(σ, δ)-codes over rings

M. **Boulagouaz** et A. **Leroy**
Université de Fès, Faculté des Sciences et Techniques, Maroc
Université d'Artois, Faculté Jean Perrin,France

Non Commutative rings and their applications
14 th-16 th June 2011
Jean Perrin Faculty, Artois University

INTRODUCTION

In this talk we will :

1. introduce the notion of (σ, δ)-codes generalizing the θ-codes as introduced by D. Boucher, F. Ulmer, W. Geiselmann...
2. show how to attach to such a code an ideal in some quotient of Ore extension.
3. give the control map .

A key role will be played by the

pseudo-linear transformations

Left sigma derivation and left skew polynomial ring

Définition

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

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

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

(b) *The* ***left*** *skew polynomial ring is defined by*

$$A[t;\sigma,\delta]_l := \{\sum_{i=1}^{n} a_i t^i / a_i \in A \text{ and } n \in N\},$$

where elements of $A[t;\sigma,\delta]_l$ are :
◇ *added as ordinary polynomials*
◇ *multiplied by the commutation law :* $ta = \sigma(a)t + \delta(a)$ *for $a \in A$.*

(c) *The degree of a nonzero polynomial*

$$f = a_0 + a_1 t + a_2 t^2 + \ldots a_n t^n \in R :$$

$$\deg(f) = max\{i | a_i \neq 0\} \text{ if } f \neq 0 \text{ and } \deg(0) = -\infty.$$

Right sigma derivation and right skew polynomial ring

Définition

with 1 *and* σ *a ring endomorphism of A.*

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

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

(b) *The* ***right*** *skew polynomial ring is defined by :*

$$A[t;\sigma,\delta]_r = \{\sum_{i=1}^{n} t^i b_j / b_j \in A \text{ and } n \in N\},$$

where elements of $A[t;\sigma,\delta]_r$ *are :*

- ◇ *added as ordinary polynomials*
- ◇ *multiplied by the commutation law :* $bt = t\sigma(b) + \delta(b)$.

Sigma derivation and skew polynomial ring

Proposition

Let A be a ring with $1, \sigma$ a ring automorphism of A and δ a left σ-derivation, of A. Then we have

(a) $\delta' := \delta\sigma^{-1}$ *is a right* σ^{-1} *derivation.*

(b) $A[t; \sigma, \delta]_l \simeq A[t; \sigma^{-1}, -\delta\sigma^{-1}]_r$.

Examples of left skew polynomial rings

(1) If $\sigma = id.$ and $\delta = 0$,
we have $A[t; \sigma, \delta]_l = A[t]$,
the usual polynomial ring in a commuting variable.

(2) If $\sigma = id$ and $\delta \neq 0$
we denote $A[t; id., \delta]_l$ as $A[t; \delta]_l$,
and speak of a polynomial ring of derivation type.

(3) if $\delta = 0$ and $\sigma \neq id.$
we write $A[t; \sigma, \delta]_l$ as $A[t; \sigma]_l$,
and refer to it as a polynomial ring of endomorphism type.

(4) $A = \mathbb{F}_{P^n}$ a finite field and, for $a \in A$, define $\theta(a) = a^p$

We get $\mathbb{F}_q[t; \theta]$ which has been used recently in the context of noncommutative codes (Boucher, Ulmer...).

Examples of left skew polynomial rings

(5) For $a \in A$

$\diamond$ we define the inner σ-derivation induced by a (denoted $d_{a,\sigma}$) in the following way :

$$d_{a,\sigma} : A \longrightarrow A$$
$$r \longrightarrow d_a(r) := ar - \sigma(r)a, \text{ for any } r \in A.$$

And we have $A[t; \sigma, d_{a,\sigma}]_l = A[t - a, \sigma]_l$.

Remark : If A is a **finite field** then all derivation on A is a $d_{a,\sigma}$.

$\diamond$ And similarly for an inner automorphism induced by $a \in U(A)$ denoted by l_a and defined by :

$$l_a : A \longrightarrow A$$
$$x \longrightarrow l_a(x) = axa^{-1}, \text{ for } x \in A.$$

And we have $A[t; l_a]_l = A[a^{-1}t]_l$.

(6) Let F be a field, $A := \{a + b\epsilon / (a, b) \in F^2 \text{ and } \epsilon^2 = 0\}$ and $\sigma(a + b\epsilon) = a - b\epsilon$. Then $\delta(a + b\epsilon) = b\epsilon$ is a σ-derivation witch is not a inner derivation $\Rightarrow A[t; \sigma, \delta]_l$.

Non commutative polynomial maps

Let A, σ and δ be a ring an endomorphism and a left-σ-derivation of A respectively.

For any monic $f(t) \in A[t;\sigma,\delta]_l$ and $a \in A$ there exists a unique $q(t) \in A[t,\sigma,\delta]_l$ and a unique $s \in A$ such that :

$$f(t) = q(t)(t-a) + s_l.$$

Définition

With these notations, polynomial map associated to $f(t) \in A[t;\sigma,\delta]_l$ is the map

$$\begin{aligned} f : A &\longrightarrow A \\ a &\longrightarrow f(a) := s. \end{aligned}$$

Non commutative polynomial maps

Let A, σ and δ be a ring an **automorphism** and a left-σ-derivation of A respectively.

For any **monic** $f(t) \in A[t;\sigma,\delta]_l$ and $a \in A$ there exists a unique $(q_l(t), q_r(t)) \in A[t,\sigma,\delta]_l^2$ and a unique $(s_l, s_r) \in A^2$ such that :

$$f(t) = q_l(t)(t-a) + s_l.$$
$$f(t) = (t-a)q_r(t) + s_r.$$

Définition

With these notations, polynomial maps associated to $f(t) \in A[t;\sigma,\delta]_l$ *are maps*

$$f_l : A \longrightarrow A \qquad\qquad f_r : A \longrightarrow A$$
$$a \longrightarrow f_l(a) := s_l. \qquad\qquad a \longrightarrow f_r(a) := s_r.$$

✓ Hereafter we denote f_l by **f**.
✓ For $i \geq 0$, we denote N_i the polynomial map determined by t^i.

Left pseudo-linear transformation

Let A, σ, δ and V be a ring an endomorphism, a σ-derivation of A and a left A-module respectiveley.

Définition

An additive map $T : V \longrightarrow V$ such that :

$$(\forall \alpha \in A)(\forall v \in V) :$$

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v$$

is called a left (σ, δ) pseudo-linear transformation (or a left (σ, δ)-PLT).

Examples : If $a \in A$ the map :

$$T_a : A \longrightarrow A$$
$$x \mapsto T_a(x) = \sigma(x)a + \delta(x)$$

is a (σ, δ)-PLT defined on ${}_AA$.

- $\diamond$ if $\sigma = id$ and $\delta = 0$ we get $T_a(x) = xa$.
- $\diamond$ if $a = 0$ we get $T_0 = \delta$
- $\diamond$ if $a = 1$ and $\delta = 0$ we get that $T_1 = \sigma$.

Examples

Let A, σ, δ and V be a ring an endomorphism, a σ-derivation of A and a left A-module respectiveley.

Let : $\diamond V$ be a free left A-module with basis $\beta = \{e_1, \ldots, e_n\}$
$\diamond T : V \longrightarrow V$ be a (σ, δ)-PLT.
$\diamond T(e_i) = \sum_i^n c_{ij} e_j$
$\diamond C_T = (c_{ji}) \in M_n(A)$.
$\diamond$ For $(a_1 ... a_n) \in M_{(1,n)}(A)$ put $v_{(a_1 ... a_n)} = (a_1, ..., a_n) \in A^n$.

Then :

$$T_C : A^n \longrightarrow A^n.$$
$$(a_1, ..., a_n) \longrightarrow T_C(a_1, ..., a_n) := v_{(\sigma(a_1)...\sigma(a_n))C} + (\delta(a_1), ..., \delta(a_n)).$$
is a left (σ, δ)-PLT on the left A-module A^n.

The left pseudo-linear transformation associated to a monic polynomial

A useful example : the pseudo-linear transformation associated to a given monic polynomial f of degree n (or rather to its companion matrix C_f) :

Proposition-Définition

*Let $f \in A[t;\sigma,\delta]$ be a monic polynomial of degree **n** and C_f its companion matrix. Then the map*

$$T_f : A^n \longrightarrow A^n.$$
$$(a_1, ..., a_n) \longrightarrow T_f(a_1, ..., a_n) := v_{(\sigma(a_1)...\sigma(a_n))C_f} + (\delta(a_1), ..., \delta(a_n)).$$

is a pseudo-linear transformation.

T_f is called the left pseudo-linear transformation associated to the monic polynomial f.

Right pseudo-linear transformation

Let A, σ, δ and V be a ring an endomorphism, a right-σ-derivation of A and a right A-module respectively.

Définition

An additive map $T : V \longrightarrow V$ such that :

$$(\forall \alpha \in A)(\forall v \in V) :$$

$$T(v\alpha) = T(v)\sigma(\alpha) + v\delta(\alpha)$$

is called a (δ, σ) pseudo-linear transformation (or a (δ, σ)-PLT).

Examples :

If $a \in A$ the map :

$$\begin{aligned} {}_aT : A &\longrightarrow A \\ x &\mapsto T_a(x) = a\sigma(x) + \delta(x) \end{aligned}$$

is a (σ, δ)-PLT defined on ${}_AA$.

- $\diamond$ if $\sigma = id$ and $\delta = 0$ we get ${}_aT(x) = ax$.
- $\diamond$ if $a = 0$ we get $T_0 = \delta$

Examples

Let A, σ, δ and V be a ring an endomorphism, a right-σ-derivation of A and a right A-module respectively.

Let : $\diamond V$ be a free right A-module with basis $\beta = \{e_1, \ldots, e_n\}$
$\diamond T : V \longrightarrow V$ be a (δ, σ)-PLT.
$\diamond T(e_i) = \sum_i^n e_j c_{ji}$
$\diamond {}_T C = (c_{ij}) \in M_n(A)$.
$\diamond$ For $(a_1 ... a_n) \in M_{(1,n)}(A)$ put :
$\checkmark v_{(a_1 ... a_n)} = (a_1, ..., a_n) \in A^n$.
$\checkmark {}^t(a_1 ... a_n)$ the transpose matrix of $(a_1 ... a_n)$.

Then :

$${}_C T : A^n \longrightarrow A^n.$$
$$(a_1, ..., a_n) \longrightarrow {}_C T(a_1, ..., a_n) := C({}^t v_{(\sigma(a_1) ... \sigma(a_n))}) + (\delta(a_1), ..., \delta(a_n)).$$
is a (σ, δ)-PLT on the left A-module A^n.

The right pseudo-linear transformation associated to a monic polynomial

A useful example : the pseudo-linear transformation associated to a given monic polynomial f of degree n (or rather to its companion matrix C_f) :

Proposition-Définition

*Let $f \in A[t;\sigma,\delta]_l$ be a monic polynomial of degree **n** and C_f its companion matrix. Then the map*

$$ {}_fT : A^n \longrightarrow A^n.$$
$$(a_1,...,a_n) \longrightarrow_f T(a_1,...,a_n) := v_f C(^t(\sigma(a_1)...\sigma(a_n))) + (\delta(a_1),...,\delta(a_n)).$$

is a right pseudo-linear transformation.

${}_fT$ is called the right pseudo-linear transformation associated to the monic polynomial f.

Link between the pseudo-linear transformation and polynomial map

Example :
For $a \in A$ the map :

$$T_a : A \longrightarrow A$$
$$x \longrightarrow T_a(x) = \sigma(x)a + \delta(x)$$

is the pseudo-linear transformation associated to $f(t) = t - a$.

Proposition

Let $a \in A$ and $p(t) \in A[t; \sigma, \delta]$.

$$p(T_a)(1) = p(a).$$

In what follows we denote $A[t, \sigma, \delta]_l$ by $A[t, \sigma, \delta]$.

(σ, δ)-codes

Let A be a ring, σ, δ be an endomorphism and σ derivation of A respectively.

Proposition

Let $f \in R = A[t; \sigma, \delta]$ be a monic polynomial of degree $n > 0$.
The map

$$\begin{aligned} \varphi_f : R/Rf &\longrightarrow A^n \\ p + Rf &\longrightarrow \varphi_f(p + Rf) := p(T_f)(1, 0, \ldots, 0) \end{aligned}$$

is a bijection.

φ_f shows how to translate results from the R/Rf to A^n if $n = \deg(f)$.

Définition

Let f be a monic invariant polynomial in $R = A[t; \sigma, \delta]$.
A (σ, δ)-polynomial code $C(t)$ is a left principal ideal I of R/Rf.
A (σ, δ)-word code C in A^n is the image of a (σ, δ)-polynomial code via the map φ_f described in the above proposition.

(σ, δ)-codes and their generic matrices

Let f be a **monic invariant polynomial** in $R = A[t; \sigma, \delta]$.
$\diamond$ For a left principal ideal I of R/Rf there exists $g(t) = \sum_{i=0}^{r} g_i t^i \in R$ such that $I = Rg/Rf$
$\diamond$ there exists $h \in R$ such that $f = gh$.

Théorème

With the above notations we have :

(a) *The code C_g corresponding to $C_g(t) := Rg/Rf$ is of dimension $n - r$ where $\deg(f) = n$ and $\deg(g) = r$.*

(b) *If $v := (a_0, a_1, \ldots, a_{n-1}) \in C_g$ then $T_f(v) \in C_g$.*

(c) *The rows of the generic matrix of C_g are given by $(T_f)^k(g_0, g_1, \ldots, g_r)$ for $1 \leq k \leq n - r$.*

Examples of (σ, δ)-codes.

Examples :

Let $A = \mathbb{F}_{p^n}$ a finite field.

1. If $\sigma = Id.$, $\delta = 0$, $f = t^n - 1$ and $f = gh$
   - ◇ get back the usual cyclic codes
   - ◇ (b) gives the cyclicity condition for the code.
2. If $\sigma = Id.$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$
   - ◇ get back the usual constacyclic codes
   - ◇ (b) gives the constacyclicity condition for the code.
3. $f = t^n - 1 \in R = \mathbb{F}_q[t; \theta]$ ($\theta =$ "*Frobenius*") and $f = gh \in R$
   - ◇ We get back θ-cyclic codes.
   - ◇ Again (b) above gives "θ-cyclicity".
4. If $\sigma = \theta$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$
   - ◇ get back the usual θ-constacyclic codes
   - ◇ (b) gives the θ-constacyclicity condition for the code.

Examples of (σ, δ)-codes.

Examples :

(5) $R = \mathbb{F}_p[x]/(X^p)[t; id., \delta]$ where δ is defined by $\delta(x) = x$. $f(t) = t^p - t$ is central. $f = gh$ we get "derivative codes".

(6) Let A be a ring and $R = A[x][t\ , id\ , X^2\frac{d}{dX}\ ]$. We have

$$f(t) = t^2 = (t - X)(t + X) \neq (t + X)(t - X).$$

This shows that we have more factorizations than "usually".

(7) Let $A := \mathbb{F}_3[X]/(X^6)$ and consider $R := A[t\ , id\ , X^2\frac{d}{dX}\ ]$. t^3 is a central polynomial and, writing $x := X + (X^6)$, we have $t^3 = (t + x)t(t - x)$. We can thus consider the code given by $f = t^3$ and $g = t(t - x)$

(8) In $\mathbb{F}_p[X][t\ , id\ , X^2\frac{d}{dX}\ ]$ we have $f(t) = t^p$ is central and $f(ix) = 0$ for $0 \leq i < p$ we then get factorizations of f leading to different codes. Here we can replace $\mathbb{F}_p[X]$ by $\mathbb{F}_p[X^p]/(X^n)$ for any $n > 1$, getting a finite ring as an alphabet.

Control matrix of a (σ, δ)-codes

Property (b) in the above theorem :

$$\text{If } v := (a_0, a_1, \ldots, a_{n-1}) \in C_g \text{ then } T_f(v) \in C_g.$$

characterizes the codes that can be obtained using a factor of an invariant polynomial f.

What is a control matrix for the (σ, δ)-code C_g corresponding to the left ideal $C_g(t) := Rg/Rf$?.

Key lemma :

Lemme

If $C_g(t) := Rg/Rf$ and $h \in R$ such that $f = gh$ then :

$$C_g(t) = lann_{R/Rf} h.$$

Correspondence between right modules and right pseudo-linear transformations

Let A be a ring, σ, δ be an endomorphism and σ derivation of A respectively. Let $f = \sum_{i=0}^{n} t^i a_i$ be an invariant monic polynomial. Then we have that the right action of t on $A^n \simeq R/fR$ is given by :

${}_fT \in End(R/fR, +) \simeq End(A^n, +)$ defined by

$$(a_1, ..., a_n).t == v_{{}_fC(^t(\sigma^{-1}(a_1)...\sigma^{-1}(a_n)))} + (\delta'(a_1), ..., \delta'(a_n)),$$

Where $\delta' = \delta\sigma^{-1}$
and ${}_fC$ stands for the matrix :

$$\begin{pmatrix} 0 & 0 & \dots & \dots & -a_0 \\ 1 & 0 & \dots & \dots & -a_1 \\ 0 & 1 & \dots & \dots & -a_2 \\ 0 & 0 & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -a_{n-1} \end{pmatrix}$$

Correspondence between right modules and right pseudo-linear transformations

One way of obtaining the code as a kernel is to look at the right A structure of R/Rf.

Let A be a ring, σ, δ be an automorphism and σ derivation of A respectively.

Lemme

Let $f \in R = A[t; \sigma, \delta]$ be a monic invariant polynomial of degree n. Then :

(a) $fa = \sigma^n(a)f$ *for all* $a \in A$.

(b) $ft = (t + c)f$ *where* $c \in A$ *is such that* $cf_0 + \delta(f_0) = 0$.

(c) $\sigma^n\delta - \delta\sigma^n = \delta_{c,\sigma^n}$.

Correspondence between right modules and right pseudo-linear transformations

Let A be a ring, σ, δ be an automorphism and σ derivation of A respectively.
From the basic relation $ta = \sigma(a)t + \delta(a)$ *for* $a \in A$, we get :

- $\diamond$ $at = t\sigma^{-1}(a) - \delta\sigma^{-1}(a)$.
- $\diamond$ $\delta' := \delta\sigma^{-1}$ is a right σ^{-1} derivation, i.e.

$$\delta'(ab) = \delta'(a)\sigma^{-1}(b) + a\delta'(b).$$

$\diamond$ There is a one one correspondence between right R-modules and some right (σ^{-1}, δ')-pseudo-linear transformations.

$\diamond$ If V_R is a right R-module the action of t on V gives rise to a map $T \in End(V, +)$ such that

$$T(v\alpha) = T(v)\sigma^{-1}(\alpha) + v\delta'(\alpha).$$

(σ, δ)-codes and their control map

Let $f = \sum_{i=0}^{n} t^i a_i$, the right action of t on R/fR is given by :

$$(a_1, ..., a_n).t = v_f C({}^t(\sigma^{-1}(a_1)...\sigma^{-1}(a_n))) + (\delta'(a_1), ..., \delta'(a_n)),$$

Where $\delta' = \delta\sigma^{-1}$.

The following theorem gives a control map for the code C_g.

Théorème

Let $f = gh \in R$ be as above. Then, writing $h = \sum_{i=0}^{l} t^i h_i$.
Then we have

$$c = \sum_{i=0}^{l} t^i p_i \in C_g \Leftrightarrow, h({}_f T)(c) = 0$$

$$C_g = \ker h({}_f T) = \ker(\sum_{i=0}^{l} ({}_f T^i) h_i).$$

Coding with Wedderburn polynomials

We now define a code as the multiple of a Wedderburn polynomial.

Définition

(a) $g \in R = A[t;\sigma,\delta]$ *monic is Wedderburn if there exist* $\{a_1,\ldots,a_r\} \subseteq A$ *such that*
- $\diamond\ g = [t - a_i | i = 1,\ldots,r]$
- $\diamond\ \deg g = r.$

(b)

$$V_{n\times r}(a_1,\ldots,a_r) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ a_1 & a_2 & \ldots & a_r \\ N_2(a_1) & N_2(a_2) & \ldots & N_2(a_r) \\ \ldots & \ldots & \ldots & \ldots \\ N_{n-1}(a_1) & \ldots & \ldots & N_{n-1}(a_r) \end{pmatrix}$$

If $f(t) = \sum_{i=0}^{n} c_i t^i \in A[t;\sigma,\delta]$ we then get :
$$(f(a_1)\ldots f(a_r)) = (c_0.c_1\ldots c_{n-1})V_{n\times r}(a_1\ldots a_r).$$

(σ, δ) g-polynomial code

Définition

Let $g \in R = A[t; \sigma, \delta]$ of degre r. A (σ, δ) g-polynomial code C is the set of n-tuples, $n > r$, in A^n corresponding to the coefficients of polynomials in Rg of degree $\leq n - 1$.

We collect in the following proposition basic properties

Proposition

Let $g \in R = A[t; \sigma, \delta]$ be a Wedderburn polynomial and C the corresponding. Then

(a) *The generating matrix of a (σ, δ) $g =$-polynomial code C is given by the coefficients of $g(t), tg(t), \ldots, t^{n-r-1}g(t)$.*

(b) *$(c_0, c_1, \ldots, c_{n-1}) \in C$ if and only if $(c_0.c_1.\ldots.c_{n-1})V_{n\times r}(a_1.\ldots.a_r) = (0.\ldots.0)$, where $V_{n\times r}(a_1, \ldots, a_r)$ denotes the generalized vandermonde matrix based on $a_1, \ldots, a_r$*

THANK YOU