$G_i := A[Y]/(g_i)^{p^a}, \quad H'_j := A[Y]/(h_j)^{p^a}, \quad H''_j := A[Y]/(h_j^*)^{p^a}$$

$$R^\ell = \left(\bigoplus_{i=1}^s G_i^\ell \right) \oplus \left(\bigoplus_{j=1}^t \left(H'_j{}^\ell \oplus H''_j{}^\ell \right) \right).$$

The Ring $R(A, m)$

Every R -linear code C of length ℓ can be decomposed as

$$C = \left(\bigoplus_{i=1}^s C_i \right) \oplus \left(\bigoplus_{j=1}^t (C'_j \oplus C''_j) \right),$$

C_i : linear code over G_i of length ℓ ,

C'_j : linear code over H'_j of length ℓ and

C''_j : linear code over H''_j of length ℓ .

The Ring $R(A, m)$

Every element of R may be written as $\mathbf{c}(Y)$ for some polynomial $\mathbf{c} \in A[Y]$.

$$R = \left(\bigoplus_{i=1}^s G_i \right) \oplus \left(\bigoplus_{j=1}^t (H'_j \oplus H''_j) \right).$$

Hence,

$$\mathbf{c}(Y) = (c_1(Y), \dots, c_s(Y), c'_1(Y), c''_1(Y), \dots, c'_t(Y), c''_t(Y)), \quad (4)$$

$$c_i(Y) \in G_i \quad (1 \leq i \leq s), \quad c'_j(Y) \in H'_j \quad \text{and} \quad c''_j(Y) \in H''_j \quad (1 \leq j \leq t).$$

The Ring $R(A, m)$

Recall “conjugate” map $Y \mapsto Y^{-1}$ in R .

For $f \in A[Y]$ dividing $Y^m - 1$, have isomorphism

$$\begin{aligned} \frac{A[Y]}{(f)} &\longrightarrow \frac{A[Y]}{(f^*)} \\ c(Y) + (f) &\longmapsto c(Y^{-1}) + (f^*). \end{aligned} \tag{5}$$

(Note: $Y^{-1} = Y^{m-1}$.)

The Ring $R(A, m)$

Recall “conjugate” map $Y \mapsto Y^{-1}$ in R .

For $f \in A[Y]$ dividing $Y^m - 1$, have isomorphism

$$\begin{aligned} \frac{A[Y]}{(f)} &\longrightarrow \frac{A[Y]}{(f^*)} \\ c(Y) + (f) &\longmapsto c(Y^{-1}) + (f^*). \end{aligned} \tag{5}$$

(Note: $Y^{-1} = Y^{m-1}$.)

When f and f^* are associates,

map $Y \mapsto Y^{-1}$ induces automorphism of $A[Y]/(f)$.

For $r \in A[Y]/(f)$, \bar{r} : image under this map.

When $\deg(f) = 1$, induced map is identity, so $\bar{r} = r$.

The Ring $R(A, m)$

Let

$$\mathbf{r} = (r_1, \dots, r_s, r'_1, r''_1, \dots, r'_t, r''_t),$$

where $r_i \in G_i$ ($1 \leq i \leq s$), $r'_j \in H'_j$ and $r''_j \in H''_j$ ($1 \leq j \leq t$).

Then

$$\bar{\mathbf{r}} = (\bar{r}_1, \dots, \bar{r}_s, r'_1, r''_1, \dots, r'_t, r''_t).$$

The Ring $R(A, m)$

Let

$$\mathbf{r} = (r_1, \dots, r_s, r'_1, r''_1, \dots, r'_t, r''_t),$$

where $r_i \in G_i$ ($1 \leq i \leq s$), $r'_j \in H'_j$ and $r''_j \in H''_j$ ($1 \leq j \leq t$).

Then

$$\bar{\mathbf{r}} = (\bar{r}_1, \dots, \bar{r}_s, r''_1, r'_1, \dots, r''_t, r'_t).$$

When f and f^* are associates,

for $\mathbf{c} = (c_1, \dots, c_\ell)$, $\mathbf{c}' = (c'_1, \dots, c'_\ell) \in (A[Y]/(f))^\ell$,
 define **Hermitian inner product** on $(A[Y]/(f))^\ell$ as

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^{\ell} c_i \bar{c}'_i. \quad (6)$$

The Ring $R(A, m)$

Remark

*When $\deg(f) = 1$, since $r \mapsto \bar{r}$ is identity,
Hermitian inner product (6) is usual Euclidean inner product \cdot on
 A .*

The Ring $R(A, m)$

Proposition

$\mathbf{a} = (\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{\ell-1}) \in R^\ell$ and $\mathbf{b} = (\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{\ell-1}) \in R^\ell$.

$$\begin{aligned}\mathbf{a}_i &= (a_{i1}, \dots, a_{is}, a'_{i1}, a''_{i1}, \dots, a'_{it}, a''_{it}) \\ \mathbf{b}_i &= (b_{i1}, \dots, b_{is}, b'_{i1}, b''_{i1}, \dots, b'_{it}, b''_{it}),\end{aligned}$$

$a_{ij}, b_{ij} \in G_j$, $a'_{ij}, b'_{ij}, a''_{ij}, b''_{ij} \in H'_j$ (with H'_j, H''_j identified). Then

$$\begin{aligned}\langle \mathbf{a}, \mathbf{b} \rangle &= \sum_{i=0}^{\ell-1} \mathbf{a}_i \overline{\mathbf{b}_i} \\ &= \left(\sum_i a_{i1} \overline{b_{i1}}, \dots, \sum_i a_{is} \overline{b_{is}}, \sum_i a'_{i1} \overline{b''_{i1}}, \sum_i a''_{i1} \overline{b'_{i1}}, \dots, \sum_i a'_{it} \overline{b''_{it}}, \sum_i a''_{it} \overline{b'_{it}} \right).\end{aligned}$$

In particular, $\langle \mathbf{a}, \mathbf{b} \rangle = 0 \Leftrightarrow \sum_i a_{ij} \overline{b_{ij}} = 0$ ($1 \leq j \leq s$) and $\sum_i a'_{ik} \overline{b''_{ik}} = 0 = \sum_i a''_{ik} \overline{b'_{ik}}$ ($1 \leq k \leq t$).

The Ring $R(A, m)$

Theorem

Linear code C over $R = A[Y]/(Y^m - 1)$ of length ℓ is self-dual wrt Hermitian inner product if and only if

$$C = \left(\bigoplus_{i=1}^s C_i \right) \oplus \left(\bigoplus_{j=1}^t (C'_j \oplus (C'_j)^\perp) \right),$$

C_i : self-dual code over G_i of length ℓ (wrt Hermitian inner product)

C'_j : linear code of length ℓ over H'_j

$C'_j{}^\perp$: dual wrt Euclidean inner product.

Finite Chain Rings

Assume: m and characteristic of A relatively prime
 m is a unit in A

Finite Chain Rings

Assume: m and characteristic of A relatively prime

m is a unit in A

A : finite chain ring with maximal ideal (t)

Residue field $k = A/(t) = \mathbb{F}_q$.

Every element x of A can be expressed uniquely as

$$x = x_0 + x_1 t + \cdots + x_{d-1} t^{d-1},$$

where x_0, \dots, x_{d-1} belong to Teichmüller set.

Galois Extensions

g_i, h_j, h_j^* – monic basic irreducible polynomials

G_i, H_j' and H_j'' are Galois extensions of A .

- ▶ Galois extensions of local ring are unramified
- ▶ Unique maximal ideal in such a Galois extension of A again generated by t .

Frobenius & Trace

For B/A Galois extension,

Frobenius map $F : B \rightarrow B$ – map induced by $Y \mapsto Y^q$, acting as identity on A .

e : **degree** of extension B over A

Then F^e is identity.

Frobenius & Trace

For B/A Galois extension,

Frobenius map $F : B \rightarrow B$ – map induced by $Y \mapsto Y^q$, acting as identity on A .

e : **degree** of extension B over A

Then F^e is identity.

$x \in B$, **trace**

$$\text{Tr}_{B/A}(x) = x + F(x) + \cdots + F^{e-1}(x).$$

Fourier Transform

In (3),

$$R = \frac{A[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^s \frac{A[Y]}{(g_i)^{p^a}} \right) \oplus \left(\bigoplus_{j=1}^t \left(\frac{A[Y]}{(h_j)^{p^a}} \oplus \frac{A[Y]}{(h_j^*)^{p^a}} \right) \right).$$

Direct factors on RHS correspond to irreducible factors of $Y^m - 1$ in $A[Y]$ (assumed $a = 0$).

Fourier Transform

In (3),

$$R = \frac{A[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^s \frac{A[Y]}{(g_i)^{\rho^a}} \right) \oplus \left(\bigoplus_{j=1}^t \left(\frac{A[Y]}{(h_j)^{\rho^a}} \oplus \frac{A[Y]}{(h_j^*)^{\rho^a}} \right) \right).$$

Direct factors on RHS correspond to irreducible factors of $Y^m - 1$ in $A[Y]$ (assumed $a = 0$).

There is one-to-one correspondence between these factors and the **q -cyclotomic cosets** of $\mathbb{Z}/m\mathbb{Z}$.

U_i ($1 \leq i \leq s$): cyclotomic coset corresponding to g_i ,

V_j and W_j ($1 \leq j \leq t$): cyclotomic cosets corresponding to h_j and h_j^* , respectively.

Fourier Transform

For $\mathbf{c} = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$,

its **Fourier Transform**: $\hat{\mathbf{c}} = \sum_{h \in \mathbb{Z}/m\mathbb{Z}} \hat{c}_h Y^h$, where

$$\hat{c}_h = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g \zeta^{gh} = \mathbf{c}(\zeta^h),$$

ζ : primitive m th root of 1 in some (sufficiently large) Galois extension of A .

Fourier Transform

For $\mathbf{c} = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$,

its **Fourier Transform**: $\hat{\mathbf{c}} = \sum_{h \in \mathbb{Z}/m\mathbb{Z}} \hat{c}_h Y^h$, where

$$\hat{c}_h = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g \zeta^{gh} = \mathbf{c}(\zeta^h),$$

ζ : primitive m th root of 1 in some (sufficiently large) Galois extension of A .

The Fourier Transform gives rise to isomorphism (3).

Fourier Transform

For $\mathbf{c} = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$,

its **Fourier Transform**: $\hat{\mathbf{c}} = \sum_{h \in \mathbb{Z}/m\mathbb{Z}} \hat{c}_h Y^h$, where

$$\hat{c}_h = \sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g \zeta^{gh} = \mathbf{c}(\zeta^h),$$

ζ : primitive m th root of 1 in some (sufficiently large) Galois extension of A .

The Fourier Transform gives rise to isomorphism (3).

Inverse transform:

$$c_g = m^{-1} \sum_{h \in \mathbb{Z}/m\mathbb{Z}} \hat{c}_h \zeta^{-gh} = m^{-1} \hat{\mathbf{c}}(\zeta^{-g}).$$

Fourier Transform

Well known:

- ▶ $\hat{c}_{qh} = F(\hat{c}_h)$
- ▶ for $h \in U_i$, $\hat{c}_h \in G_i$, while for $h \in V_j$ (resp. W_j), $\hat{c}_h \in H'_j$ (resp. H''_j).

Fourier Transform

Well known:

- ▶ $\hat{c}_{qh} = F(\hat{c}_h)$
- ▶ for $h \in U_i$, $\hat{c}_h \in G_i$, while for $h \in V_j$ (resp. W_j), $\hat{c}_h \in H'_j$ (resp. H''_j).

Backward direction of (3):

G_i , H'_j and H''_j : Galois extensions of A corresponding to g_i , h_j and h_j^* , with corresponding cyclotomic cosets U_i , V_j and W_j .

For each i , fix some $u_i \in U_i$.

For each j , fix some $v_j \in V_j$ and $w_j \in W_j$.

Fourier Transform & Trace Formula

Let $\hat{c}_i \in G_i$, $\hat{c}'_j \in H'_j$ and $\hat{c}''_j \in H''_j$.

To $(\hat{c}_1, \dots, \hat{c}_s, \hat{c}'_1, \hat{c}''_1, \dots, \hat{c}'_t, \hat{c}''_t)$,

associate $\sum_{g \in \mathbb{Z}/m\mathbb{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$, where

$$mc_g = \sum_{i=1}^s \text{Tr}_{G_i/A}(\hat{c}_i \zeta^{-gu_i}) + \sum_{j=1}^t (\text{Tr}_{H'_j/A}(\hat{c}'_j \zeta^{-gv_j}) + \text{Tr}_{H''_j/A}(\hat{c}''_j \zeta^{-gw_j})),$$

$\text{Tr}_{B/A}$: trace from B to A .

Fourier Transform of vector \mathbf{x} : vector whose i th entry is Fourier Transform of i th entry of \mathbf{x} .

Trace of \mathbf{x} : vector whose coordinates are traces of coordinates of \mathbf{x} .

Trace Formula

Theorem

m relatively prime to characteristic of A .

Quasi-cyclic codes over A of length ℓm and of index ℓ given by following construction:

Write $Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$, (δ, g_i, h_j, h_j^* as earlier).

$A[Y]/(g_i) = G_i$, $A[Y]/(h_j) = H'_j$ and $A[Y]/(h_j^*) = H''_j$.

U_i, V_j, W_j : corresponding q -cyclotomic coset of $\mathbb{Z}/m\mathbb{Z}$.

$u_i \in U_i, v_j \in V_j$ and $w_j \in W_j$.

C_i, C'_j, C''_j : codes of length ℓ over G_i, H'_j, H''_j , resp.

Trace Formula

Theorem

For $\mathbf{x}_i \in C_i$, $\mathbf{y}'_j \in C'_j$, $\mathbf{y}''_j \in C''_j$, and $0 \leq g \leq m - 1$:

$$\mathbf{c}_g = \sum_{i=1}^s \text{Tr}_{G_i/A}(\mathbf{x}_i \zeta^{-gu_i}) + \sum_{j=1}^t (\text{Tr}_{H'_j/A}(\mathbf{y}'_j \zeta^{-gv_j}) + \text{Tr}_{H''_j/A}(\mathbf{y}''_j \zeta^{-gw_j})).$$

Then $C = \{(\mathbf{c}_0, \dots, \mathbf{c}_{m-1}) \mid \mathbf{x}_i \in C_i, \mathbf{y}'_j \in C'_j \text{ and } \mathbf{y}''_j \in C''_j\}$ is quasi-cyclic code over A of length ℓm and of index ℓ .

Converse also true.

Moreover, C self-dual $\Leftrightarrow C_i$ self-dual wrt Hermitian inner product and $C''_j = (C'_j)^\perp$ for each j wrt Euclidean inner product.

Quasi-Cyclic Codes of Index 2

$$\ell = 2$$

Theorem

m: any positive integer.

Self-dual 2-quasi-cyclic codes over \mathbb{F}_q of length $2m$ exist \Leftrightarrow exactly one of following satisfied:

- 1. q is a power of 2;*
- 2. $q = p^b$ (p prime $\equiv 1 \pmod{4}$); or*
- 3. $q = p^{2b}$ (p prime $\equiv 3 \pmod{4}$).*

Proof

Case I: m relatively prime to q

Proof

Case I: m relatively prime to q

Self-dual codes (wrt Euclidean inner product) of length 2 over \mathbb{F}_q exist if and only -1 is a square in \mathbb{F}_q – true when one of following holds:

1. q is a power of 2;
2. $q = p^b$ (p prime $\equiv 1 \pmod{4}$; or
3. $q = p^{2b}$ (p prime $\equiv 3 \pmod{4}$).

Proof

Case I: m relatively prime to q

Self-dual codes (wrt Euclidean inner product) of length 2 over \mathbb{F}_q exist if and only -1 is a square in \mathbb{F}_q – true when one of following holds:

1. q is a power of 2;
2. $q = p^b$ (p prime $\equiv 1 \pmod{4}$; or
3. $q = p^{2b}$ (p prime $\equiv 3 \pmod{4}$).

If self-dual 2-quasi-cyclic code over \mathbb{F}_q of length $2m$ exists, then by (3) there is self-dual code of length 2 over $G_1 = \mathbb{F}_q$. Hence conditions in Proposition are necessary.

Proof

Conversely, if any condition in Proposition satisfied,
then there exists $i \in \mathbb{F}_q$ such that $i^2 + 1 = 0$.

Proof

Conversely, if any condition in Proposition satisfied,
then there exists $i \in \mathbb{F}_q$ such that $i^2 + 1 = 0$.

Hence every finite extension of \mathbb{F}_q also contains such an i .

Proof

Conversely, if any condition in Proposition satisfied, then there exists $i \in \mathbb{F}_q$ such that $i^2 + 1 = 0$.

Hence every finite extension of \mathbb{F}_q also contains such an i .

Code generated by $(1, i)$ over any extension of \mathbb{F}_q is self-dual (wrt Euclidean and Hermitian inner products) of length 2.

Hence existence of self-dual 2-quasi-cyclic code of length $2m$ over \mathbb{F}_q .

Proof

Case II: m not relatively prime to q

Proof

Case II: m not relatively prime to q

$q = p^b$ and $m = p^a m'$, where $a > 0$.

By (3), G_i are finite chain rings of depth p^a .

Proof

Case II: m not relatively prime to q

$q = p^b$ and $m = p^a m'$, where $a > 0$.

By (3), G_i are finite chain rings of depth p^a .

Self-dual 2-quasi-cyclic code over \mathbb{F}_q of length $2m$ exists \Leftrightarrow for each i , there exists self-dual linear code of length 2 over G_i .

Proof

Case II: m not relatively prime to q

$q = p^b$ and $m = p^a m'$, where $a > 0$.

By (3), G_i are finite chain rings of depth p^a .

Self-dual 2-quasi-cyclic code over \mathbb{F}_q of length $2m$ exists \Leftrightarrow for each i , there exists self-dual linear code of length 2 over G_i .

Simplify notation

G : finite chain ring of depth $d = p^a$, with maximal ideal (t) and residue field \mathbb{F}_{q^e} .

(So G has q^{de} elements.)

Proof

Sufficiency:

If any condition in Theorem satisfied, then $X^2 + 1 = 0$ has solution in $G/(t) = \mathbb{F}_{q^e}$.

Proof

Sufficiency:

If any condition in Theorem satisfied, then $X^2 + 1 = 0$ has solution in $G/(t) = \mathbb{F}_{q^e}$.

Such a solution lifts to one in $G/(t^c)$, for any $1 \leq c \leq d$.

Proof

Sufficiency:

If any condition in Theorem satisfied, then $X^2 + 1 = 0$ has solution in $G/(t) = \mathbb{F}_{q^e}$.

Such a solution lifts to one in $G/(t^c)$, for any $1 \leq c \leq d$.

Hence, there exists $i \in G$ such that $i^2 + 1 = 0$.

Proof

Sufficiency:

If any condition in Theorem satisfied, then $X^2 + 1 = 0$ has solution in $G/(t) = \mathbb{F}_{q^e}$.

Such a solution lifts to one in $G/(t^c)$, for any $1 \leq c \leq d$.

Hence, there exists $i \in G$ such that $i^2 + 1 = 0$.

Clear: free code with generator matrix $(1, i)$ self-dual of length 2.

Proof

Necessity:

Assume q odd (case q even trivially true)

Proof

Necessity:

Assume q odd (case q even trivially true)

Let $G = G_1$ corresponding to $Y - 1$ in (3).

Depth d odd.

In fact, $G = \mathbb{F}_q[t]/(t)^{p^a}$ and $Y \mapsto Y^{-1}$ induces identity on G .
(Hermitian and Euclidean inner products coincide.)

Proof

Necessity:

Assume q odd (case q even trivially true)

Let $G = G_1$ corresponding to $Y - 1$ in (3).

Depth d odd.

In fact, $G = \mathbb{F}_q[t]/(t)^{p^a}$ and $Y \mapsto Y^{-1}$ induces identity on G .
(Hermitian and Euclidean inner products coincide.)

Any nonzero element of G : $t^\lambda a$ (a unit in G).

Nonzero codeword of length 2 of one of:

(i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

Proof

Nonzero codeword of length 2 of one of:
(i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

Proof

Nonzero codeword of length 2 of one of:
(i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

For word of form (i) to be self-orthogonal,
must have $\mu \geq \frac{d+1}{2}$.

Proof

Nonzero codeword of length 2 of one of:
(i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

For word of form (i) to be self-orthogonal,
must have $\mu \geq \frac{d+1}{2}$.

For word of type (ii) to be self-orthogonal,
need $\lambda \geq \frac{d+1}{2}$.

Proof

Nonzero codeword of length 2 of one of:
 (i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

For word of form (i) to be self-orthogonal,
 must have $\mu \geq \frac{d+1}{2}$.

For word of type (ii) to be self-orthogonal,
 need $\lambda \geq \frac{d+1}{2}$.

For word of type (iii) to be self-orthogonal,
 need

$$t^{2\lambda} a^2 + t^{2\mu} b^2 = 0. \quad (7)$$

Proof

Nonzero codeword of length 2 of one of:
 (i) $(0, t^\mu b)$, (ii) $(t^\lambda a, 0)$ or (iii) $(t^\lambda a, t^\mu b)$.

For word of form (i) to be self-orthogonal,
 must have $\mu \geq \frac{d+1}{2}$.

For word of type (ii) to be self-orthogonal,
 need $\lambda \geq \frac{d+1}{2}$.

For word of type (iii) to be self-orthogonal,
 need

$$t^{2\lambda} a^2 + t^{2\mu} b^2 = 0. \quad (7)$$

If both $\lambda, \mu \geq \frac{d+1}{2}$,
 then (7) automatically satisfied.

Proof

If at least one of them is at most $\frac{d-1}{2}$:

Proof

If at least one of them is at most $\frac{d-1}{2}$:

If $\lambda \neq \mu$,
then (7) never satisfied.

Hence, need $\lambda = \mu$.

Proof

If at least one of them is at most $\frac{d-1}{2}$:

If $\lambda \neq \mu$,
then (7) never satisfied.

Hence, need $\lambda = \mu$.

Then (7) implies

$$a^2 + b^2 \in (t^{d-2\lambda}). \quad (8)$$

Proof

If at least one of them is at most $\frac{d-1}{2}$:

If $\lambda \neq \mu$,
 then (7) never satisfied.

Hence, need $\lambda = \mu$.

Then (7) implies

$$a^2 + b^2 \in (t^{d-2\lambda}). \quad (8)$$

Hence, $a^2 + b^2 \in (t)$, so -1 is a square in \mathbb{F}_q .

Proof

If at least one of them is at most $\frac{d-1}{2}$:

If $\lambda \neq \mu$,
 then (7) never satisfied.

Hence, need $\lambda = \mu$.

Then (7) implies

$$a^2 + b^2 \in (t^{d-2\lambda}). \quad (8)$$

Hence, $a^2 + b^2 \in (t)$, so -1 is a square in \mathbb{F}_q .

Self-dual code of length 2 over G certainly contains at least a codeword of type (iii) (not enough words of other types).

$m = 3$ & Leech Lattice

$$m = 3$$

$$A = \mathbb{Z}_4$$

$GR(4, 2)$: unique Galois extension of \mathbb{Z}_4 of degree 2.

$m = 3$ & Leech Lattice

$$m = 3$$

$$A = \mathbb{Z}_4$$

$GR(4, 2)$: unique Galois extension of \mathbb{Z}_4 of degree 2.

$$R = \mathbb{Z}_4 \oplus GR(4, 2)$$

$m = 3$ & Leech Lattice

$$m = 3$$

$$A = \mathbb{Z}_4$$

$GR(4, 2)$: unique Galois extension of \mathbb{Z}_4 of degree 2.

$$R = \mathbb{Z}_4 \oplus GR(4, 2)$$

ℓ -quasi-cyclic code C over \mathbb{Z}_4 of length $3\ell - (C_1, C_2)$,

C_1 : code over \mathbb{Z}_4 of length ℓ

C_2 : code over $GR(4, 2)$ of length ℓ .

$m = 3$ & Leech Lattice

$$m = 3$$

$$A = \mathbb{Z}_4$$

$GR(4, 2)$: unique Galois extension of \mathbb{Z}_4 of degree 2.

$$R = \mathbb{Z}_4 \oplus GR(4, 2)$$

ℓ -quasi-cyclic code C over \mathbb{Z}_4 of length $3\ell - (C_1, C_2)$,

C_1 : code over \mathbb{Z}_4 of length ℓ

C_2 : code over $GR(4, 2)$ of length ℓ .

$$C = \{(\mathbf{x} + 2\mathbf{a}' - \mathbf{b}' | \mathbf{x} - \mathbf{a}' + 2\mathbf{b}' | \mathbf{x} - \mathbf{a}' - \mathbf{b}') \mid \mathbf{x} \in C_1, \mathbf{a}' + \zeta \mathbf{b}' \in C_2\},$$

$\zeta \in GR(4, 2)$ satisfies $\zeta^2 + \zeta + 1 = 0$.

$m = 3$ & Leech Lattice

C'_2 : linear code of length ℓ over \mathbb{Z}_4

$C_2 := C'_2 + C'_2\zeta$: linear code over $GR(4, 2)$.

$m = 3$ & Leech Lattice

C'_2 : linear code of length ℓ over \mathbb{Z}_4

$C_2 := C'_2 + C'_2\zeta$: linear code over $GR(4, 2)$.

Consider: $\mathbf{a} = -2\mathbf{a}' + \mathbf{b}'$ and $\mathbf{b} = -\mathbf{a}' + 2\mathbf{b}'$

Construction equivalent to $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
 with $\mathbf{x} \in C_1$ and $\mathbf{a}, \mathbf{b} \in C'_2$.

$m = 3$ & Leech Lattice

C'_2 : linear code of length ℓ over \mathbb{Z}_4

$C_2 := C'_2 + C'_2\zeta$: linear code over $GR(4, 2)$.

Consider: $\mathbf{a} = -2\mathbf{a}' + \mathbf{b}'$ and $\mathbf{b} = -\mathbf{a}' + 2\mathbf{b}'$

Construction equivalent to $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
 with $\mathbf{x} \in C_1$ and $\mathbf{a}, \mathbf{b} \in C'_2$.

C'_2 : Klemm-like code κ_8 (over \mathbb{Z}_4)

C_1 : self-dual \mathbb{Z}_4 -code O'_8 , obtained from octacode O_8 by negating
 a single coordinate.

$m = 3$ & Leech Lattice

C'_2 : linear code of length ℓ over \mathbb{Z}_4

$C_2 := C'_2 + C'_2\zeta$: linear code over $GR(4, 2)$.

Consider: $\mathbf{a} = -2\mathbf{a}' + \mathbf{b}'$ and $\mathbf{b} = -\mathbf{a}' + 2\mathbf{b}'$

Construction equivalent to $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction, with $\mathbf{x} \in C_1$ and $\mathbf{a}, \mathbf{b} \in C'_2$.

C'_2 : Klemm-like code κ_8 (over \mathbb{Z}_4)

C_1 : self-dual \mathbb{Z}_4 -code O'_8 , obtained from octacode O_8 by negating a single coordinate.

$$\kappa_8 \Delta O'_8 := \{(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b}) \mid \mathbf{x} \in O'_8, \mathbf{a}, \mathbf{b} \in \kappa_8\}.$$

$m = 3$ & Leech Lattice

C : \mathbb{Z}_4 -linear code of length n
Quaternary lattice

$$\Lambda(C) = \{\mathbf{z} \in \mathbb{Z}^n \mid \mathbf{z} \equiv \mathbf{c} \pmod{4} \text{ for some } \mathbf{c} \in C\}.$$

$m = 3$ & Leech Lattice

C : \mathbb{Z}_4 -linear code of length n
Quaternary lattice

$$\Lambda(C) = \{\mathbf{z} \in \mathbb{Z}^n \mid \mathbf{z} \equiv \mathbf{c} \pmod{4} \text{ for some } \mathbf{c} \in C\}.$$

Theorem

$\Lambda(\kappa_8 \Delta O'_8)/2$ is the Leech lattice Λ_{24} .

Proof

From the $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
Clear: $\kappa_8 \Delta O'_8$ is self-dual.

Proof

From the $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
Clear: $\kappa_8 \Delta O'_8$ is self-dual.

Code generated by $(-\mathbf{a}, \mathbf{0}, \mathbf{a})$, $(\mathbf{0}, \mathbf{b}, -\mathbf{b})$ and $(\mathbf{x}, \mathbf{x}, \mathbf{x})$,
 $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in O'_8$.

Proof

From the $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
Clear: $\kappa_8 \Delta O'_8$ is self-dual.

Code generated by $(-\mathbf{a}, \mathbf{0}, \mathbf{a})$, $(\mathbf{0}, \mathbf{b}, -\mathbf{b})$ and $(\mathbf{x}, \mathbf{x}, \mathbf{x})$,
 $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in O'_8$.

All have Euclidean weights $\equiv 0 \pmod{8}$.

Hence all words in code have weights divisible by 8.

Proof

From the $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction,
Clear: $\kappa_8 \Delta O'_8$ is self-dual.

Code generated by $(-\mathbf{a}, \mathbf{0}, \mathbf{a})$, $(\mathbf{0}, \mathbf{b}, -\mathbf{b})$ and $(\mathbf{x}, \mathbf{x}, \mathbf{x})$,
 $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in O'_8$.

All have Euclidean weights $\equiv 0 \pmod{8}$.

Hence all words in code have weights divisible by 8.

Hence, $\Lambda(\kappa_8 \Delta O'_8)$ is even unimodular lattice.

Proof

Known: $\kappa_8 \cap \mathcal{O}'_8 = 2\mathcal{O}'_8$.

Remains to show: min Euclidean weight in lattice ≥ 16

Proof

Known: $\kappa_8 \cap \mathcal{O}'_8 = 2\mathcal{O}'_8$.

Remains to show: min Euclidean weight in lattice ≥ 16

Suppose Euclidean weight of $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ is 8, for some $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in \mathcal{O}'_8$.

Proof

Known: $\kappa_8 \cap \mathcal{O}'_8 = 2\mathcal{O}'_8$.

Remains to show: min Euclidean weight in lattice ≥ 16

Suppose Euclidean weight of $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ is 8, for some $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in \mathcal{O}'_8$.

$\mathbf{x} \equiv \mathbf{0} \pmod{2}$ and

$\mathbf{a} \equiv \mathbf{b} \equiv \mathbf{0} \pmod{2}$.

Proof

Known: $\kappa_8 \cap \mathcal{O}'_8 = 2\mathcal{O}'_8$.

Remains to show: min Euclidean weight in lattice ≥ 16

Suppose Euclidean weight of $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b})$ is 8, for some $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in \mathcal{O}'_8$.

$\mathbf{x} \equiv \mathbf{0} \pmod{2}$ and

$\mathbf{a} \equiv \mathbf{b} \equiv \mathbf{0} \pmod{2}$.

Then $(\mathbf{x} - \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} - \mathbf{b}) = (\mathbf{x} + \mathbf{a} | \mathbf{x} + \mathbf{b} | \mathbf{x} + \mathbf{a} + \mathbf{b})$,
 so has Euclidean weight at least 16.

$m = 6$ & Golay Code

$$m = 6$$

$$A = \mathbb{F}_2$$

$$R = (\mathbb{F}_2 + u\mathbb{F}_2) \oplus (\mathbb{F}_4 + u\mathbb{F}_4),$$

$\mathbb{F}_2 + u\mathbb{F}_2 = \mathbb{F}_2[Y]/(Y-1)^2$ and $\mathbb{F}_4 + u\mathbb{F}_4 = \mathbb{F}_2[Y]/(Y^2 + Y + 1)^2$,
so $u^2 = 0$ in both $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$.

$m = 6$ & Golay Code

C_1 : unique $\mathbb{F}_2 + u\mathbb{F}_2$ -code of length 4 whose Gray image is binary extended Hamming code with coordinates in reverse order

C_2 : $\mathbb{F}_4 + u\mathbb{F}_4$ -code $C'_2 + C'_2\zeta$,

C'_2 : unique $\mathbb{F}_2 + u\mathbb{F}_2$ -code of length 4 whose Gray image is binary extended Hamming code.

$m = 6$ & Golay Code

C_1 : unique $\mathbb{F}_2 + u\mathbb{F}_2$ -code of length 4 whose Gray image is binary extended Hamming code with coordinates in reverse order

C_2 : $\mathbb{F}_4 + u\mathbb{F}_4$ -code $C'_2 + C'_2\zeta$,

C'_2 : unique $\mathbb{F}_2 + u\mathbb{F}_2$ -code of length 4 whose Gray image is binary extended Hamming code.

Both C_1, C_2 self-dual:

Proposition

Binary extended Golay code is 4-quasi-cyclic.

Vandermonde Construction

A : finite chain ring

m : integer, unit in A

Suppose: A contains unit ζ of order m .

$$Y^m - 1 = (Y - 1)(Y - \zeta) \cdots (Y - \zeta^{m-1}).$$

Vandermonde Construction

(By Fourier Transform)

If $f = f_0 + f_1 Y + \cdots + f_{m-1} Y^{m-1} \in A[Y]/(Y^m - 1)$,
 where $f_i \in A$ for $0 \leq i \leq m-1$, then

$$\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{m-1} \end{pmatrix} = V^{-1} \begin{pmatrix} \hat{f}_0 \\ \hat{f}_1 \\ \vdots \\ \hat{f}_{m-1} \end{pmatrix},$$

\hat{f}_i : Fourier coefficients

$V = (\zeta^{ij})_{0 \leq i, j \leq m-1}$: $m \times m$ **Vandermonde matrix**.

Vandermonde Construction

$\mathbf{a}_0, \dots, \mathbf{a}_{m-1} \in A^\ell$: vectors.

$$V^{-1} \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{pmatrix} \in R^\ell.$$

– Vandermonde product

Vandermonde Construction

Theorem

A, m as above.

C_0, \dots, C_{m-1} : linear codes of length ℓ over A .

Then the Vandermonde product of C_0, \dots, C_{m-1} is a quasi-cyclic code over A of length ℓm and of index ℓ .

Moreover, every ℓ -quasi-cyclic code of length ℓm over A is obtained via the Vandermonde construction.

Codes over \mathbb{Z}_{2^k}

Note: \mathbb{Z}_{2^k} is **not** local.

Codes over \mathbb{Z}_{2k}

Note: \mathbb{Z}_{2k} is **not** local.

Self-dual code over \mathbb{Z}_{2k} is Type II if and only if Euclidean weight of every codeword multiple of $4k$.

Codes over \mathbb{Z}_{2k}

Note: \mathbb{Z}_{2k} is **not** local.

Self-dual code over \mathbb{Z}_{2k} is Type II if and only if Euclidean weight of every codeword multiple of $4k$.

Let $2k = p_1^{e_1} \cdots p_r^{e_r}$ (p_1, \dots, p_r distinct primes).

For $f \in \mathbb{Z}_{2k}[Y]$,

$$\frac{\mathbb{Z}_{2k}[Y]}{(f)} = \frac{\mathbb{Z}_{p_1^{e_1}}[Y]}{(f)} \times \cdots \times \frac{\mathbb{Z}_{p_r^{e_r}}[Y]}{(f)}. \quad (9)$$

Codes over \mathbb{Z}_{2^k}

$Y^2 + Y + 1$ irreducible modulo 2,
so $Y^2 + Y + 1$ irreducible modulo 2^k for all k .

Codes over \mathbb{Z}_{2^k}

$Y^2 + Y + 1$ irreducible modulo 2,
so $Y^2 + Y + 1$ irreducible modulo 2^k for all k .

Suppose k relatively prime to 3.

Then 3 is unit in $\mathbb{Z}_{p_i^{e_i}}$ for every $1 \leq i \leq r$.

Codes over \mathbb{Z}_{2k}

$Y^2 + Y + 1$ irreducible modulo 2,
 so $Y^2 + Y + 1$ irreducible modulo $2k$ for all k .

Suppose k relatively prime to 3.

Then 3 is unit in $\mathbb{Z}_{p_i^{e_i}}$ for every $1 \leq i \leq r$.

$Y - 1$, $Y^2 + Y + 1$ relatively prime in $\mathbb{Z}_{p_i^{e_i}}[Y]$, as

$$1 = 3^{-1}(Y^2 + Y + 1) + 3^{-1}(Y + 2)(Y - 1),$$

so,

$$\frac{\mathbb{Z}_{p_i^{e_i}}[Y]}{(Y^3 - 1)} = \mathbb{Z}_{p_i^{e_i}} \oplus \frac{\mathbb{Z}_{p_i^{e_i}}[Y]}{(Y^2 + Y + 1)}, \quad (10)$$

for every $1 \leq i \leq r$.

Codes over \mathbb{Z}_{2^k}

Therefore,

$$\frac{\mathbb{Z}_{2^k}[Y]}{(Y^3 - 1)} = \mathbb{Z}_{2^k} \oplus \frac{\mathbb{Z}_{2^k}[Y]}{(Y^2 + Y + 1)}.$$

(k relatively prime to 3)

Codes over \mathbb{Z}_{2k}

Therefore,

$$\frac{\mathbb{Z}_{2k}[Y]}{(Y^3 - 1)} = \mathbb{Z}_{2k} \oplus \frac{\mathbb{Z}_{2k}[Y]}{(Y^2 + Y + 1)}.$$

(k relatively prime to 3)

ℓ -quasi-cyclic code of length 3ℓ over $\mathbb{Z}_{2k} \leftrightarrow (C_1, C_2)$,

C_1 : code of length ℓ over \mathbb{Z}_{2k}

C_2 : code of length ℓ over $\mathbb{Z}_{2k}[Y]/(Y^2 + Y + 1)$.

Codes over \mathbb{Z}_{2^k}

Proposition

k : integer coprime with 3

C : self-dual code over \mathbb{Z}_{2^k} .

Then C Type II ℓ -quasi-cyclic code of length 3ℓ if and only if its \mathbb{Z}_{2^k} component C_1 of Type II.

Proof

Necessity:

C contains $(\mathbf{x}, \mathbf{x}, \mathbf{x})$, where \mathbf{x} ranges over C_1 , and, by hypothesis, $(4k, 3) = 1$.

Proof

Necessity:

C contains $(\mathbf{x}, \mathbf{x}, \mathbf{x})$, where \mathbf{x} ranges over C_1 , and, by hypothesis, $(4k, 3) = 1$.

Sufficiency:

A spanning set of codewords of Euclidean weights $\equiv 0 \pmod{4k}$ is

$$(\mathbf{x}, \mathbf{x}, \mathbf{x}), (-\mathbf{a}, \mathbf{b}, \mathbf{a} - \mathbf{b}),$$

with \mathbf{x} running over C_1 , and $\mathbf{a} + \zeta\mathbf{b}$ running over C_2 .

Proof

Note: self-duality of C_2 entails $(\mathbf{a} + \zeta\mathbf{b})(\mathbf{a} + \bar{\zeta}\mathbf{b}) = 0$.

Proof

Note: self-duality of C_2 entails $(\mathbf{a} + \zeta\mathbf{b})(\mathbf{a} + \bar{\zeta}\mathbf{b}) = 0$.

Since

$$\zeta + \bar{\zeta} = -1 \ \& \ \zeta\bar{\zeta} = 1,$$

have

$$\mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b} \equiv 0 \pmod{2k}.$$

Proof

Note: self-duality of C_2 entails $(\mathbf{a} + \zeta\mathbf{b})(\mathbf{a} + \bar{\zeta}\mathbf{b}) = 0$.

Since

$$\zeta + \bar{\zeta} = -1 \ \& \ \zeta\bar{\zeta} = 1,$$

have

$$\mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b} \equiv 0 \pmod{2k}.$$

By bilinearity of $(\ , \)$:

$$(\mathbf{a} - \mathbf{b}, \mathbf{a} - \mathbf{b}) = \mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} - 2\mathbf{a} \cdot \mathbf{b},$$

Norm of $(-\mathbf{a}, \mathbf{b}, \mathbf{a} - \mathbf{b})$:

$$\mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} + (\mathbf{a} - \mathbf{b}) \cdot (\mathbf{a} - \mathbf{b}) = 2(\mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b}),$$

multiple of $4k$.

Alternative Descriptions

Back to local rings.

Alternative Descriptions

Back to local rings.

For simplicity, restrict to \mathbb{Z}_{p^r} , $(m, p) = 1$

$GR(p^r, \ell)$: Galois ring of degree ℓ over \mathbb{Z}_{p^r}

Alternative Descriptions

Back to local rings.

For simplicity, restrict to \mathbb{Z}_{p^r} , $(m, p) = 1$

$GR(p^r, \ell)$: Galois ring of degree ℓ over \mathbb{Z}_{p^r}

Natural isomorphism:

$$\begin{aligned} GR(p^r, \ell)^m &\rightarrow GR(p^r, \ell)[Y]/(Y^m - 1) \\ (c_0, \dots, c_{m-1}) &\mapsto c_0 + c_1 Y + \dots + c_{m-1} Y^{m-1} \end{aligned}$$

Alternative Descriptions

Back to local rings.

For simplicity, restrict to \mathbb{Z}_{p^r} , $(m, p) = 1$

$GR(p^r, \ell)$: Galois ring of degree ℓ over \mathbb{Z}_{p^r}

Natural isomorphism:

$$\begin{aligned} GR(p^r, \ell)^m &\rightarrow GR(p^r, \ell)[Y]/(Y^m - 1) \\ (c_0, \dots, c_{m-1}) &\mapsto c_0 + c_1 Y + \dots + c_{m-1} Y^{m-1} \end{aligned}$$

$T^\ell \leftrightarrow$ Multiplication by Y

Alternative Description

Isomorphism between $\mathbb{Z}_{p^r}^{\ell m}$ and $GR(p^r, \ell)^m$:

$$\begin{aligned} \mathbb{Z}_{p^r}^{\ell m} &\rightarrow GR(p^r, \ell)^m \\ (c_{00}, c_{01}, \dots, c_{0, \ell-1}, \dots, c_{m-1, 0}, \dots, c_{m-1, \ell-1}) &\mapsto (c_0, \dots, c_{m-1}) \end{aligned}$$

where

$$c_i = c_{i,0} + c_{i,1}\xi + \dots + c_{i,\ell-1}\xi^{\ell-1} \in GR(p^r, \ell),$$

ξ : root of monic basic irred polynomial of deg ℓ over \mathbb{Z}_{p^r}

Alternative Description

Isomorphism between $\mathbb{Z}_{p^r}^{\ell m}$ and $GR(p^r, \ell)^m$:

$$\begin{aligned} \mathbb{Z}_{p^r}^{\ell m} &\rightarrow GR(p^r, \ell)^m \\ (c_{00}, c_{01}, \dots, c_{0,\ell-1}, \dots, c_{m-1,0}, \dots, c_{m-1,\ell-1}) &\mapsto (c_0, \dots, c_{m-1}) \end{aligned}$$

where

$$c_i = c_{i,0} + c_{i,1}\xi + \dots + c_{i,\ell-1}\xi^{\ell-1} \in GR(p^r, \ell),$$

ξ : root of monic basic irred polynomial of deg ℓ over \mathbb{Z}_{p^r}

T^ℓ on LHS \leftrightarrow cyclic shift on RHS

Alternative Description

Hence, isomorphism between $\mathbb{Z}_{p^r}^{\ell m}$ and $GR(p^r, \ell)[Y]/(Y^m - 1)$.

Alternative Description

Hence, isomorphism between $\mathbb{Z}_{p^r}^{\ell m}$ and $GR(p^r, \ell)[Y]/(Y^m - 1)$.

$C \subseteq \mathbb{Z}_{p^r}^{\ell m}$: quasi-cyclic code of index ℓ

C : \mathbb{Z}_{p^r} -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$.

Alternative Description

Hence, isomorphism between $\mathbb{Z}_{p^r}^{\ell m}$ and $GR(p^r, \ell)[Y]/(Y^m - 1)$.

$C \subseteq \mathbb{Z}_{p^r}^{\ell m}$: quasi-cyclic code of index ℓ

C : \mathbb{Z}_{p^r} -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$.

Easy: $C \in GR(p^r, \ell)[Y]/(Y^m - 1)$ clearly invariant under multiplication by Y ,

So, C : $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$.

Generators

If C as $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$ generated by $\mathbf{c}_1(Y), \dots, \mathbf{c}_t(Y)$, then

$$C = \{a_1(Y)\mathbf{c}_1(Y) + \dots + a_t(Y)\mathbf{c}_t(Y) \mid a_i(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1)\}.$$

Generators

If C as $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$ generated by $\mathbf{c}_1(Y), \dots, \mathbf{c}_t(Y)$, then

$$C = \{a_1(Y)\mathbf{c}_1(Y) + \dots + a_t(Y)\mathbf{c}_t(Y) \mid a_i(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1)\}.$$

As \mathbb{Z}_{p^r} -submodule, generated by

$$\{\mathbf{c}_1(Y), Y\mathbf{c}_1(Y), \dots, Y^{m-1}\mathbf{c}_1(Y), \dots, \mathbf{c}_t(Y), Y\mathbf{c}_t(Y), \dots, Y^{m-1}\mathbf{c}_t(Y)\}.$$

Generators

If C as $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$ generated by $\mathbf{c}_1(Y), \dots, \mathbf{c}_t(Y)$, then

$$C = \{a_1(Y)\mathbf{c}_1(Y) + \dots + a_t(Y)\mathbf{c}_t(Y) \mid a_i(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1)\}.$$

As \mathbb{Z}_{p^r} -submodule, generated by

$$\{\mathbf{c}_1(Y), Y\mathbf{c}_1(Y), \dots, Y^{m-1}\mathbf{c}_1(Y), \dots, \mathbf{c}_t(Y), Y\mathbf{c}_t(Y), \dots, Y^{m-1}\mathbf{c}_t(Y)\}.$$

$t = 1$: **1-generator** quasi-cyclic code

Digression to Cyclic Codes

Proposition

C : nonzero cyclic code of length m over $GR(p^r, \ell)$.

C is free module over $GR(p^r, \ell)$ if and only if C is generated by a monic polynomial $g(Y)$ dividing $Y^m - 1$ over $GR(p^r, \ell)$.

Then:

C of rank $m - \deg g$, and

basis $g(Y), Yg(Y), \dots, Y^{m-\deg g-1}g(Y)$.

Proof

Sufficiency:

Proof

Sufficiency:

There exists monic $h(Y)$ such that

$$Y^m - 1 = g(Y)h(Y) \equiv 0 \pmod{Y^m - 1}.$$

Say $\deg g = m - k$ and $\deg h = k$.

Proof

Sufficiency:

There exists monic $h(Y)$ such that

$$Y^m - 1 = g(Y)h(Y) \equiv 0 \pmod{Y^m - 1}.$$

Say $\deg g = m - k$ and $\deg h = k$.

Then $Y^t g(Y)$ ($t \geq k$) is linear combination (over $GR(p^r, \ell)$) of $g(Y), Yg(Y), \dots, Y^{k-1}g(Y)$.

Proof

Sufficiency:

There exists monic $h(Y)$ such that

$$Y^m - 1 = g(Y)h(Y) \equiv 0 \pmod{Y^m - 1}.$$

Say $\deg g = m - k$ and $\deg h = k$.

Then $Y^t g(Y)$ ($t \geq k$) is linear combination (over $GR(p^r, \ell)$) of $g(Y), Yg(Y), \dots, Y^{k-1}g(Y)$.

Hence, every element of C (as ideal in $GR(p^r, \ell)[Y]/(Y^m - 1)$) is linear combination of $g(Y), Yg(Y), \dots, Y^{k-1}g(Y)$.

Proof

If there exist $a_0, a_1, \dots, a_{k-1} \in GR(p^r, \ell)$ such that

$$a_0g(Y) + a_1Yg(Y) + \dots + a_{k-1}Y^{k-1}g(Y) = 0,$$

then

$$Y^m - 1 \mid (a_0 + a_1Y + \dots + a_{k-1}Y^{k-1})g(Y).$$

Proof

If there exist $a_0, a_1, \dots, a_{k-1} \in GR(p^r, \ell)$ such that

$$a_0g(Y) + a_1Yg(Y) + \dots + a_{k-1}Y^{k-1}g(Y) = 0,$$

then

$$Y^m - 1 \mid (a_0 + a_1Y + \dots + a_{k-1}Y^{k-1})g(Y).$$

By degree consideration, $a_0 = \dots = a_{k-1} = 0$.

Proof

If there exist $a_0, a_1, \dots, a_{k-1} \in GR(p^r, \ell)$ such that

$$a_0g(Y) + a_1Yg(Y) + \dots + a_{k-1}Y^{k-1}g(Y) = 0,$$

then

$$Y^m - 1 \mid (a_0 + a_1Y + \dots + a_{k-1}Y^{k-1})g(Y).$$

By degree consideration, $a_0 = \dots = a_{k-1} = 0$.

Hence, C free, of rank $k = m - \deg g$, and basis $g(Y), Yg(Y), \dots, Y^{m-\deg g-1}g(Y)$.

Proof

Necessity:

Proof

Necessity:

Suppose C free with basis c_1, \dots, c_s .

Proof

Necessity:

Suppose C free with basis c_1, \dots, c_s .

$$C \simeq GR(p^r, \ell)^s \Rightarrow C \pmod{p} \simeq \mathbb{F}_{p^\ell}^s$$

Known: C generated by monic polynomial $g(Y)$ over $GR(p^r, \ell)$

Proof

Necessity:

Suppose C free with basis c_1, \dots, c_s .

$$C \simeq GR(p^r, \ell)^s \Rightarrow C \pmod{p} \simeq \mathbb{F}_{p^\ell}^s$$

Known: C generated by monic polynomial $g(Y)$ over $GR(p^r, \ell)$

Then: $C \pmod{p}$ generated by $g(Y) \pmod{p}$.

Proof

$$\deg g = \deg(g \pmod{p}) \quad (g \text{ monic})$$

Proof

$$\deg g = \deg(g \pmod{p}) \quad (g \text{ monic})$$

Size of $C \pmod{p}$ implies $\deg g = m - s$.

Proof

$\deg g = \deg(g \pmod{p})$ (g monic)

Size of $C \pmod{p}$ implies $\deg g = m - s$.

Easy: $\{g(Y), Yg(Y), \dots, Y^{s-1}g(Y)\}$ linearly indep over $GR(p^r, \ell)$,

hence basis for C .

Proof

$Y^s g(Y) \in C \Rightarrow$ there exists monic $a(Y)$ such that $a(Y)g(Y) = 0$,
i.e., $Y^m - 1 | a(Y)g(Y)$.

Proof

$Y^s g(Y) \in C \Rightarrow$ there exists monic $a(Y)$ such that $a(Y)g(Y) = 0$,
i.e., $Y^m - 1 | a(Y)g(Y)$.

Considering degrees, $Y^m - 1 = a(Y)g(Y)$, i.e., $g(Y) | Y^m - 1$.

1-Generator Codes

As $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$,

$$C = \{a(Y)g(Y) \mid a(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1)\}.$$

1-Generator Codes

As $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ -submodule of $GR(p^r, \ell)[Y]/(Y^m - 1)$,

$$C = \{a(Y)\mathbf{g}(Y) \mid a(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1)\}.$$

$$\mathbf{g}(Y) = (g_0(Y), \dots, g_{\ell-1}(Y)),$$

$$g_i(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1).$$

1-Generator Quasi-Cyclic Codes

Theorem

C : 1-generator ℓ -QC code over \mathbb{Z}_{p^r} of length $n = m\ell$ with generator

$$\mathbf{g}(Y) = (g(Y)f_0(Y), g(Y)f_1(Y), \dots, g(Y)f_{\ell-1}(Y)),$$

$$g(Y) \mid Y^m - 1,$$

$$g(Y), f_i(Y) \in \mathbb{Z}_{p^r}[Y]/(Y^m - 1),$$

$$(f_i(Y), h(Y)) = 1, \text{ where } h(Y) = (Y^m - 1)/g(Y).$$

Then: C free \mathbb{Z}_{p^r} -module of rank $m - \deg g$, with basis $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{m-\deg g-1}\mathbf{g}(Y)\}$.

Proof

Write $g(Y)h(Y) = Y^m - 1$.

If $\deg g = m - k$, then $\deg h = k$.

Proof

Write $g(Y)h(Y) = Y^m - 1$.

If $\deg g = m - k$, then $\deg h = k$.

Every codeword in C :

$$\mathbf{c}(Y) = a(Y)\mathbf{g}(Y).$$

Proof

Write $g(Y)h(Y) = Y^m - 1$.

If $\deg g = m - k$, then $\deg h = k$.

Every codeword in C :

$$\mathbf{c}(Y) = a(Y)\mathbf{g}(Y).$$

By Division Algorithm,

$$a(Y) = q(Y)h(Y) + r(Y),$$

$\deg r < \deg h$ or $r(Y) = 0$.

Proof

Write $g(Y)h(Y) = Y^m - 1$.

If $\deg g = m - k$, then $\deg h = k$.

Every codeword in C :

$$\mathbf{c}(Y) = a(Y)\mathbf{g}(Y).$$

By Division Algorithm,

$$a(Y) = q(Y)h(Y) + r(Y),$$

$\deg r < \deg h$ or $r(Y) = 0$.

Hence, $\mathbf{c}(Y) = a(Y)\mathbf{g}(Y) = r(Y)\mathbf{g}(Y)$.

Therefore, C generated by $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{k-1}\mathbf{g}(Y)\}$.

Proof

Need to show: $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{k-1}\mathbf{g}(Y)\}$ linearly independent.

Proof

Need to show: $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{k-1}\mathbf{g}(Y)\}$ linearly independent.

Suppose there are $a_0, \dots, a_{k-1} \in \mathbb{Z}_{p^r}$ such that

$$\sum_{i=0}^{k-1} a_i Y^i \mathbf{g}(Y) = 0.$$

Proof

Need to show: $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{k-1}\mathbf{g}(Y)\}$ linearly independent.

Suppose there are $a_0, \dots, a_{k-1} \in \mathbb{Z}_{p^r}$ such that

$$\sum_{i=0}^{k-1} a_i Y^i \mathbf{g}(Y) = 0.$$

Write $a(Y) = \sum_{i=0}^{k-1} a_i Y^i$.

Then: $a(Y)f_i(Y)g(Y) = 0$ in $\mathbb{Z}_{p^r}[Y]/(Y^m - 1)$ for all i ,

i.e., $Y^m - 1 | a(Y)f_i(Y)g(Y)$ for all i .

Proof

Equivalently, $\frac{Y^m-1}{g(Y)} \mid a(Y)f_i(Y)$.

Proof

Equivalently, $\frac{Y^m-1}{g(Y)}|a(Y)f_i(Y)$.

Since $(f_i(Y), (Y^m - 1)/g(Y)) = 1$, follows that $h(Y)|a(Y)$.

Proof

Equivalently, $\frac{Y^m-1}{g(Y)}|a(Y)f_i(Y)$.

Since $(f_i(Y), (Y^m - 1)/g(Y)) = 1$, follows that $h(Y)|a(Y)$.

Considering degrees, $a(Y) = 0$.

Proof

Equivalently, $\frac{Y^m-1}{g(Y)}|a(Y)f_i(Y)$.

Since $(f_i(Y), (Y^m - 1)/g(Y)) = 1$, follows that $h(Y)|a(Y)$.

Considering degrees, $a(Y) = 0$.

Hence, $\{\mathbf{g}(Y), Y\mathbf{g}(Y), \dots, Y^{k-1}\mathbf{g}(Y)\}$ linearly independent.