PLT, Coding
and
Factorisations in Ore extensions

Saint Louis, October 2013

Based on works with M.Boulagouaz and A. Cherchem

.

A)**PLT and (σ, δ)-codes**.

B) **Untwisting $\mathbb{F}_q[t;\theta]$.**

C)**Exponents**

D) **Norms**

.

1 A)PLT and (σ, δ)-codes

1) Skew polynomial rings and skew polynomial maps.

A a ring, $\sigma \in End(A)$, δ a σ-derivation:

$$\delta \in End(A, +) \quad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \forall a, b \in A.$$

$R := A[t; \sigma, \delta] = \{f(t) = \sum_{i=0}^{n} a_i t^i \mid a_i \in A\}$.
The product is based on:

$$\forall a \in A, \quad ta = \sigma(a)t + \delta(a).$$

Examples 1.1. 1) If $\sigma = id.$ and $\delta = 0$ we get the usual polynomial ring $A[t]$.

2) $R = \mathbb{C}[t; \sigma]$ where σ is the complex conjugation. If $x \in \mathbb{C}$ is such that $\sigma(x)x = 1$ then

$$t^2 - 1 = (t + \sigma(x))(t - x).$$

On the other hand $t^2 + 1$ is central and irreducible in R.

3) $R = \mathbb{Q}(x)[t; id., \frac{d}{dx}]$. $tx - xt = 1$; for any $t^2 = (t + (x + a)^{-1})(t - (x + a)^{-1})$ for any $a \in \mathbb{Q}$.

Definition 1.2. $a \in A$, $f(t) \in R = A[t; \sigma, \delta]$ there exist $q(t) \in R, c \in A$ such that $f(t) = q(t)(t - a) + c$.
The (right) evaluation of $f(t)$ at a is the element c above. We write $c = f(a)$. We say a is a (right) root of $f(t)$ if $f(a) = 0$. This defines the (σ, δ)-polynomial maps.

Examples: 1) For $a \in A,\ t^2(a) = \sigma(a)a + \delta(a)$.
2) If $\delta = 0,\ t^n(a) = \sigma^{n-1}(a) \cdots \sigma(a)a$.

2) $\underline{(\sigma, \delta)\text{-PLT}}$

Definition 1.3. V be a left A-module. $T : V, + \longrightarrow V, +$ such that:

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v \qquad \forall v \in V,\ \forall \alpha \in A$$

T is called a (σ, δ) pseudo-linear map.

Fact: There is one-one correspondence between (σ, δ)-PLT's and left $A[t; \sigma, \delta]$-module.

Examples 1.4. (a) $a \in A$, $T_a \in End(A, +)$ is defined by

$$T_a(x) = \sigma(x)a + \delta(x) \quad \forall x \in A.$$

In particular, $T_0 = \delta,\ T_1 = \sigma + \delta$.

b) If $p(t) \in A[t; \sigma, \delta]$ is a monic polynomial and C_p is its companion matrix then the PLT corresponding to R/Rp is the map T_p given by

$$T_p : A^n \longrightarrow A^n : \underline{v} \mapsto \sigma(\underline{v})C_p + \delta(\underline{v})$$

Fact: T a (σ, δ)-PLT on V. The map $\varphi_T : R \longrightarrow End(V, +)$

$$\varphi_T(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} a_i T^i, \quad \text{is a ring homomorphism.}$$

Theorem 1.5. *(a)* $f(T_a)(1) = f(a)$.

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

3) (σ, δ)-codes, definition and examples.

Proposition 1.6. *Let* $f \in R = A[t; \sigma, \delta]$ *be a monic polynomial of degree* $n > 0$. *The map* $\varphi : R/Rf \longrightarrow A^n$

$$\varphi(p + Rf) = p(T_f)(1, 0, \ldots, 0)$$

is a bijection.

Definitions 1.7. Let $f \in A[t; \sigma, \delta]$ be a monic polynomial of degree n.
A polynomial (f, σ, δ)-code $C(t)$ is the left cyclic module Rg/Rf where g is monic.
A (f, σ, δ) code C in A^n is the image of a polynomial (f, σ, δ)-code $C(t)$ via the map described in Proposition 1.6.

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

Theorem 1.8. *(a) The code corresponding to* Rg/Rf *is of dimension* $n - r$ *where* $\deg(f) = n$ *and* $\deg(g) = r$.

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

(c) The rows of the matrix generating the code C *are*

$$(T_f)^k(g_0, g_1, \ldots, g_r, 0, \ldots, 0), \quad 0 \leq k \leq n - r - 1$$

.

Examples 1.9. In the examples hereunder $A = \mathbb{F}_{p^n}$ stands for a finite field and θ denotes the Frobenius map: $\theta(a) = a^p$, for $a \in A$.

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

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

3. $f = t^n - \lambda \in R = \mathbb{F}_q[t;\theta]$ and $f = gh$.
   (b) gives the θ-constacyclicity condition for the code.
   (c) we get the standard generating matrix of a θ-constacyclic code.

4. $R := \mathbb{F}_p[x]/(x^p)[t; \frac{d}{dx}]$ where $\frac{d}{dx}$ denotes the usual derivation. $f(t) = t^p - 1$ is a central polynomial.

Proposition 1.10. *Assume there exists $h, h' \in R$, monic such that $f = hg = gh'$ then $C(t) = lann_{R/Rf}h'$. Moreover 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) $\sum_{i=0}^{n-1} c_i T_f^i(\underline{h'}) = \underline{0}$,

2 B) Untwisting $\mathbb{F}_q[t;\theta]$

1) From factorization in $\mathbb{F}_q[t;\theta]$ to factorisation in $\mathbb{F}_q[x]$

$f(t) = \sum_{i=0}^{n} a_i t^i \in R := \mathbb{F}_q[t;\theta] \subset S := \mathbb{F}_q[x][t;\theta]$, where $\theta(x) = x^p$. We evaluate at x:

$$f(x) = \sum_{i=0}^{n} a_i x^{[i]} \in \mathbb{F}_q[x]$$

where for $i \geq 1$; $[i] := \frac{p^i - 1}{p-1} = p^{i-1} + p^{i-2} + \cdots + 1$ and $[0] = 0$.
$\mathbb{F}_q[x^{[\,]}] := \{\sum_{i\geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$

Theorem 2.1. $f(t) = \sum_{i=0}^{n} a_i t^i \in R := \mathbb{F}_q[t;\theta]$.

1) for every $b \in \mathbb{F}_q$, $f(b) = \sum_{i=0}^{n} a_i b^{[i]} = f^{[\,]}(b)$.

2) For $h(t) \in R$, $f(t) \in Rh(t)$ iff $f^{[\,]}(x) \in \mathbb{F}_q[x]h^{[\,]}(x)$.

Corollaire 2.2. *$f(t) \in \mathbb{F}_q[t;\theta]$ is irrducible iff the corresponding p-polynomial $f^{[\,]}$ does not have non trivial factors in $\mathbb{F}_q[x^{[\,]}]$.*

2) Factoring

Let $f(t) \in R := \mathbb{F}_q[t;\theta]$.
Step 1 Compute $f^{[\,]}$; if $f^{[\,]}$ has no proper factor in $\mathbb{F}_q[x^{[\,]}]$ then $f(t)$ is irreducible in R.
Step 2 If $f^{[\,]}(x) = q(x)h^{[\,]}(x)$ for some polynomial $h(t)$ then $h(t)$ divides $f(t)$ and write $f(t) = g(t)h(t)$. Come back to step 1 replacing $f(t)$ by $g(t)$.

Example 2.3. $\mathbb{F}_4 = \{1, 0, a, 1+a\}$, with $a^2 + a + 1 = 0$. Consider $f(t) = t^4 + (a+1)t^3 + a^2t^2 + (1+a)t + 1 \in \mathbb{F}_4[t;\theta]$. its associated polynomial is $x^{15} + (a+1)x^7 + (a+1)x^3 + (1+a)x + 1 \in \mathbb{F}_4[x]$. We may factorize it as:

$$(x^{12}+ax^{10}+x^9+(a+1)x^8+(a+1)x^5+(a+1)x^4+x^3+ax^2+x+1)(x^3+ax+1)$$

This last factor is a $[p]$-polynomial that corresponds to $t^2 + at + 1 \in \mathbb{F}_4[t;\theta]$. Since $x^3 + ax + 1$ is irreducible in $\mathbb{F}_4[x]$, we have $t^2 + at + 1$ is irreducible as well in $\mathbb{F}_4[t;\theta]$. We conclude that $f(t) = (t^2 + t + 1)(t^2 + at + 1)$ is a decomposition of $f(t)$ in irreducible factors in $\mathbb{F}_4[t;\theta]$.

3 C) Exponents

Motivation. Coding theory (cyclic codes, linear recurring sequences)

Lemme 3.1. *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 3.2. $q = p^n$, p prime.

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.

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 $g(t) \mid t^e - 1$ 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 $g \mid t^{pe} - 1$.

Definition 3.3. 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).

Lemme 3.4. *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 3.5. *$g, g_1, \dots g_s$ 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 $e(t-\alpha) = (p-1)n$.

Corollaire 3.6. *$\alpha \in F_q$, $q = p^n$, $\theta =$ Frobenius, $\theta^n = id$. $e(t-\alpha) \,|\, n(p-1)$ 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 3.7. 1. $e_r(t-\alpha) = e_l(t-\alpha)$ (right and left exponents)

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

3) <u>More general settings.</u>

a) $A[t;\sigma]$ where A is finite ring.
b) $A[t;\sigma,\, \delta]$ where A is a finite ring.

"t" replaced by $f(t) \in R = A[t;\sigma,\, \delta]$ a monic polynomial such that $f(t)R = Rf(t)$.

Let $g(t) \in A[t;\sigma,\,\delta]$ be a monic polynomial such that $Rg + Rf = R \quad e_f(g) = min\{s|g(t)|_r\ f^s - 1\}$ ($e_f(g)$ exists, thanks to Lemma 2).

Proposition 3.8. *A a finite ring, $f(t) \in R = A[t;\sigma,\,\delta]$ monic of degree l such that $f(t)R = Rf(t)$. Let $g(t) \in R$ s.t. $Rg + Rf = R$.*

1. $R(t-\alpha) + Rf = R \Rightarrow e_f(t-\alpha) = ord_{\sigma^l}(f(\alpha))$

2. *$g(t)$ monic of degree n, $C_g \in M_n(A)$ companion matrix* $\quad N_{r,\sigma^l}(f(C_g)) = I_l \Rightarrow e_f(g)\,|\,r \quad$ *i.e.* $ord_{\sigma^l}(f(C_g)) = r \Rightarrow \exists\, q(t) \in R$ *s.t.* $q(t)g(t)\ |_r\ f^r - 1$.

4 Norms

In the sequel, we assume that σ has finite order s.

Definition 4.1. (a) Let k be a field and let $\sigma \in Aut(k)$. Let $p \in R := k\,[t;\sigma]$ a monic polynomial of degree n and C_p its companion matrix. The norm of $C = C_p$, denoted by $N\,(C)$, is then defined by

$$N\,(C) = \sigma^{s-1}\,(C)\,\sigma^{s-2}\,(C)\cdots\sigma\,(C)\,C.$$

(b) Two monic polynomials p and q in R are similar (we write $p \underset{\sigma}{\sim} q$,) if we have $R/Rp \cong R/Rq$ as left R-modules.

For $M \in M_n(k)$, denote by $\chi_M = \det(xI_n - M) \in k[x]$ the characteristic polynomial of M.
Denote S the monoid of monic polynomials in $R = k[t;\sigma]$.
We then have an application

$$\begin{aligned} S &\rightarrow k\left[x\right] \\ p &\rightarrow \varphi\left(p\right) = \chi_{N\left(C_p\right)}. \end{aligned}$$

The application φ has the following properties.

Proposition 4.2. *Let $p, q \in S$. Then:*

1. $\varphi(p) \in k^{\sigma}[x]$.
2. (1) $\chi_{N\left(C_p\right)} = \chi_{\sigma\left(N\left(C_p\right)\right)}$
3. *If* $p \underset{\sigma}{\sim} q$, *then* $\varphi\left(p\right) = \varphi\left(q\right)$.
4. $\varphi(pq) = \varphi(p)\varphi(q)$.

Thank you !!