Title

Coding and Ore extensions

André Leroy, Université d'Artois, France

Tehran, January 2019

Joint work with A. Alahmadi, A. Boulagouaz, A. Cherchem

Outlines

1. Ore polynomials
2. Definition and examples
3. Properties and roots
4. PLT, counting the roots
5. Ore Frobenius extensions
6. untwisting and examples
7. Classical codes
8. Skew codes
9. Generating and control matrices
10. Boucher Ulmer's work
11. Skew exponents
12. Concluding remarks

Ore Polynomials, Definitions and examples

A a ring, $S \in End(A)$, D a S-derivation:

$$D \in End(A,+) \qquad D(ab) = S(a)D(b) + D(a)b, \forall a, b \in A.$$

For $a \in A$, L_a left multiplication by a.
In $End(A,+)$, we then have : $D \circ L_a = L_{S(a)} \circ D + L_{D(a)}$.
Define a ring $R := A[t; S, D]$; Polynomials $f(t) = \sum_{i=0}^{n} a_i t^i \in R$.
Degree and addition are defined as usual, the product is based on:

$$\forall a \in A, \quad ta = S(a)t + D(a).$$

Examples

Examples

1) If $S = id.$ and $D = 0$ we get back the usual polynomial ring $A[x]$.
2) If $a \in A$ $D_a(x) = xa - s(x)a$ defines a S-derivation.
3) $R = \mathbb{C}[t; S]$ where S is the complex conjugation. If $x \in \mathbb{C}$ is such that $S(x)x = 1$ then

$$t^2 - 1 = (t + S(x))(t - x)$$

. On the other hand $t^2 + 1$ is central and irreducible in R.
4) K a field, $q \in K \setminus \{0\}$ and $S \in End_K(K[x])$ defined by $S(x) = qx$. $R = K[x][y; S]$. Commutation rule: $yx = qxy$.

properties

Facts Let K be a division ring.

a) Ore (1933): $R = K[t; S, D]$ is a left principal ideal domain.

b) Ore (1933): $R = K[t; S, D]$ is a unique factorization domain: If $f(t) = p_1(t) \dots p_n(t) = q_1(t) \dots q_m(t)$, $p_i(t), q_i(t)$ irreducible then $m = n$ and there exists $\sigma \in \mathcal{S}_n$ such that,

$$\text{For } 1 \leq i \leq n, \qquad \frac{R}{Rq_i} \cong \frac{R}{Rp_{\sigma(i)}}$$

PLT

Definitions

Let A be a ring, S an endomorphism of A and D a S-derivation of A. Let also V stand for a left A-module.

a) An additive map $T : V \longrightarrow V$ such that, for $\alpha \in A$ and $v \in V$,

$$T(\alpha v) = S(\alpha)T(v) + D(\alpha)v.$$

is called an (S, D) pseudo-linear transformation (or a (S, D)-PLT, for short).

b) For $f(t) \in R = A[t; S, D]$ and $a \in A$, we define $f(a)$ to be the only element in A such that $f(t) - f(a) \in R(t - a)$.

Proposition

Let A be a ring $S \in End(A)$ and D a S-derivation of A. For an additive group $(V, +)$ the following conditions are equivalent:

(i) *V is a left $R = A[t; S, D]$-module;*

(ii) *V is a left A-module and there exists an (S, D) pseudo-linear transformation $T : V \longrightarrow V$;*

(iii) *There exists a ring homomorphism $\Lambda : R \longrightarrow End(V, +)$.*

Proposition

Let A be a ring $S \in End(A)$ and D a S-derivation of A. For an additive group $(V,+)$ the following conditions are equivalent:

(i) *V is a left $R = A[t; S, D]$-module;*

(ii) *V is a left A-module and there exists an (S, D) pseudo-linear transformation $T : V \longrightarrow V$;*

(iii) *There exists a ring homomorphism $\Lambda : R \longrightarrow End(V,+)$.*

Corollary

For any $f, g \in R = A[t; S, D]$ and any pseudo-linear transformation T we have: $(fg)(T) = f(T)g(T)$.

Example

For $a \in A$, $T_a \in End(A,+)$ is defined by

$$T_a(x) = S(x)a + D(x) \quad \forall x \in V.$$

1. $T_0 = D$, $T_1 = S + D$.
2. For $B \in M_n(A)$ we can define 2 different PLT's
    - $T_B : A^n \longrightarrow A^n : x \mapsto S(x)B + D(x)$
    - $T'_B : M_n(A) \longrightarrow M_n(A) : C \mapsto S(C)B + D(C)$

For $a \in A$ and c invertible in A we define
$a^c = S(c)ac^{-1} + D(c)c^{-1}$ For $a \in A$, we also define

$$\Delta(a) = \{a^c \mid c \in U(A)\}, \quad C_{S,D}(a) = \{c \in A \mid a^c c = ac\}$$

For $a \in A$ and c invertible in A we define $a^c = S(c)ac^{-1} + D(c)c^{-1}$ For $a \in A$, we also define

$$\Delta(a) = \{a^c \mid c \in U(A)\}, \quad C_{S,D}(a) = \{c \in A \mid a^c c = ac\}$$

Link between $\ker f(T_a)$ and (right) roots of $f(t)$?

Theorem

(a) *$f(T_a)(1) = f(a)$.*

(b) *For $f, g \in R$, $fg(a) = f(T_a)(g(a))$.*

(c) *For $a, c \in A$ with $c \in U(A)$, we have $(t-b)c = S(c)(t-a)$ where $b = a^c$).*

(d) *$C_{S,D}$ is a ring.*

(e) *T_a is left $C_{S,D}(a)$-linear.*

We define

$$E(f,a) := \ker f(T_a)$$

If $A = K$ is a division ring we have

$$E(f,a) = \{0 \neq b \in K \mid f(a^b) = 0\} \cup \{0\}$$

We define

$$E(f,a) := \ker f(T_a)$$

If $A = K$ is a division ring we have

$$E(f,a) = \{0 \neq b \in K \mid f(a^b) = 0\} \cup \{0\}$$

K a division ring. $a \in K$, $R = K[t;S,D]$, K a division ring.
$\Delta(a) := \{a^c = S(c)ac^{-1} + D(c)c^{-1} \mid 0 \neq c \in K\}$.

Theorem

Let $f(t) \in R = K[t;S,D]$ be of degree n. We have

(a) *The roots of $f(t)$ belong to at most n conjugacy classes, say $\Delta(a_1), \dots, \Delta(a_r)$; $r \leq n$ (Gordon Motzkin in "classical" case).*

(b) $\sum_{i=1}^{r} dim_{C_i} \ker f(T_{a_i}) \leq n$, *where* $C_i = C(a_i) := \{0 \neq x \in K \mid a_i^x = a_i\} \cup \{0\}$

Theorem

let p be a prime number, $\mathbb{F}_q$ a finite field with $q = p^n$ elements, θ the Frobenius automorphism ($\theta(x) = x^p$). Then:

a) *There are p distinct classes of θ-conjugation in $\mathbb{F}_q$.*

b) $0 \neq a \in \mathbb{F}_q$ *we have* $C^\theta(a) = \mathbb{F}_p$ *and* $C^\theta(0) = \mathbb{F}_q$.

c) $R = \mathbb{F}_q[t;\theta]$,

$$G(t) := [t - a \,|\, a \in \mathbb{F}_q]_l = t^{(p-1)n+1} - t$$

. *We have* $RG(t) = G(t)R$.

The polynomial $G(t)$ in the above theorem is the analogue of $x^q - x \in \mathbb{F}_q[x]$.

Untwisting, I

1. If $S = Inn(u)$, $u \in U(A)$, $A[t; I_a; D] = A[u^{-1}t; D]$
2. If there exists $c \in Z(a)$, the center of A, such that $u := c - S(c) \in U(A)$ then $A[t; S, D] = A[t - d; S]$, where $d = u^{-1}D(c)$.

For a prime p and an integer $i \geq 1$, we define $[i] := \frac{p^i - 1}{p-1} = p^{i-1} + p^{i-2} + \cdots + 1$ and put $[0] = 0$.
For $n \geq 1$ we denote $q = p^n$. Let us introduce the following subset of $\mathbb{F}_q[x]$:

$$\mathbb{F}_q[x^{[]}] := \{\sum_{i \geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$$

A polynomial belonging to this set will be called a $[p]$-polynomial.
We extend θ to the ring $\mathbb{F}_q[x]$ and put $\theta(x) = x^p$ i.e. $\theta(g) = g^p$ for all $g \in \mathbb{F}_q[x]$. We thus have $R := \mathbb{F}_q[t; \theta] \subset S := \mathbb{F}_q[x][t; \theta]$.

Untwisting, II

Considering $f \in R := \mathbb{F}_q[t;\theta]$ as an element of $\mathbb{F}_q[x][t;\theta]$ we can evaluate f at x. Denote $f^{[]}[x] \in \mathbb{F}_q[x]$ i.e. $f(t)(x) = f^{[]}(x)$.

Untwisting, II

Considering $f \in R := \mathbb{F}_q[t;\theta]$ as an element of $\mathbb{F}_q[x][t;\theta]$ we can evaluate f at x. Denote $f^{[]}[x] \in \mathbb{F}_q[x]$ i.e. $f(t)(x) = f^{[]}(x)$.

Theorem

Let $f(t) = \sum_{i=0}^{n} a_i t^i$ be a polynomial in $R := \mathbb{F}_q[t;\theta] \subset S := \mathbb{F}_q[x][t;\theta]$. With the above notations we have:

1) *For any $h = h(x) \in \mathbb{F}_q[x]$, $f(h) = \sum_{i=0}^{n} a_i h^{[i]}$.*
2) $\{f^{[]} | f \in R = \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{[]}]$.
3) *For $i \geq 0$ and $h(x) \in \mathbb{F}_q[x]$ we have $T_x^i(h) = h^{p^i} x^{[i]}$.*
4) *For any $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ if and only if $f^{[]}(x) \in \mathbb{F}_q[x]h^{[]}(x)$.*

Corollary

A polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ is irreducible if and only if its attached $[p]$-polynomial $f^{[]} \in \mathbb{F}_q[x^{[]}] \subset \mathbb{F}_q[x]$ has no non trivial factor belonging to $\mathbb{F}_q[x^{[]}]$.

Examples

Consider $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$ where $a^2 + a + 1 = 0$.
$\theta(a) = a^2 = a + 1$; $\theta(a + 1) = (a + 1)^2 = a$.

a) $f(t) = t^3 + a \in \mathbb{R} = F_4[t; \theta]$, we compute $f^{[]} = x^7 + a \in \mathbb{F}_4[x]$. Since $a^7 + a = 0$, a is also a root of $t^3 + a$ and $t^3 + a = (t^2 + at + 1)(t + a)$ in R. We have $(t^2 + at + 1)^{[]} = x^3 + ax + 1 \in \mathbb{F}_4[x]$ is irreducible. We conclude that $t^3 + a = (t^2 + at + 1)(t + a)$ is a factorisation into irreducible polynomials.

Examples

Consider $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$ where $a^2 + a + 1 = 0$.
$\theta(a) = a^2 = a + 1;\ \theta(a + 1) = (a + 1)^2 = a$.

a) $f(t) = t^3 + a \in \mathbb{R} = F_4[t;\theta]$, we compute $f^{[]} = x^7 + a \in \mathbb{F}_4[x]$. Since $a^7 + a = 0$, a is also a root of $t^3 + a$ and $t^3 + a = (t^2 + at + 1)(t + a)$ in R. We have $(t^2 + at + 1)^{[]} = x^3 + ax + 1 \in \mathbb{F}_4[x]$ is irreducible. We conclude that $t^3 + a = (t^2 + at + 1)(t + a)$ is a factorisation into irreducible polynomials.

b) Consider $f(t) = t^4 + (a+1)t^3 + a^2t^2 + (1+a)t + 1 \in \mathbb{F}_4[t;\theta]$. $f^{[]} = x^{15}+(a+1)x^7+(a+1)x^3+(1+a)x+1 = (x^{12}+ax^{10}+x^9+(a+1)x^8+(a+1)x^5+(a+1)x^4+x^3+ax^2+x+1)(x^3+ax+1)$ The last factor corresponds to $t^2 + at + 1 \in \mathbb{F}_4[t;\theta]$ is irreducible in $\mathbb{F}_4[t;\theta]$. We then easily conclude that $f(t) = (t^2 + t + 1)(t^2 + at + 1)$ is a decomposition of $f(t)$ into irreducible factors in $\mathbb{F}_4[t;\theta]$.

One more example:
Let us consider the polynomial $f(t) = t^5 + at^4 + (1+a)t^3 + at^2 + t + 1$. Its attached $[p]$-polynomial is $x^{31} + ax^{15} + (1+a)x^7 + ax^3 + x + 1$. It is easy to remark that a is a root and we get $f(t) = q_1(t)(t+a)$ in $\mathbb{F}_4[t;\theta]$ where $q_1(t) = t^4 + (a+1)(t^2+t+1)$. The $[p]$-polynomial attached to $q_1(t)$ is $x^{15} + (a+1)(x^3+x+1)$. Again we get that a is a root and we obtain that $q_1(t) = (q_2(t))(t+a)$ in $\mathbb{F}_4[t;\theta]$ where $q_2(t) = t^3 + (a+1)t^2 + at + a$. The $[p]$-polynomial attached to $q_2(t)$ is $x^7 + (a+1)x^3 + ax + a$. Once again a is a root and we have $q_2(t) = (t^2+t+1)(t+a)$. Since t^2+t+1 is easily seen to be irreducible in $\mathbb{F}_4[t;\theta]$, we have the following factorization of our original polynomial:
$f(t) = (t^2+t+1)(t+a)^3$. We can also factorize $f(t)$ as follows:
$f(t) = (t+a+1)(t+1)(t+a)(t^2+(a+1)t+1)$.

Classical codes, I

Let A be a set and $n \in N$. A code of length n c is a subset $C \subseteq A^n$.
Classically, $A = \mathbb{F}_q$. The code is linear if C is a subspace of $\mathbb{F}_q^n$.
For $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in C$ defne $d(a, b) = |\{i \mid a_i \neq b_i\}|$.
The minimal distance of C is $d = d_C = min\{d(a, b)|a, b \in C\}$.
Such a code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.
$\mathbb{F}_q^n$ has a structure of $\mathbb{F}_q[x]$ module via $x.(a_1, \dots, a_n) = (a_n, a_1, \dots, a_{n-1})$ and as such is isomorphic to $\mathbb{F}_q[x]/(x^n - 1)$.

Classical codes, I

Let A be a set and $n \in N$. A code of length n c is a subset $C \subseteq A^n$.
Classically, $A = \mathbb{F}_q$. The code is linear if C is a subspace of $\mathbb{F}_q^n$.
For $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in C$ defne $d(a, b) = |\{i \mid a_i \neq b_i\}|$.
The minimal distance of C is $d = d_C = min\{d(a, b)|a, b \in C\}$.
Such a code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.
$\mathbb{F}_q^n$ has a structure of $\mathbb{F}_q[x]$ module via $x.(a_1, \ldots, a_n) = (a_n, a_1, \ldots, a_{n-1})$ and as such is isomorphic to $\mathbb{F}_q[x]/(x^n - 1)$. A linear code C is cyclic if $(a_1, a_2, \ldots, a_n) \in C \Rightarrow (a_n, a_1, \ldots, a_{n-1}) \in C$. C is then a $\mathbb{F}_q[x]$ submodule of $\mathbb{F}_q^n$ and $ann_{\mathbb{F}_q[x]} C = (X^n - 1)$. Hence C is isomorphic to a submodule of $\mathbb{F}_q[x]/(x^n - 1)$ and there exists $g(x) = \sum_{i=0}^r a_i x^i \in \mathbb{F}_q[x]$ dividing $x^n - 1$ such that $C \cong g(x)\mathbb{F}_q[x]/(x^n - 1)$.

Classical codes, II

The code C is of dimension $k = n - r$ and a generating matrix $G \in M_{k,n}(\mathbb{F}_q)$ for C is then of the form:

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & 0 \\ 0 & a_0 & \dots & a_{r-1} & a_r & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix} \in M_{n-r,n}(\mathbb{F}_q).$$

Classical codes, II

The code C is of dimension $k = n - r$ and a generating matrix $G \in M_{k,n}(\mathbb{F}_q)$ for C is then of the form:

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & 0 \\ 0 & a_0 & \dots & a_{r-1} & a_r & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix} \in M_{n-r,n}(\mathbb{F}_q).$$

Definition

1. $C^\perp := \{x \in \mathbb{F}_q^n \mid x.c = 0, \forall c \in C\}$.
2. For $h(x) = \sum_{i=0}^{l} h_i x^i$ the reciprocal polynomial is $h^*(x) = x^l h(\frac{1}{x})$.

If C is cyclic genearted by $g(x)$ and $h(x)$ is such that $g(x)hx) = x^n - 1$ then $C^\perp$ is also cyclic with generating polynomial $h^*(x)$.

Skew codes, I

Let A be a ring, S, D be an endomorphism and a S-derivation of A respectively.

Proposition

Let $f(t) \in R = A[t; S, D]$ be a monic polynomial of degree $n > 0$. The map $\varphi : R/Rf(t) \longrightarrow A^n$ given by $\varphi(p + Rf) = p(T_f)(1, 0, \ldots, 0)$ is a bijection.

Skew codes, I

Let A be a ring, S, D be an endomorphism and a S-derivation of A respectively.

Proposition

Let $f(t) \in R = A[t; S, D]$ be a monic polynomial of degree $n > 0$. The map $\varphi : R/Rf(t) \longrightarrow A^n$ given by $\varphi(p + Rf) = p(T_f)(1, 0, \ldots, 0)$ is a bijection.

The above bijection endows A^n with a left $R = A[t; S, D]$-module structure.
Let us remark that if $(a_0, a_1, \ldots, a_{n-1}) \in A^n$ then $\varphi(\sum_{i=0}^{n-1} a_i t^i + Rf) = (a_0, \ldots, a_{n-1})$. Notice also that the practical effect of this proposition is a way of computing the remainder of the euclidean right division by $f(t)$.

Skew codes, II

Definitions

Let $f(t) \in R = A[t; S, D]$ be monic. $C = \varphi(Rg/Rf)$ is called a cyclic (f, S, D)-code (φ is defined on the previous slide). So $C \subseteq A^n$ consists of the coordinates of the elements of Rg/Rf in the basis $\{1, t, \ldots, t^{n-1}\}$ for some right monic factor $g(t)$ of $f(t)$.

Theorem

Let $g(t) := g_0 + g_1 t + \cdots + g_r t^r \in R$ be a monic polynomial $(g_r = 1)$. With the above notations we have

(a) *The code corresponding to Rg/Rf is a free left A-module of dimension $n - r$ where $\deg(f) = n$ and $\deg(g) = r$.*

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

(c) *The rows of the matrix generating the code C are given by*
$$(T_f)^k(g_0, g_1, \ldots, g_r, 0, \ldots, 0), \quad \text{for } 0 \leq k \leq n - r - 1.$$

Examples

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

(1) If $\sigma = Id.$, $\delta = 0$, $f = t^n - 1$ and $f = gh$
(b) gives the cyclicity condition for the code.
(c) we get the standard generating matrix of a cyclic code.

(2) If $\sigma = Id.$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$
(b) gives the constacyclicity condition for the code.
(c) we get the standard generating matrix of a constacyclic code.

(3) $f = t^n - 1 \in R = \mathbb{F}_q[t;\theta]$ ($\theta =$ "*Frobenius*") and $f = gh \in R$
(b) gives the θ-cyclicity condition for the code.
(c) gives the standard generating matrix of a θ-cyclic code.

(4) If $\sigma = \theta$, $\delta = 0$, $f = t^n - \lambda$ and $f = gh$.
(b) gives the θ-constacyclicity condition for the code.
(c) gives the standard generating matrix of a θ-constacyclic code.

Examples

(5) If $A = \mathbb{F}_q$ is a finite field and $\theta \in Aut(\mathbb{F}_q)$ we get the skew codes defined in several papers.

(6) Let R be the Ore extension $R := \mathbb{F}_p[x]/(x^p - 1)[t; \frac{d}{dx}]$, where $\frac{d}{dx}$ denotes the usual derivation. $f(t) = t^p - 1 \in Z(R)$. Let us fix $p = 5$. In this case x and $x + x^4$ are roots of $t^5 - 1$ and one compute that the polynomial $g(t) := t^2 - 2xt + x^2 - 1$ is the least left common multiple of $t - x$ and $t - (x + x^4)$ in R. $g(t)$ is a right (and hence left, since $f(t)$ is central) factor of $t^5 - 1$. The generating matrix of the cyclic $(id., \frac{d}{dx})$-code corresponding to the left module Rg/Rf is given by:

$$G := \begin{pmatrix} x^2 - 1 & -2x & 1 & 0 & 0 \\ 2x & x^2 + 2 & -2x & 1 & 0 \\ 2 & 4x & x^2 & -2x & 1 \end{pmatrix}$$

Lemma

Let $f, g, h, h' \in R$ be monic polynomials such that $f = gh = h'g$. Then

(a) $gR = ann_R(h' + fR)$ *and*
$gR/fR = \{p + fR \mid p \in ann_R(h' + fR)\}$.

(b) $Rg = ann_R(h + Rf)$ *and*
$Rg/Rf = \{p + Rf \mid p \in ann_R(h + Rf)\}$.

Theorem

Let $f, g, h, h' \in R$ be monic polynomials such that $f = gh = h'g$ and let C denote the code corresponding to the cyclic module Rg/Rf. Then the following statements are equivalent:

(i) $(c_0, \dots, c_{n-1}) \in C$,

(ii) $(\sum_{i=0}^{n-1} c_i t^i) h(t) \in Rf$,

(iii) $\sum_{i=0}^{n-1} c_i T_f^i(\underline{h}) = \underline{0}$,

(iv) $\sum_{j=0}^{n-1} (\sum_{i=j}^{n-1} c_i f_j^i(\underline{h})) N_j(C_f) = \underline{0}$.

In view of the above it seems natural to set the following definition.

Definition

For a left (resp. right) linear code $C \subseteq A^n$, we say that a matrix H is a control matrix if $C = lann(H)$ (resp. $C = rann(H)$).

Corollary

For a code C determined by the left R-module Rg/Rf such that there exist monic polynomials $h, h' \in R$ with $f = gh = h'g$ the matrix H whose i^{th} row is $T_f^{i-1}(\underline{h})$, for $1 \leq i \leq \deg(f)$ is a control matrix.

The above Theorem and Corollary give back the control matrix of classical cyclic and skew cyclic codes.

Examples

(1) Let $f(t) = t^n - 1 \in R = F[t]$, where F is a (finite) field and let $g(t), h(t) \in R$ be such that $t^n - 1 = g(t)h(t) = h(t)g(t)$. We write $h(t) = \sum_{i=0}^{k} h_i t^i$. For $\underline{v} = (v_0, \ldots, v_{n-1}) \in k^n$, the action of T_f^i is given by $T_f^i(\underline{v}) = (v_0, \ldots, v_{n-1})C^i$, where C is the companion matrix associated to the polynomial $t^n - 1$. The control matrix associated to C corresponding to Rg/Rf defined above gives back the classical control matrix.

Examples

(2) Let A, S, D be a ring, an automorphism and a S-derivation. Assume $t^n - 1 = gh = h'g$, where $g, h, h' \in R$ are monic. Let us write $h(t) = \sum_{i=0}^{k} h_i t^i$, with $h_k = 1$. The PLT defined by $f(t) = t^n - 1$ is the map $T_f = T_C$, where C is the companion matrix associated to $t^n - 1$. The control matrix H for the code C determined by the module Rg/Rf:

$$H = \begin{pmatrix} h_0 & h_1 & \dots & h_k & 0 & 0 & 0 \\ 0 & S(h_0) & \dots & S(h_{k-1}) & S(h_k) & 0 & 0 \\ 0 & 0 & S^2(h_0) & \dots & \dots & \dots & \dots \\ \vdots & \dots & & \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & \dots & S^{n-k}(h_k) \\ \vdots & \vdots & * & 0 & & * & * \\ & * & * & \vdots & * & h_0 & * \\ * & * & * & 0 & * & * & \dots \end{pmatrix}$$

Examples

So the last $n-k$ columns are in echelon form and hence linearly independent. The dimension of the code being equal to k, in good cases (e.g. if the ring is a field), this means that they define a control matrix as well. The transpose of these last columns is exactly the control matrix obtained by other authors in the case when A is a commutative field.

Examples

(3) Let A be a ring and δ be a (usual) derivation on A. For $a \in A$ we consider the polynomial $f(t) := (t^2 - a)^2 \in A[t;\delta]$ and put $g = h = t^2 - a$. We have $f(t) = t^4 - 2at^2 - 2\delta(a)t - \delta^2(a) + a^2$. We get

$$G = H = \begin{pmatrix} -a & 0 & 1 & 0 \\ -\delta(a) & -a & 0 & 1 \\ -a^2 & 0 & a & 0 \\ a\delta(a) - \delta(a)a & -a^2 & \delta(a) & a \end{pmatrix}$$

One can check that $\underline{g}H = (-a, 0, 1, 0)H = (0, 0, 0, 0)$. Set H_1, H_2, H_3, H_4 to represent the different columns of H, then $H_1 + H_3(-a) + H_4\delta(a) = 0 \in A^4$ and $H_2 + aH_4 = 0 \in A^4$. Let H' be the 4×2 matrix $H' = (H_3, H_4)$. We get that $lann(H') = lann(H) = C$. This shows that H' is a control matrix of the code C.

Examples

(4) Consider $R := \mathbb{F}_5[x]/(x^5-1)[t; \frac{d}{dx}]$, and $f(t) = t^5 - 1$. This last polynomial is central and can be factorized as $f(t) = g(t)h(t) = h(t)g(t)$ where $g(t) := t^2 - 2xt + x^2 - 1$ and $h(t) = t^3 + 2xt^2 + (3x^2+2)t + (4x^3+3x)$. The code we are considering corresponds to the module $Rg(t)/(t^5-1)$. The rows of the control matrix are given by $T_f^i(\underline{h})$, $0 \leq i \leq 4$. The first row is thus $\underline{h}$ the second row is $\underline{h}C_f + \frac{d}{dx}(\underline{h})$. Here C_f is the companion matrix of $t^5 - 1$ and acts as cyclic permutation. Hence we get

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

Boucher, Ulmer

In a series of papers D. Boucher and F. Ulmer studied codes defined by skew polynomials (they initiated this kind of codes). They computed the distance of these codes and showed that they are sometimes better than usual codes.
In the table, n is the length of the codes over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ and corresponds to the degree of $f \in R = \mathbb{F}_4[t;\theta]$. The integer r is the degree of g, $n - r = dim(C) = Rg/Rf$.
C_d means that the best known linear $n, n-r]_4$ code is of minimal distance d andis a cyclic codes.
C_d^θ means that the best known linear $n, n-r]_4$ code is of minimal distance d and is a an (ideal-) θ cyclic code.
M_d means that the best known linear $n, n-r]_4$ code is of minimal distance d and is a module θ-codes.
A negative entry $-j$ indicates that the best module θ-code has a distance $d-j$, where d is the distance of the best known linear $n, n-r]_4$ code.

Skew exponents

Lemma

f a nonzero divisor in a ring R. Suppose $fR = Rf$ and $|R/Rf| < \infty$. Let $g \in R$ such that $|R/Rg| < \infty$ and $r_g : R/Rf \xrightarrow{\cdot g} R/Rf$ is $1-1$.

$$\exists e \in \mathbb{N} \quad \text{such that} \quad f^e - 1 \in Rg$$

Skew exponents

Lemma

f a nonzero divisor in a ring R. Suppose $fR = Rf$ and $|R/Rf| < \infty$. Let $g \in R$ such that $|R/Rg| < \infty$ and $r_g : R/Rf \overset{\cdot g}{\to} R/Rf$ is $1-1$.

$$\exists e \in \mathbb{N} \quad \text{such that} \quad f^e - 1 \in Rg$$

Examples

1) $R = \mathbb{F}_q[x]$, $f(x) = x$, $g(x) \in \mathbb{F}_q[x]$ s.t. $g(0) \neq 0$. We obtain the classical exponent of g ($q = p^n$, p prime).
2) $R = \mathbb{F}_q[t;\theta]$ where $\theta(a) = a^p$ for $a \in \mathbb{F}_q$; $f(t) = t$, $g(t) \in R$ such that $g(0) \neq 0$. There exists $e = e(g)$ such that $g(t) \,|\, t^e - 1$ in R.
3) $R = F_q[x]/(x^p)[t; \frac{d}{dx}]$; $f = t^p; g = g(t)$ monic with $Rg + Rt^p = R$. There exists e such that $g \,|\, t^{pe} - 1$.

Let us notice that for any $a \in \mathbb{F}_q$, $g(t) = t - a$ is such that $t - a|_d t^e - 1$ implies that $(t^e - 1)(a) = 0$, i.e. $S^{e-1}(a)S^{e-1}(a) \dots S(a)a = 0$. On introduit

Definition

G a group, $\sigma \in Aut(G)$.

1) $g \in G$, $n \in \mathbb{N}$ $\quad N_n(g) = \sigma^{n-1}(g)\sigma^{n-2}(g) \cdots \sigma(g)g$.
2) $ord_\sigma(g)$ is the smallest l such that $N_l(g) = 1$ (if it exists).

Lemma

G a finite group, $g \in G$

a) $N_{l+s}(g) = \sigma^l(N_s(g))N_l(g)$.
b) *if* $ord_\sigma(g) = l$ *then* $(N_s(g) = 1 \Leftrightarrow l/s)$.
d) *If* $\sigma^l = id$. *then* $\sigma(N_l(g)) = gN_l(g)g^{-1}$.
e) $\sigma^l = id$. *then* $ord_\sigma(g) | l \cdot ord(N_l(g))$.

Proposition

$g, g_1, \dots g_s$ monic polynomials in $F_q[t;\theta]$ ($q = p^n$) such that $g(0) \neq 0 \neq g_i(0)$, for $i = 1, \dots, s$. Then

a) $g(t)|_r t^l - 1 \Leftrightarrow e(g)|l$.

b) $g|_r h \Rightarrow e(g)|e(h)$.

c) $e([g_1, \dots, g_s]_l) = [e(g_1), \dots, e(g_s)]$.

d) $e(g(t)) = ord_\theta(C_g)$ *where* $C_g \in GL_r(F_q)$ *is the companion matrix of* $g(t)$.

e) *If* $\alpha \in \overline{F_q}^*$ *is such that* $t - \alpha|_r g(t)$ *in* $\overline{F}_q[t;\theta]$ *and* $g(t)$ *is irreducible in* $F_q[t;\theta]$, *then* $e(g) = ord_\theta(\alpha)$.

f) θ *can be extended to* $F_q[t;\theta]$ *via* $\theta(t) = t$ $e(g(t)) = e(\theta(g(t))$ *for* $g(t) \in F_q[t;\theta]$.

g) $h(t) = [g(t), \theta(g(t)), \dots, \theta^{n-1}(g(t))]_l$ *then* $e(h(t)) = e(g(t))$ *and* $\theta(h(t)) = h(t)$.

h) $\alpha \in F_{p^n}^*$ *s.t.* $ord(\alpha) = p^n - 1$ *then* $e(t - \alpha) = (p-1)n$.

Corollary

$\alpha \in F_q$, $q = p^n$, $\theta =$ Frobenius, $\theta^n = id$. $e(t-\alpha) \mid n(p-1)$ and $G_0(t) := [t-\alpha \mid \alpha \in F_q^*]_l$ then $G_0(t) = t^{n(p-1)} - 1$ is central in $R = \mathbb{F}_q[t;\sigma]$.

Examples

1. $e_r(t-\alpha) = e_l(t-\alpha)$ (right and left exponents)
2. In $F_4[t;\theta]$ where $F_4 = \{0, 1, a, a^2\}$ $a^2 = 1 + a$ $e_r(t^3 + a^2t^2 + at + a) \neq e_l(t^3 + a^2t^2 + at + a)$.

Final remarks

Let us remark the following commutation.

Proposition

Let A be a finite ring, $S \in Aut(A)$. For any $n \in \mathbb{N}$, $g, h^i nR$
$t^n - 1 = gh \Leftrightarrow t^n - 1 = hg$.

Other works around codes with skew polynomial rings Pumpluen's papers.
Noncommutative Frobenius rings play a crucial role in coding theory (see e.g. J. Wood).