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
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 $p(x) \in F_2[x]$ with $deg(p(x)) = m$
- $A = F_2[x]/p(x)$ with euclidian division.
Codes over finite quotient of polynomial rings: motivations and notations

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

- \( A = \mathbb{F}_2[x]/p(x) \) with euclidien division.

- \( E = A^\ell \) where \( \ell \) in \( \mathbb{N}^* \)

**Definition**

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

$$
\phi : A^k \longrightarrow A^\ell \\
x \longmapsto \phi(x) = x.M
$$

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 \( \text{Ker} \phi = \{(y(x^4 + x + 1), 0) \mid y \in A \} \) and \( |C| = 8 \)
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

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

where $d = \deg(p \gcd(p(x), g_1(x), g_2(x), \ldots, g_l(x)))$
**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 :

\[
M = \begin{pmatrix}
 x^3 + x + 1 & x(x^3 + x + 1) & (x^2 + 1)(x^3 + x + 1) \\
 x^4 + x^3 + x & x^5 + x^3 + x^2 & x^6 + x^5 + x^4 + x \\
 x^5 + x^4 + x^2 & x^6 + x^5 + x^3 & x^6 + x^3 + 1 \\
 x^6 + x^5 + x^3 & x^6 + x^4 + x^3 + x^2 + 1 & x^5 + x^4 + x^3 + x^2 + x + 1 \\
 0 & x^4 + x + 1 & x \\
 0 & x^5 + x^2 + x & x^2 \\
 0 & x^6 + x^3 + x^2 & x^3 \\
 0 & x^5 + x^4 + x^2 + 1 & x^4 \\
 0 & x^6 + x^5 + x^3 + x & x^5 \\
 0 & x^6 + x^5 + x^4 + x^3 + 1 & x^6 \\
 0 & x^6 + x^4 + x^3 + x^2 + x + 1 & x^5 + x^3 + x^2 + 1
\end{pmatrix}
\]
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:
   \[ \deg(g_{ij}) > \deg(g_{(i-t)j}) \text{ where } 1 \leq t < i. \]

Reduction algorithm

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

Example

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

The Hermite normal form of \( M \) is:

\[ \begin{pmatrix} x^3 + x + 1 & x^3 + 1 & x^5 + x^4 + x + 1 \\ 0 & x^4 + x + 1 & x + 1 \end{pmatrix} \]
**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 $\ell$ over $A$.

$$C^\perp = \{ v \in E / \langle u, v \rangle = 0 \mod p(x) \ \forall u \in C \}$$
Binary image of codes over $A$

**Notations**

\[ \varphi : A \to \mathbb{F}_2^m : \]
\[ u(x) = \sum_{i=0}^{m-1} a_i x^i \to (a_0, a_1, \ldots, a_{m-1}). \]

\[ \omega : A^\ell \to \mathbb{F}_2^{m\ell} : \]
\[ (u_1(x), \ldots, u_\ell(x)) \to (\varphi(u_1), \ldots, \varphi(u_\ell)). \]
Multiplication matrix by $x$:

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

where $\varphi(p(x)) = (p_0, \ldots, p_{m-1})$. 
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 $\ell$, and that has zero everywhere, except at position ”$i$” where it has the coefficient of index ”$i$” of the polynomial $f(x)$.

\[
\begin{bmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & 0 \\
p_0 & p_1 & \ldots & \ldots & p_{m-1}
\end{bmatrix}
\]

$$f_i \cdot M_p = (f_0, \ldots, f_{m-1}).\begin{bmatrix}
f_{m} p_0 \\
f_0 + f_{m-1} p_1 \\
\vdots \\
f_{m-2} + f_{m-1} p_{m-1}
\end{bmatrix}$$

For $a(x) \in A : \varphi(a(x)f(x)) = \varphi(a(x))M_f(x)$
Let $G_a$ a matrix $k \times \ell$ over $A$, we denote by $\psi$ the application that associate to each matrix of $A$ his binary image over $\mathbb{F}_2$.

$$\psi(G_a) = G_b = \begin{pmatrix}
M_{f11} & M_{f12} & \ldots & M_{f1\ell} \\
\vdots & \vdots & \ddots & \vdots \\
M_{fk1} & M_{fk2} & \ldots & M_{fk\ell}
\end{pmatrix}$$

**Definition**

Let $C_A$ be a code over $A$ of length $\ell$, 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 $\ell$ on $A$ and $M$ be a generator matrix of $C$, then
\[ C^\perp = \{ h \in A/G. h^t = 0 \} \]
\[ \iff \{ i \in \{1, \ldots, k\} \langle g_i, h \rangle = 0 \} . \]
where $g_i$ is a row vector of $M$.

2 Binary image
\[ \sum_{j=1}^{\ell} M_{g_{i,j}(x)}^t \varphi(h_j(x))^t = 0, \text{ for all } i \in \{1, \ldots, k\}, \text{ with} \]
the $g_{i,j}(x)$ are the coefficients of the vector $g_i$. 
Theorem

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

\[
H = \begin{pmatrix}
M_{g_1,1}^t & \ldots & M_{g_1,\ell}^t \\
\vdots & \ddots & \vdots \\
M_{g_k,1}^t & \ldots & M_{g_k,\ell}^t
\end{pmatrix}
\]

$H$ 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 $\omega(C)\perp \neq \omega(C\perp)$. 
Search for primitive $n^{th}$ roots in the group of invertible $A^*$ in $A$ to Build Reed-Solomon codes.
Thank you for your attention