Codes over finite quotient of polynomial rings

Nora EL AMRANI

Limoges University, XLIM Laboratory and Mohammed V-Agdal University Rabat

Plan

1. Codes over finite quotient of polynomial rings
   - motivations and notations
   - Special Cases
   - Generator Matrix
   - Hermit Normal Form
   - Duality
     - Scalar product
   - Binary image of codes
     - Matrix code generator of a binary image
     - Calculating of the dual
2. Perspective

Codes over finite quotient of polynomial rings: motivations and notations

- Let be $p(x) \in \mathbb{F}_2[x]$ with $deg(p(x)) = m$

Codes over finite quotient of polynomial rings: motivations and notations

- Let be $p(x) \in \mathbb{F}_2[x]$ with $deg(p(x)) = m$
- $A = \mathbb{F}_2[x]/p(x)$ with euclidien division.

Codes over finite quotient of polynomial rings: motivations and notations

- Let be $p(x) \in \mathbb{F}_2[x]$ with $deg(p(x)) = m$
- $A = \mathbb{F}_2[x]/p(x)$ with euclidien division.
- $E = A^\ell$ where ℓ in $\mathbb{N}^*$

Definition

A code C of length ℓ over a ring A, is a submodule of E, that is stable by addition and multiplication by element of A.

Special Cases

- when $p(x) = x^m - 1$ C is a quasi-cyclic code.

Special Cases

- when $p(x) = x^m - 1$ C is a quasi-cyclic code.
- When $p(x)$ irreducible we have $A \cong \mathbb{F}_{2^m}$ which gives codes over $\mathbb{F}_{2^m}$.

Special Cases

- when $p(x) = x^m - 1$ C is a quasi-cyclic code.
- When $p(x)$ irreducible we have $A \cong \mathbb{F}_{2^m}$ which gives codes over $\mathbb{F}_{2^m}$.
- When $p(x) = p_1(x)p_2(x)$ and $p_1(x)$ and $p_2(x)$ are irreducible, is the case that we consider to study in this talk.

Generator Matrix

Let C be a binary code of length ℓ on A, a matrix M of size $k \times \ell$ is called a generator matrix of the code C, if the application defined as

$$\begin{aligned} \phi \quad : \quad & A^k \longrightarrow A^\ell \\ & x \longmapsto \phi(x) = x.M \end{aligned}$$

satisfy : $\phi(A^k) = C$.

Example

Let

$$M = \begin{pmatrix} x^3+x+1 & x(x^3+x+1) & (x^2+1)(x^3+x+1) \\ 0 & x^4+x+1 & x \end{pmatrix}$$

be a matrix generator of a code C *of length* 3 *over* $\mathbb{F}_2[x]/p(x)$*, with* $p(x) = (x^3+x+1)(x^4+x+1)$*.*
we have $Ker\phi = \{(y(x^4+x+1), 0)$ *with* y *in* A $\}$ *and* $|C| = 8$

$\mathbb{F}_2$ generator matrix

Proposition

Let $M = (g_1(x), g_2(x), \ldots, g_l(x))$ *be a generator matrix of a single line, the* $\mathbb{F}_2$*-generator matrix is*

$$M' = \begin{pmatrix} g_1(x) & g_2(x) & \ldots & g_l(x) \\ xg_1(x) & xg_2(x) & \ldots & xg_l(x) \\ x^2g_1(x) & x^2g_2(x) & \ldots & x^2g_l(x) \\ \vdots & \vdots & \vdots & \vdots \\ x^{m-d}g_1(x) & x^{m-d}g_2(x) & \ldots & x^{m-d}g_l(x) \end{pmatrix}$$

where $d = deg(pgcd(p(x), g_1(x), g_2(x), \ldots, g_l(x)))$

Remark

If M is a generator matrix of multiple rows, the $\mathbb{F}_2$-generator matrix is the concatenation of the $\mathbb{F}_2$-generator matrix of each line.

Example

Let $M = \begin{pmatrix} x^3+x+1 & x(x^3+x+1) & (x^2+1)(x^3+x+1) \\ 0 & x^4+x+1 & x \end{pmatrix}$ *be a matrix generator of a code* C *of length* 3 *over* $\mathbb{F}_2[x]/p(x)$*, with* $p(x) = (x^3+x+1)(x^4+x+1)$*, the* $\mathbb{F}_2$*-generator matrix of* C *is :*

$$M = \begin{pmatrix} x^3+x+1 & x(x^3+x+1) & (x^2+1)(x^3+x+1) \\ x^4+x^3+x & x^5+x^3+x^2 & x^6+x^5+x^4+x \\ x^5+x^4+x^2 & x^6+x^5+x^3 & x^6+x^3+1 \\ x^6+x^5+x^3 & x^6+x^5+x^4+x^3+x^2+1 & x^5+x^4+x^3+x^2+x+1 \\ 0 & x^4+x+1 & x \\ 0 & x^5+x^2+x & x^2 \\ 0 & x^6+x^3+x^2 & x^3 \\ 0 & x^5+x^4+x^2+1 & x^4 \\ 0 & x^6+x^5+x^3+x & x^5 \\ 0 & x^6+x^5+x^4+x^3+1 & x^6 \\ 0 & x^6+x^4+x^3+x^2+x+1 & x^5+x^3+x^2+1 \end{pmatrix}$$

Hermite Normal Form

Definition

An $k \times \ell$ matrix M is in Hermite normal form if :

1. *M is echeloned.*
2. *all the first non zero polynomials in each line are divisors of $p(x)$.*
3. *if g_{ij} is the first non zero polynomial in the line "i" and column "j" we have :* $deg(g_{ij} > deg(g_{(i-t)j})$ *where* $1 \leq t < i$.

Kristine Lally, Patrick Fitzpatrick, "Algebraic structure of quasicyclic codes" Original Research Article Discrete Applied Mathematics, Volume 111, Issues 1–2, 15 July 2001, Pages 157-175

Reduction algorithm

1. Vector reduction.
2. Gaussian elimination.
3. Echlonned matrix.
4. Hermite normal form.

Example

$$M = \begin{pmatrix} x^4 + x2 + x & x^4 + x & x^6 + x^3 + x^2 + x \\ x^4 + x^3 + x^2 + 1 & x^6 + x^2 & x^6 + x^5 + x^2 + x \end{pmatrix}$$

The Hermite normal form of M is :

$$\begin{pmatrix} x^3 + x + 1 & x^3 + 1 & x^5 + x^4 + x + 1 \\ 0 & x^4 + x + 1 & x + 1 \end{pmatrix}$$

Duality in E

Definition

Scalar product in E:
Let $u, v \in E$ such that $u = (u_1(x), u_2(x), \ldots, u_\ell(x))$ and $v = (v_1(x), v_2(x), \ldots, v_\ell(x))$.

We denote by $\langle u(x), v(x)\rangle = \sum_{i=1}^{\ell} u_i(x)v_i(x)$ the application which associate to two vectors in E an element of A: the scalar product of u and v in the ring E.

Proposition

Let C be a linear code of length ℓ over A.

$$C^{\perp} = \{v \in E / < u, v >= 0 \ mod \ p(x) \ \forall u \in C\}$$

binary image of codes over A

Notations

$\varphi : A \longrightarrow \mathbb{F}_2^m$:
$u(x) = \sum_{i=0}^{m-1} a_i x^i \longrightarrow (a_0, a_1, \ldots, a_{m-1})$.
$\omega : A^\ell \longrightarrow \mathbb{F}_2^{m\ell}$:
$(u_1(x), \ldots, u_\ell(x)) \longrightarrow (\varphi(u_1), \ldots, \varphi(u_\ell))$.

Multiplication matrix by x

Multiplication matrix by x:

$$M_p = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_0 & p_1 & \dots & \dots & p_{m-1} \end{pmatrix}$$

where $\varphi(p(x)) = (p_0, \dots, p_{m-1})$.

Multiplication matrix by an element in A

Let $f(x) \in A$ the multiplication matrix by f in A is :

$$M_{f(x)} = \sum_{i=0}^{m-1} f_i M_p^i$$

Where f_i is a vector of size ℓ, and that has zero everywhere, except at position "i" where it has the coefficient of index "i" of the polynomial $f(x)$.

$$f_i.M_p = (f_0, \dots, f_{m-1}).\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ p_0 & p_1 & \dots & \dots & p_{m-1} \end{pmatrix}$$

$$= \begin{pmatrix} f_{m_1} p_0 \\ f_0 + f_{m-1} p_1 \\ \vdots \\ f_{m-2} + f_{m-1} p_{m-1} \end{pmatrix}$$

For $a(x) \in A$:$\varphi(a(x)f(x)) = \varphi(a(x))M_{f(x)}$

generator matrix of a binary image code

Let G_a a matrix $k \times \ell$ over A, we denote by ψ the application that associate to each matrix of A his binary image over $\mathbb{F}_2$.

$$\psi(G_a) = G_b = \begin{pmatrix} M_{f_{11}} & M_{f_{12}} & \dots & M_{f_{1\ell}} \\ \vdots & \vdots & \vdots & \vdots \\ M_{f_{k1}} & M_{f_{k2}} & \dots & M_{f_{k\ell}} \end{pmatrix}$$

Definition

Let C_A be a code over A of length ℓ, then $C_B = \omega(C_A)$, where C_B is a binary image of C_A over $\mathbb{F}_2^n$ where $n = m\ell$.

Theorem

If M_A is a generator matrix of a code C over A, Then $\psi(M_A) = M_B$ is a matrix whose lines generates C_B.

Calculating of the dual

1. **Codes over A**
   Let C be a code of length ℓ on A and M be a generator matrix of C, then
   $C^{\perp} = \{h \in A/G.h^t = 0\}$
   $\Longleftrightarrow \ \{\ i \in \{1, \dots, k\} \langle g_i, h\rangle = 0\}$.
   where g_i is a row vector of M.
2. **Binary image**
   $\sum_{j=1}^{\ell} M^t_{g_{i,j}(x)} \varphi(h_j(x))^t = 0$, for all $i \in \{1, \dots, k\}$, with the $g_{i,j}(x)$ are the coefficients of the vector g_i.

Theorem

Let C be a code of length ℓ on A and M be a generator matrix of C.
Set:

$$H = \begin{pmatrix} M^t_{g_{1,1}} & \dots & M^t_{g_{1,\ell}} \\ \vdots & \vdots & \vdots \\ M^t_{g_{k,1}} & \dots & M^t_{g_{k,\ell}} \end{pmatrix}$$

H is a matrix which generates $\omega(C^\perp)^\perp$ (H is not necessarily full rank).

Example

Let C be a binary linear code of length $\ell = 7$ on $\mathbb{F}[x]_2/p(x)$ where $p(x) = (x^3+x+1)(x^4+x+1) = x^7+x^5+x^3+x^2+1$ and its canonical generator matrix M of size $4\times$ 7:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & x^6+x^5+x^4+x & x^6+x^5+x^4+x^2+1 & x^4+x^3+1 \\ 0 & 1 & 0 & 0 & x^6+x^5+x^4+x^3+x^2+x+1 & x^6+x^5+x^3+1 & x^6+x^5+x^4+x^2+1 \\ 0 & 0 & 1 & 0 & x^3+x+1 & x^4+x^3+x+1 & x^6+x^5+1 \\ 0 & 0 & 0 & 1 & x^6 & x^5+x^4+x^2+x+1 & x^6+x^5+x+1 \end{pmatrix}$$

The binary image $\omega(C)$ parameters are $[49, 28, 6]$, and its dual binary image $\omega(C)^{\perp}$ has parameters $[49, 21, 8]$.
The dual of C over A is:

$$M^{\perp} =$$

$$\begin{pmatrix} 1 & 0 & 0 & x^4+x^3+1 & x^4+x^3+x^2+x & x^5+x^4+x^3+x & x^6+x^5+x \\ 0 & 1 & 0 & x^4+x^3+x+1 & x^6+x^4 & x^6+x^5+x^4+1 & x^6+x^4+x^3+1 \\ 0 & 0 & 1 & x^6+x^4+x^3+x^2+x & x^5+x^3+1 & x^4+x^3+x^2+x & 0 \end{pmatrix}$$

The binary image $\omega(C^{\perp})$ to its dual A is of parameters $[49, 21, 9]$.
Then we can see that $\omega(C)^{\perp} \neq \omega(C^{\perp})$.

Perspective

- Search for primitive n^{th} roots in the group of invertible A^* in A to Build Reed-Solomon codes.

Thank you for your attention