Skew polynomial rings and coding

Patrick Solé

I3S, UMR 6070, Université de Nice Sophia antipolis

Conference Non Commutative Rings June 09

Plan

Skew polynomial rings form an interesting class of non commutative rings. We survey recent applications to coding theory

- skew cyclics codes over finite fields and Galois rings (with Boucher, Ulmer, AMC 2008)
- cyclic algebras for space time block codes (with Oggier, Belfiore, ISIT 2009)
- quasi-cyclic codes (with Yemen)
- convolutional codes (after Gluesing Luersen)

Polynomial approach to cyclic codes

$$
\begin{array}{rcl}
(\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[x]/(x^n-1) \\
a=(a_0,a_1,\ldots,a_{n-1}) & \leftrightsquigarrow & a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \\
C & \leftrightsquigarrow & \mathcal{C}=(g \pmod{x^n-1})
\end{array}
$$

C is cyclic iff $\mathcal{C}$ is an ideal of the ring $\mathbb{F}_q[x]/(x^n-1)$
invariance by shift

$$a=(a_0,a_1,\ldots,a_{n-2},a_{n-1})\in\mathcal{C}\Rightarrow(a_{n-1},a_0,a_1,\ldots,a_{n-2})\in\mathcal{C}$$

Duality of cyclic codes

Dual Code :

$$\mathcal{C}^{\perp} = \{b \in (\mathbb{F}_q)^n \mid \forall a \in \mathcal{C}, < a, b >= 0\}.$$

$x^n - 1 \;=\; h \cdot g \;\in \mathbb{F}_q[x]$ with $h = h_0 + h_1 x + \ldots + x^k$ the check polynomial

$\Rightarrow (g)^{\perp}$ is also a cyclic code with generator the reciprocal of h the complement of g ie $h_0 x^k + h_1 x^{k-1} + \ldots + 1$

Skew polynomial rings (of automorphism type)

Let R be a ring and $\theta \in \mathrm{Aut}(R)$:

$$R[X,\theta] = \{a_0 + a_1 X + \ldots + a_n X^n \mid a_i \in R \text{ et } n \in \mathbb{N}\}.$$

1. **addition :** as in $R[X]$ componentwise
2. **multiplication :** for $a \in R$ get $X \cdot a = \theta(a) \cdot X$ and distribute ...

Example : $R = \mathbb{F}_q$ a finite field. $\Rightarrow \mathbb{F}_q[X,\theta]$ left and right euclidean

Ideals of skew polynomial rings

Two sided ideals are generated by $X^t \cdot f$ with $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ where $|\theta| =$ order of θ in $Gal(\mathbb{F}_q/\mathbb{F}_p)$.
Consider ideals in the quotient ring by a two sided ideal

$$\begin{array}{rcl} (\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) & \leftrightsquigarrow & a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \\ C & \leftrightsquigarrow & \mathcal{C} = (g \pmod{f}) \text{ with } f = h \cdot g \end{array}$$

$$f = X^n - 1 \Rightarrow h^\perp = \theta^k(h_0)X^k + \theta^{k-1}(h_1)X^{k-1} + \ldots + 1$$

Skew polynomial rings with coefficient ring a Galois ring

$$\varphi\colon \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Definition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ with $h \in \mathbb{Z}_4[y]$ such that

1. $\varphi(h) \in \mathbb{F}_2[y]$ is unitary irreducible of degree m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ generates the multiplicative group of $\mathbb{F}_{2^m}$

Representation of elements :

1. $\alpha_0 + \alpha_1\xi + \ldots + \alpha_{m-1}\xi^{m-1}$ with $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ with a and b in $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta\colon a + 2b \mapsto a^2 + 2b^2$ is an automiorphism of $GR(4^m)$ of order m.
NB : $\theta(\xi) = \xi^2$.

$\boxed{\Rightarrow R[X,\theta] = GR(4^m)[X,\theta] \textbf{ is a skew polynomial rings}}$

Ideals of $GR(4^m)[X,\theta]$ and skew cyclic codes over $GR(4^m)$

Compare the situation in $\mathbb{Z}[x]$:

1. Ideals are not all principal
2. division by monic polynomials is possible.

The polynomials $f \in \mathbb{Z}_4[X^m]$ that are monic of degree n generate two sided ideals. If $n = deg(f)$ then

$$
\begin{array}{rcl}
(GR(4^m))^n & \leftrightsquigarrow & GR(4^m)[X,\theta]/(f) \\
a = (a_0, a_1, \ldots, a_{n-1}) & \leftrightsquigarrow & a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \\
\mathcal{C} & \leftrightsquigarrow & \mathcal{C}(X) = (g \pmod{f}) \text{ avec } f = h \cdot g
\end{array}
$$

with g monic.

Self dual constacyclic codes over $GR(4^m)$

If $h\,g = X^n \pm 1$ with $h = X^k + \sum_{i=0}^{r-1} h_i X^i$, then

$$g^\perp \;=\; h_k + \theta(h_{k-1})X + \ldots + \theta^k(h_0)X^k.$$

Hence for a euclidean self dual code :

$$h = X^k + \sum_{i=1}^{k-1} \left(\theta^{k-i}(g_0^{-1})\, \theta^{k-i}(g_{k-i}) X^i \right) + \theta^r(g_0^{-1})$$

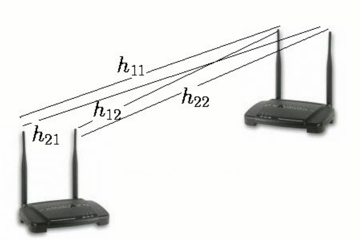
Let

$$\left(\sum_{i=0}^{k-1} g_i X^i + X^k \right) \left(\theta^k(g_0^2) + \sum_{i=1}^{k} \theta^{k-i}(g_0^2\, g_{r-i}) X^i \right) = X^{2k} \pm 1$$

for a self dual Hermitian code

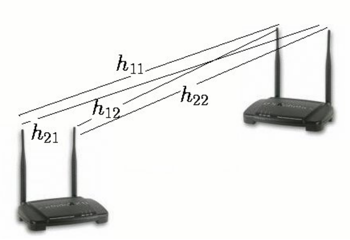
$$g^H = \sum_{i=0}^{k} \theta^{m-1+i}(h_{k-i})\, X^i$$

Space Time Codes : example



1. Time $t = 1$:
   - 1st receive antenna :$y_{11} = h_{11}x_{11} + h_{12}x_{21} + v_{11}$
   - 2nd receive antenna :$y_{21} = h_{21}x_{11} + h_{22}x_{21} + v_{21}$
2. Time $t = 2$:
   - 1st receive antenna :$y_{12} = h_{11}x_{12} + h_{12}x_{22} + v_{12}$
   - 2nd receive antenna :$y_{22} = h_{21}x_{12} + h_{22}x_{22} + v_{22}$

Space Time Codes : matrix formalism



We get the matrix equation

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \underbrace{\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}}_{\textit{space-time}\text{ codeword }\mathbf{x}} + \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}.$$

Code design criteria (Coherent case)

- *Reliability* is modeled by the *pairwise probability of error*, bounded by

$$P(\mathbf{X} \to \hat{\mathbf{X}}) \leq \frac{const}{|\det(\mathbf{X} - \hat{\mathbf{X}})|^{2M}}.$$

- We assume the receiver knows the channel (*coherent case*).
- We need

$$\det(\mathbf{X} - \mathbf{X}') \neq 0 \quad \forall\ \mathbf{X} \neq \mathbf{X}'$$

called *fully diverse* codes.

- We attempt to maximize the *minimum determinant*

$$\min_{\mathbf{X} \neq \mathbf{X}'} |\det(\mathbf{X} - \mathbf{X}')|^2.$$

The idea behind division algebras

- The difficulty in building $\mathcal{C}$ such that

$$\det(\mathbf{X}_i - \mathbf{X}_j) \neq 0, \ \mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C},$$

  comes from the *non-linearity* of the determinant.
- If $\mathcal{C}$ is taken inside an *algebra* of matrices, the problem simplifies to

$$\det(\mathbf{X}) \neq 0, \ \mathbf{0} \neq \mathbf{X} \in \mathcal{C}.$$

- A *division algebra* is a non-commutative field.

An example : cyclic division algebras

- Let $\mathbb{Q}(i) = \{a + ib,\ a, b \in \mathbb{Q}\} \supset$ information symbols.
- Let $L/\mathbb{Q}(i)$ be a *cyclic* number field of degree n.
- A *cyclic algebra* $\mathcal{A}$ is defined as follows

$$\mathcal{A} = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in L\}$$

  with basis $\{1, e, \ldots, e^{n-1}\}$ and $e^n = \gamma \in \mathbb{Q}(i)$.
- Think of $i^2 = -1$.
- A *non-commutativity rule* : $\lambda e = e\sigma(\lambda)$, $\sigma : L \to L$ the generator of the Galois group of $L/\mathbb{Q}(i)$.
- $\mathcal{A}$ is the quotient of the *skew polynomial ring* $L[e;\sigma]$ by the principal ideal $(e^n - \gamma)$.

The "Golden code"

A codeword X belonging to the Golden Code $\mathcal{G}$ has the form

$$X = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ i\bar{\alpha}(c+d\bar{\theta}) & \bar{\alpha}(a+b\bar{\theta}) \end{pmatrix}$$

where a, b, c, d are QAM symbols (that is, $a, b, c, d \in \mathbb{Z}[i]$), $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$ and $\bar{\alpha} = 1 + i - i\bar{\theta}$. Its minimum determinant is given by

$$\delta = \min_{\mathbf{0} \neq X \in \mathcal{G}} |\det(X)|^2 = \frac{1}{5}.$$

Codes over $M_2(\mathbb{F}_2)$

When using a coset code from the "Golden code"

$$= (X_1, \dots, X_L),\ X_i \in \mathcal{G}$$

for $i = 1, \dots, L$, (Cf Construction A of Lattices from Codes)

$$\mathcal{G} = \alpha(\mathbb{Z}[i, \theta] \oplus \mathbb{Z}[i, \theta]j),$$

(where $j^2 = i$) the quotient that appears is the ring $M_2(\mathbb{F}_2)$

$$\mathcal{G}/(1+i)\mathcal{G} \simeq \mathcal{M}_2(\mathbb{F}_2),$$

A useful metric on codes over that ring to bound below the determinant is induced by the Bachoc weight defined for nonzero $M's$ by $w_B(M) = 1$ if M is invertible
$w_B(M) = 2$ if M is non-invertible

The Bachoc map

Bachoc (1997) has shown that codes over $\mathcal{M}_2(\mathbb{F}_2)$ reduce to codes over $\mathbb{F}_4 = \mathbb{F}_2(\omega)$, where $\omega^2 + \omega + 1 = 0$. Indeed, first note that

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)j \qquad (1)$$

where $j^2 = 1$ and $j\omega = \bar{\omega}j = \omega^2 j$. The isomorphism is given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto j, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto \omega.$$

Bachoc map and Ore rings

More formally denote by $\mathbb{F}_4[X;\sigma]$ the Ore ring with base field $\mathbb{F}_4$ and field automorphism $\sigma : x \mapsto x^2$. With this notation we have the ring isomorphism

$$R := \mathbb{F}_4[X;\sigma]/(X^2+1) \simeq \mathcal{M}_2(\mathbb{F}_2)$$

by identifying X and j. This isomorphism in turn induces an isomorphism of $\mathbb{F}_2$ left vector spaces

$$\phi : \mathbb{F}_4 \times \mathbb{F}_4 \to \mathcal{M}_2(\mathbb{F}_2).$$

The Bachoc map is an isometry from Bachoc weight to Hamming weight

We have that ϕ maps a pair $(a, b) \in \mathbb{F}_4 \times \mathbb{F}_4$ to a matrix in $\mathcal{M}_2(\mathbb{F}_2)$,
the elements $(a, 0)$ and $(0, b)$ can be identified with a, $bj \in R$ respectively, their image yields an invertible matrix in $\mathcal{M}_2(\mathbb{F}_2)$ whenever $a, b \in \mathbb{F}_4^*$.
These 6 elements thus correspond to the 6 invertible matrices of $\mathcal{M}_2(\mathbb{F}_2)$,
a one-to-one correspondence between elements of Hamming weight 1 in $\mathbb{F}_4^2$ and invertible matrices in $\mathcal{M}_2(\mathbb{F}_2)$.

Definitions

Linear code C of length n over a ring A : an A-submodule of A^n, i.e.,

- $x, y \in C \Rightarrow x + y \in C$;
- $\forall\lambda \in A,\ x \in C \Rightarrow \lambda x \in C$,

T : standard shift operator on A^n

$$T(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2}).$$

C quasi-cyclic of index ℓ or ℓ-quasi-cyclic : invariant under T^ℓ.
Assume : ℓ divides n
$m := n/\ell$: co-index.

Our approach

- If $\ell = 2$ and first circulant block is identity matrix, code equivalent to a so-called pure **double circulant** code.
- alternatively the generator matrix is block circulant by blocks of order ℓ
- here we view an $\ell-$ QC over A as a cyclic code of length m over A^ℓ (viewed as an $A-$module not as a ring)
- natural action of (commutative) polynomials in X with coefficients in $M_\ell(A)$
- $\Rightarrow$ How to factorize $X^m - 1$ in $M_\ell(A)[X]$?

QC codes over fields

Denote by $\mathbb{F}_{q^\ell}[X;\sigma]$ the **skew polynomial ring** ring with base field $\mathbb{F}_{q^\ell}$ and field automorphism σ;
Denote by $M_n(K)$ the ring of matrices of order n with entries in the field K.

We have the ring isomorphism

$$M_\ell(\mathbb{F}_q) \simeq \mathbb{F}_{q^\ell}[Y;\sigma]/(Y^\ell - 1)$$

which generalizes the Bachoc map

Factorization over $M_\ell(\mathbb{F}_q)[X]$

Because of the generalized Bachoc map $\mathbb{F}_{q^\ell}[X]$ is isomorphic to a subring of $M_\ell(\mathbb{F}_q)[X]$
Therefore very factorization over $\mathbb{F}_{q^\ell}[X]$ gives a factorization over $M_q^\ell(\mathbb{F}_q)[X]$.
Question When are these the only ones ?
Example : If $q = \ell = 2$ then $X^{2m} + 1 = (X^m + Y)^2$

2-QC codes over $\mathbb{F}_2$

Assume a factorization $X^n + 1 = fg$ with $f, g \in \mathbb{F}_4[X]$.
When is there a factorization $X^n + 1 = (f_1 + Yf_2)(g_1 + Yg_2)$ with $f_i, g_i \in \mathbb{F}_4[X]$ satisfying $f = f_1 + f_2$ and $g = g_1 + g_2$?
When $f \neq \sigma(f)$ we can show that there is an infinity of (explicit) solutions.
If $f = \sigma(f)$ open problem.

Cyclic Convolutional Codes (CCC)

Let A denote the auxiliary ring that enters the study of cyclic codes of length n over $\mathbb{F}$, a finite field.

$$A := \mathbb{F}[x]/(x^n - 1).$$

Let σ denote an arbitrary automorphism of A
Consider the skew polynomial ring $A[z;\sigma]$ in z with coefficients in A and the commutation rule

$$za = \sigma(a)z$$

A one sided ideal of $A[z;\sigma]$ can be regarded as a $\mathbb{F}[z]-$submodule of $\mathbb{F}[z]^n$ just by changing the order of summation between x and z. Therefore it is a convolutional code of length n over $\mathbb{F}$.

Remarks

- The case $\sigma = 1$ can be reduced to block codes.
- A can be replaced by the group algebra of an abelian group (instead of a cyclic group)
- most results are concerned with a characterization of the generator matrix
- for more info see Heide Gluesing Luerssen home page