On (σ, δ)-Codes over rings

M. **Boulagouaz** and A. **Deajim**

Non Commutative rings and their applications V
12 -15 Jun 2017
Jean Perrin Faculty, Artois University

RESULTS

In this talk we :

1. Recall the notion of (σ, δ)-codes over a ring *R* (which is not necessary commutative) introduced by Boulagouaz and Leroy (2013) and generating and control matrices of such codes.
2. Introduce a definition of a Frobenius (σ, δ)- code.

RESULTS

In this talk we :

1. Prove a recursive formulas to calculate entries of generating and control matrices of (σ, δ)-codes.
2. We deduce by using this recursive formulas :
   - A general form for generating and control matrices of a principal (σ, δ) code.
   - A generating and control matrices of a principal (σ, δ)-Frobenius code.
3. Show that the dual of a principal (σ, δ)-Frobenius code of length n and dimension r is a free code of dimension $n - r$,
4. Give a characterization of a principal $(\sigma, 0)$-Frobenius code C over a **finite commutative ring** such that the dual code $C^{\perp}$ is a principal $(\sigma, 0)$-Frobenius code.
5. Deduce a characterization of $(\sigma, 0)$-Frobenius self code.

P.L.T. associated to a polynomial

Let A be a ring with 1 and σ a ring endomorphism of A.

Definition

An additive map $\delta \in End(A,+)$ is a σ-derivation if, for any $a, b \in A$, we have :

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

Let δ a σ-derivation, $f \in A_{\sigma,\delta} := A[t;\sigma,\delta]$, a monic polynomial of degree **n** and C_f the companion matrix of f.

Proposition-Definition

Then the map

$T_f : A^n \longrightarrow A^n.$

$"\underline{v} \longrightarrow T_f(\underline{v}) = \sigma(\underline{v})C_f + \delta(\underline{v})"$

$(a_1, ..., a_n) \longrightarrow T_f(a_1, ..., a_n) := (\sigma(a_1)...\sigma(a_n))C_f + (\delta(a_1), ..., \delta(a_n))$

satisfies : $(\forall \alpha \in A)(\forall v \in A^n)$: $T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v$

T_f *is called the pseudo-linear transformation associated to f.*

(σ, δ)-codes

In the next :

- A be a ring, σ be an endomorphism,δ be a σ-derivation of A and $A_{\sigma,\delta} := A[t; \sigma, \delta]$, the skew polynomial ring over A.
- $A_{\sigma,\delta}/(f)_l$ denotes the $A_{\sigma,\delta}$-left module, where $(f)_l$ is the left ideal generated by the monic polynomilal f in $A_{\sigma,\delta}$.

Definition

- *An (σ, δ)-code of length n over A is a subset $\mathcal{C}$ of A^n consisting of the coordinates of a left $A_{\sigma,\delta}$-submodule $\mathcal{M}$ of $A_{\sigma,\delta}/(f)_l$.*
- *In other words, $\mathcal{C} \subseteq A^n$ is an (σ, δ)-code if $\{\sum_{i=0}^{n-1} c_i X^i + (f)_l/(c_0, \dots, c_{n-1}) \in \mathcal{C}\}$ is a left $A_{\sigma,\delta}$-submodule of $A_{\sigma,\delta}/(f)_l$.*

Remarks

- *A is not necessary commutative,*
- *A is not necessary finite.*

Principal (σ, δ)-codes

Definition

1. *If $\mathcal{M}$ is a cyclic submodule (i.e. $\mathcal{M} = (g)_l/(f)_l$ for some right monic divisor $g(X)$ of $f(X)$ in $A_{\sigma,\delta}$), then the (σ, δ)-code represented by $\mathcal{M}$ is called a principal (σ, δ)-code and we denote this code $\mathcal{C} = (g)_{(n,\sigma,\delta)}$.*
2. *If $f(X) = X^n - c$ for some $c \in U(A)$ (set of units of A), then the code $\mathcal{C} = (g)_{(n,\sigma,\delta)}$ is called a constacyclic (σ, δ)-code and we denote $\mathcal{C} = (g)^c_{(n,\sigma,\delta)}$.*

Particular cases of (σ, δ)-codes

1. If $A = \mathbb{F}_{p^n}, \quad \sigma = \theta$, the Frobenius automorphism of the finite field $\mathbb{F}_{p^n}$
   $\diamond$ then a module (σ, δ)-code over a field introduced in [2], is a (σ, δ)-code over $\mathbb{F}_{p^n}$.
2. If A is a Galois ring, $\sigma = \theta$, the Frobenius automorphism of the ring $A, \quad \delta = 0, \quad f = t^n - \lambda$ and $f = gh$
   $\diamond$ then a θ principal constacyclic code over the Galois ring A, introduced in [1] is a constacyclic (σ, δ)-code over A.

Generic and control matrices of a principal (σ, δ)-code

Definition

Let $\mathcal{C}$ be a free (σ, δ)-code over A(its representation polynomial is a free submodule) of dimension r. We say that a matrix :

1. $G \in M_{(n-r)\times n}(A)$ *is a generating matrix of* $\mathcal{C}$ *if* $\mathcal{C} = \{c\,G \mid c \in A^{n-r}\}$.
2. $H \in M_{n\times n}(A)$ *is a control matrix (or a parity-check matrix) of* $\mathcal{C}$ *if* $\mathcal{C} = \{c \in A^n \mid c\,H = 0\}$.

Remark

The control matrix H is a square matrix of order n.

Generic and control matrices of a (σ, δ)-codes

[Theorem1 and Corollary1, [3]]

If $g(X) = \sum_{i=0}^{r} g_i X^i$ is a right monic divisor of $f(X)$ in $A_{\sigma,\delta}$ of degree r, then :

1. The principal (σ, δ)-code $\mathcal{C}$ corresponding to $(g)_l/(f)_l$ is :
   - A free left A-module of rank $n - r$,
   - $(\forall c \in A^n)(c \in \mathcal{C} \Rightarrow T_f(x) \in \mathcal{C})$,
   - The rows of a generating matrix G of $\mathcal{C}$ are given by
     $$T_f^k(g_0, \ldots, g_r, 0, \ldots, 0), \quad \text{for } 0 \leq k \leq n - r - 1.$$
2. If, in addition, $g(X)$ is a right and left divisor of $f(X)$ and $f(X) = g(X)h(X)$ for $h(X) = \sum_{i=0}^{n-r} h_i X^i \in A_{\sigma,\delta}$, then the rows of a control matrix H of $\mathcal{C}$ are given by
   $$T_f^k(h_0, \ldots, h_{n-r}, 0, \ldots, 0), \quad \text{for } 0 \leq k \leq n - 1.$$

Generic and control matrices of a (σ, δ)-codes

For $(x_0, \ldots, x_{n-1}) \in A^n$,

$$(x_0^{(0)}, \ldots, x_{n-1}^{(0)}) = (x_0, \ldots, x_{n-1}).$$
$$(x_0^{(i)}, \ldots, x_{n-1}^{(i)}) := T_f^i(x_0, \ldots, x_{n-1}) \text{ for } i \geq 0$$

Let $g(X) = \sum_0^r g_i X^i$ and $h(X) = \sum_0^{n-r} h_i X^i$. Then

f(X)=g(X)h(X) $\Rightarrow$ $G = \begin{pmatrix} x_0^{(0)} & \cdots & x_{n-1}^{(0)} \\ x_0^{(1)} & \cdots & x_{n-1}^{(1)} \\ \vdots & \vdots & \vdots \\ x_0^{(n-r-1)} & \cdots & x_{n-1}^{(n-r-1)} \end{pmatrix}$

If in addition f(X)=k(X)g(X $\Rightarrow$ $H= \begin{pmatrix} y_0^{(0)} & \cdots & y_{n-1}^{(0)} \\ y_0^{(1)} & \cdots & y_{n-1}^{(1)} \\ \vdots & \vdots & \vdots \\ y_0^{(n-1)} & \cdots & y_{n-1}^{(n-1)} \end{pmatrix}$

$(x_0^{(0)}, \ldots, x_{n-1}^{(0)}) = (g_0, \ldots, g_r, 0, \ldots, 0)$, $(y_0^{(0)}, \ldots, y_{n-1}^{(0)}) = (h_0, \ldots, h_{n-r}, 0, \ldots, 0)$.

Particular case : module θ-codes

We check that generating and control matrices of a module θ-code over a field, generating by $g(X)$ are given respectively as follows :

$$G = \begin{pmatrix} g_0 & . & . & . & g_r & 0 & 0 & \dots & 0 \\ 0 & \theta(g_0) & . & . & . & \theta(g_r) & . & . & . \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & . & . & . & \theta^{n-r-1}(g_0) & \theta^{n-r-1}(g_1) & .. & . & \theta^{n-r-1}(g_r) \end{pmatrix}$$

and

$$H = \begin{pmatrix} h_{n-r} & . & . & . & h_0 & 0 & 0 & \dots & 0 \\ 0 & \theta(h_{n-r}) & . & . & . & \theta(h_0) & . & . & . \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & . & . & . & \theta^{r-1}(h_{n-r}) & \theta^{r-1}(h_1) & .. & . & \theta^{r-1}(h_0) \end{pmatrix},$$

if $f(X) = X^n - 1 = g(X)h(X)$ as is already known in this case.

To a recursing formulas

$T_f : A^n \to A^n$ defined by :

$T_f(x_1,\dots,x_n) = (\sigma(x_1),\dots,\sigma(x_n))C_f + (\delta(x_1),\dots,\delta(x_n))$

$$(x_1^{(0)},\dots,x_n^{(0)}) = (x_1,\dots,x_n).$$

$$(x_1^{(i)},\dots,x_n^{(i)}) := T_f^i(x_1,\dots,x_n) = (\underbrace{T_f \circ \dots \circ T_f}_{\text{i times}})(x_1,\dots,x_n), \text{ for } i \geq 1$$

Lemma

For any $(x_1,\dots,x_n) \in A^n$ and $k \in \mathbb{N}$, we have :
(1) $x_1^{(k)} = \delta(x_1^{(k-1)}) - a_0\sigma(x_n^{(k-1)})$.
(2) $x_i^{(k)} = \delta(x_i^{(k-1)}) + \sigma(x_{i-1}^{(k-1)}) - a_{i-1}\sigma(x_n^{(k-1)})$, for $2 \leq i \leq n$.

A recursing formulas

We denote by $W(\sigma,\delta)_{j,k-j}$, with $0 \leq j \leq k$, the sum of **all** possible words consisting of k letters each,
j of which are σ's and $k-j$ of which are δ's.

Lemma

For any $(x_1,\ldots,x_n) \in A^n$ *with* $x_{s+1} = \cdots = x_n = 0$ *for some* $1 \leq s \leq n-1$*, we have the following (for* $1 \leq k \leq n-s$*) :*
(1) If $1 \leq i \leq k$*, then* $x_i^{(k)} = \sum_{j=0}^{i-1} W(\sigma,\delta)_{j,k-j}(x_{i-j})$*.*
(2) If $1 \leq k < i$*, then* $x_i^{(k)} = \sum_{j=0}^{k} W(\sigma,\delta)_{j,k-j}(x_{i-j})$*.*

Theorem

Let $f(X) = g(X)h(X)$, $\mathcal{C} = (g)_l/(f)_l$ *with :*
$g(X) = g_0 + \cdots + g_r X^r$, $h(X) = h_0 + \cdots + h_{n-r}X^{n-r} \in A_{\sigma,\delta}$.

$$G = \begin{pmatrix} g_0 & \dots & g_r & 0 & \dots & 0 \\ g_0^{(1)} & \dots & g_r^{(1)} & g_{r+1}^{(1)} & \dots & g_{n-1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_0^{(n-r-1)} & \dots & g_r^{(n-r-1)} & g_{r+1}^{(n-r-1)} & \dots & g_{n-1}^{(n-r-1)} \end{pmatrix}$$

if in addition $f(X) = k(X)g(X)$ *with* $k(X) \in A_{\sigma,\delta}$ *then a control matrix* H *of* $\mathcal{C}$ *is given by :*

$$H = \begin{pmatrix} h_0 & \dots & h_{n-r} & 0 & \dots & 0 \\ h_0^{(1)} & \dots & h_{n-r}^{(1)} & h_{n-r+1}^{(1)} & \dots & h_{n-1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_0^{(n-1)} & \dots & h_{n-r}^{(n-1)} & h_{n-r+1}^{(n-1)} & \dots & h_{n-1}^{(n-1)} \end{pmatrix}$$

Where

(i) $g_i^{(k)} = \sum_{j=0}^{i-1} W(\sigma,\delta)_{j,k-j}(g_{i-j})$ for $0 \leq i \leq k-1 \leq n-r-1$,

(ii) $g_i^{(k)} = \sum_{j=0}^{k} W(\sigma,\delta)_{j,k-j}(g_{i-j})$ for $0 \leq k < i+1 \leq n-r-1$,

and

(i) $h_i^{(k)} = \sum_{j=0}^{i-1} W(\sigma,\delta)_{j,k-j}(h_{i-j})$ for $0 \leq i \leq k-1 \leq r+1$,

(ii) $h_i^{(k)} = \sum_{j=0}^{k} W(\sigma,\delta)_{j,k-j}(h_{i-j})$ for $0 \leq k < i+1 \leq r+1$.

Lemma

For any $(x_1, \ldots, x_n) \in A^n$ *with* $x_{s+1} = \cdots = x_n = 0$ *for some* $1 \leq s \leq n-1$*, we have :*
(1) $x_{s+i}^{(i)} = \sigma^i(x_s)$ *for* $1 \leq i < n - s$*.*
(2) $x_{s+j}^{(i)} = 0$ *for* $1 \leq i < j \leq n - s$*.*

A general form of generating and control matrices

$$G = \begin{pmatrix} g_0 & \dots & g_r & 0 & \dots & 0 \\ g_0^{(1)} & \dots & g_r^{(1)} & \sigma(g_r) & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_0^{(n-r-1)} & \dots & g_r^{(n-r-1)} & g_{r+1}^{(n-r-1)} & \dots & \sigma_{n-1}(g_r) \end{pmatrix}$$

if in addition $f(X) = k(X)g(X)$ with $k(X) \in A_{\sigma,\delta}$ then H is given by :

$$H = \begin{pmatrix} h_0 & \dots & h_{n-r} & 0 & \dots & 0 \\ h_0^{(1)} & \dots & h_{n-r}^{(1)} & \sigma(h_{n-r}) & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_0^{n-r-1} & \dots & h_{n-r}^{n-r-1} & h_{n-r+1}^{n-r-1} & \dots & \sigma^{n-r-1}(h_{n-r}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_0^{n-1} & \dots & h_{n-r}^{n-1} & h_{n-1}^{n-r-1} & \dots & \sigma^{n-1}(h_{n-r}) \end{pmatrix}$$

The last $r-1$ columns of H are A-free so $rk(H) \geq r-1$

Frobenius codes

For a subset $N \subseteq A^n$, define the dual $N^\perp$ of N in A^n by :

$$N^\perp := \{x \in A^n \mid \, < x, y >= 0 \;\; \text{for all} \;\; y \in N\},$$

where $< x, y >= \sum_{i=1}^{n} x_i y_i$ for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$.

Proposition

Let A be a finite ring and N an A-submodule of A^n with $|N| = |A|^s$ for some $1 \leq s \leq n$. Then :

1. *If $B \subset N$ is an A-free set with $|B| = s$, then N is A-free of rank s with basis B.*
2. *If N is an A-submodule of A^n such that $\mid N \mid\mid N^\perp \mid = \mid A \mid^n$ and $B' \subset N^\perp$ is an A-free set with $|B'| = n - s$, then $N^\perp$ is a free A-module of rank $n - s$ and has B' as a basis.*

Definition

A (σ, δ)- code $\mathcal{C}$ length n over a finite ring A is called a ***Frobenius****(σ, δ)-code if it satisfies $\mid \mathcal{C} \mid\mid \mathcal{C}^\perp \mid = \mid A \mid^n$.*

Properties of principal (σ, δ)-Frobenius codes

In the next, we suppose that,

- $g(X) = \sum_0^r g_i X^i$ and $h(X) = \sum_0^{n-r} h_i X^i$,
- $f(X) = g(X)h(X)$ and $g(X)$ is also a right divisor of $f(X)$,
- $\mathcal{C} = (g)_l/(f)_l$ is a Frobenius (σ, δ)- code.

Corollary

If H the control matrix of $\mathcal{C}$ has r A-free columns, $H_{i_1}, \dots, H_{i_r}$, then the matrix $H_* \in M_{r\times n}(A)$, whose j^{th} row is $H^t_{i_j}$, generates $\mathcal{C}^\perp$ (which, by the way, coincides with the classical control matrix in the case of a linear code over a field .

Consequences

The matrix $H_* =$

$$\begin{pmatrix} h_{n-r} & \sigma(h_{n-r-1}) & \dots & \sigma^{n-r}(h_0) & * & \dots & * \\ 0 & \sigma(h_{n-r}) & \sigma^2(h_{n-r-1}) & \dots & \sigma^{n-r+1}(h_0) & * & \dots \\ \vdots & & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \sigma^{r-1}(h_{n-r}) & h_{n-r+1}^{(r-1)} & \dots & h_{n-1}^{(r-1)} \end{pmatrix}$$

generates $\mathcal{C}^\perp$ and it is a parity check matrix of $\mathcal{C}$ and coincides with the classical control matrix in the case of a linear code over a field. $\mathcal{C}^\perp$ is free and $rk(\mathcal{C}^\perp) = deg(g)$

Properties of (σ, δ)-Frobenius codes

Lemma

For any $(x_1, \ldots, x_n) \in A^n$ *with* $x_1 = \cdots = x_s = 0$ *for some* $1 \leq s \leq n-1$ *and* $\delta = 0$ *we have :*
(1) $x_i^{(k)} = 0$ *for* $1 \leq i \leq s + k$.
(2) $x_i^{(k)} = \sigma^k(x_{i-1})$ *for* $s + k < i \leq n$.

Properties of $(\sigma, 0)$- constacyclic Frobenius codes

In case $\delta = 0$ and $f(X) = X^n - \lambda \in A[X, \sigma]$ with λ a unit, then :

$$H = \begin{pmatrix} h_0 & h_1 & \dots & h_{n-k} & 0 & 0 & 0 \\ 0 & \sigma(h_0) & \dots & \sigma(h_{n-k-1}) & \sigma(h_{n-k}) & 0 & \dots \\ \vdots & \dots & \ddots & . & . & . & \vdots \\ 0 & 0 & \dots & \sigma^{n-k}(h_0) & \dots & \dots & \sigma^{n-k}(h_{n-k}) \\ h_0^{(n-k+1)} & h_1^{(n-k+1)} & . & \ddots & . & h_{n-2}^{(n-k+1)} & h_{n-1}^{(n-k+1)} \\ \vdots & \vdots & . & 0 & & . & . \\ & & & \vdots & \ddots & \sigma^{n-2}(h_0) & \\ h_0^{(n-1)} & h_1^{(n-1)} & \dots & 0 & \dots & 0 & \sigma^{n-1}(h_0) \end{pmatrix}$$

Application to constacyclic $(\sigma, 0)$-codes

G and H^* of $\mathcal{C}$ are given as follows :

$$G = \begin{pmatrix} g_0 & \dots & g_r & 0 & \dots & 0 \\ 0 & \sigma(g_0) & \dots & \sigma(g_r) & 0 & \dots \\ & & \ddots & & \ddots & \\ & \vdots & & & & \\ 0 & \dots & 0 & \sigma^{n-r-1}(g_0) & \dots & \sigma^{n-r-1}(g_0) \end{pmatrix}$$

$$H^* = \begin{pmatrix} h_0 & \dots & h_{n-r} & 0 & \dots & 0 \\ 0 & \sigma(h_0) & \dots & \sigma(h_{n-r}) & 0 & \dots \\ & & \ddots & & \ddots & \vdots \\ 0 & \dots & 0 & \sigma^{r-1}(h_0) & \dots & \sigma^{r-1}(h_{n-r}) \end{pmatrix}$$

$\mathcal{C}^\perp$ isgenerated by $h^* = h_0 X^{n-r} + \sigma(h_1) X^{n-r-1} + \dots + \sigma^{r-1}(h_{n-r})$

On the dual of $(\sigma, 0)$-Frobenius code

Theorem

.

1. *The dual $C^{\perp}$ of C is a principal Frobenius $(\sigma, 0)$-code of length n if and only if C is a principal Frobenius constacyclic$(\sigma, 0)$-code .i.e $\exists a \in A^{\times}$ such that $C = (g)^{a}_{n,\sigma,0}$.*
2. *In this case $C^{\perp}$ is a principal constacyclic $(\sigma, 0)$-code generated by h^{*} where $gh = X^{n} - a$. In addition $C^{\perp} = (h^{*})^{a^{*}}_{n,\sigma,0}$.*

- $h^{*} := \sum_{0}^{n-r} \sigma^{i}(h_{n-r-i})X^{i}$
- $a^{*} = \frac{\sigma^{n}(g_{0})}{g_{0}\sigma^{n-k}(g_{0})(a)}$

Self dual $(\sigma, 0)$-Frobenius code

Corollary

Let $C = (g)_{n=2k,\sigma}$ be a principal Frobenius $(\sigma, 0)$-code generated by $g(X)$ then C is self-dual if and only if

$$\forall l \in \{1, ..., n-r\}, \sum_{i=0}^{l} \sigma^{n-r-l}(g_{n-r+i-l})g_i = 0$$

Bibliography

1. D. Boucher, P. Solé, and F. Ulmer *Skew constacyclic codes over Galois rings*, Adv. Math. Comm. **2** (2008) 273-292.
2. D. Boucher, and F. Ulmer *Codes as modules over skew polynomial rings*, Lecture notes in computer science, volume 5921,(2009).
3. M. Boulagouaz and A. Leroy (σ, δ)*-codes*, Adv. Math. Comm. **7** (2013) 463–474.
4. F.J. MacWilliams and N.J.A. Solane, *The Theory of Error-Correcting Codes*, North-Holland, 1998.
5. O. Ore, *Theory of non-cummtative polynomials*, Ann. Math. **34** (1933) 480–508.

THANK YOU