Gabidulin Codes

Caruso Xavier and Durand Amaury

Institute : to do

1 Introduction

In 1985, Gabidulin Ernst introduced a Reed-Solomon-like code construction in rank metric. This Gabidulin code class use linearised polynomial concept. In 2013, Wachter-Zeh Antonia proposed efficient implementations of operations with linearized polynomials as well as an equivalent of Gao's algorithm for decoding Gabidulin code. Following years, Boucher Delphine and Ulmer Felix have worked on skew coding theory using Ore's polynomials and they have generalized many code class like BCH or Reed-Solomon. In 2015, Robert Gwezheneg expanded Gabidulin construction to skew-polynomials including the characteristic zero.

Présenter ce qu'il y a dans cet article. Le faire à la fin pour le détail.

2 Ore polynomials

Throughout this article, we use the following notation: K is a field, $\theta : K \to K$ be a ring homomorphism and $\partial : K \to K$ be a θ-derivation, i.e. an additive mapping such that $\partial(ab) = \theta(a)\partial(b) + \partial(a)b$ for all $a, b \in K$.

We shall denote by F the subfield of K consisting of elements a such that $\theta(a) = a$ and $\partial(a) = 0$. **We will always assume that the extension K/F is finite.** This implies in particular that θ has finite order and thus is bijective.

Definition 1 (Ore polynomial ring). *The ring of Ore polynomials $K[X;\theta,\partial]$ is the ring whose elements are polynomials in X over A endowed with the usual addition and with the multiplication defined by the rule:*

$$X \times a = \theta(a)X + \partial(a), \quad \forall a \in A.$$

The notion of degree extends *verbatim* to Ore polynomials: if $P = \sum a_i X^i$ is an Ore polynomial, its degree is the largest integer i for which $a_i \neq 0$. Besides, one can prove the existence of a right Euclidean division for Ore polynomials: if $A, B \in K[X;\theta,\partial]$ with $B \neq 0$, there exist unique $Q, R \in K[X;\theta,\partial]$ with $A = QB + R$ and $\deg R < \deg B$. This has the usual consequences: the noncommutative ring $K[X;\theta,\partial]$ is left-principal, right GCDs and left LCMs are well defined and can be computed by Euclidean algorithm. Similarly, left Euclidean divisions, left GCDs and right LCMs do exist (since our general assumptions imply that θ is bijective).

Notation: In what follows, we will denote by $A \,\%\, B$ the remainder in the right division of A by B.

Pseudo-linear morphisms. Another important notion is that of pseudo-linear morphisms. It is defined as follows:

Definition 2 (Pseudo-linear morphism). *Let M and N be two vector spaces over K. A* pseudo-linear morphism *$u : M \to N$ is a map verifying $u(ax) = \theta(a)u(x) + \partial(a)x$ for all $a \in K$ and $x \in M$.*

We observe that any pseudo-linear morphism is *a fortiori* F-linear (where F is defined at the beginning of this section).

Pseudo-linear morphisms are relevant in the context of Ore polynomials because the Ore multiplication reflects the composition rule of pseudo-linear morphisms. More precisely, given a pseudo-linear endomorphism $u : M \to M$ and a Ore polynomial $P = \sum_i a_i X^i \in K[X; \theta, \partial]$, one defines $P(u) = \sum_i a_i u^i$. One then easily checks that $P(u) \circ Q(u) = (PQ)(u)$ where the multiplication on the right hand size is the Ore multiplication. In other words, denoting by $\mathrm{End}_F(M)$ the ring of F-linear maps from M to itself, the "evaluation" mapping

$$\mathrm{ev}_u : \quad K[X; \theta, \partial] \to \mathrm{End}_F(M), \quad P(X) \mapsto P(u)$$

is a ring homomorphism for any pseudo-linear endomorphism u.

The case where M is K itself deserves particular attention. Indeed, we first observe that evaluation is then closely related to Euclidean division thanks to the formula:

$$\mathrm{ev}_u(P)(a) = a \cdot P \,\%\, \left(X - \tfrac{u(a)}{a}\right)$$

for any pseudo-linear endomorphism u of K, any $P \in K[X; \theta, \partial]$ and any $a \in K$. Second, we have a complete classification of pseudo-linear endomorphisms of K.

Proposition 1. *The pseudo-linear endomorphisms of K are exactly the maps of the form $\partial + c\theta$ with $c \in K$.*

Proof. It is easily checked that $\partial + c\theta$ is pseudo linear for all $c \in A$. Conversely, let u be a pseudo-linear morphism. Set $g = u - \partial$. It is easily checked that g is θ-semi linear, i.e. $g(ab) = \theta(a)g(b)$ for all $a, b \in K$. Applying this with $b = 1$ and letting $c = g(1)$, we end up with $g = c\theta$ and so $u = \partial + c\theta$.

In what follows, we will often use the notation ev_c in place of $\mathrm{ev}_{\partial + c\theta}$. The properties of ev_c are summarized in the next proposition.

Proposition 2. *1. For all $c \in K$, the ring homomorphism ev_c is surjective and its kernel is a principal ideal generated by a polynomial of degree $[K : F]$ with coefficients in F.*
2. For $c_1, c_2 \in K$, the equality $\ker ev_{c_1} = \ker ev_{c_2}$ holds if and only if there exists $a \in K$, $a \neq 0$ such that

$$ev_{c_1}(P) = m_a^{-1} \circ ev_{c_2}(P) \circ m_a \tag{1}$$

for all $P \in K[X; \theta, \partial]$, where $m_a : K \to K$ is the multiplication by a.

When $\ker \mathrm{ev}_{c_1} = \ker \mathrm{ev}_{c_2}$, we shall say that c_1 and c_2 are *equivalent*. Evaluating (1) at 1, we find that c_1 and c_2 are equivalent if and only if there exists $a \in K$, $a \neq 0$ such that $c_1 a = c_2\theta(a) + \partial(a)$. In particular, we notice that the equivalence class of $c \in K$ is exactly the image of $x \mapsto \frac{(\partial + c\theta)(x)}{x}$.

Moreover, when $\theta = \mathrm{id}$, the condition resumes to the equality $c_1 = c_2 + \frac{\partial(a)}{a}$, i.e. to the fact that $c_1 - c_2$ is a logarithmic derivative. On the other hand, when $\partial = 0$, the condition is equivalent to $c_1 = c_2 \cdot \frac{\theta(a)}{a}$, that is to the fact that c_1 and c_2 has the same norm over F.

3 Generalized Gabidulin codes

For starters, let's define generalized Gabidulin codes and let's give some characteristics.

Definition 3 (Gabidulin Code). *If $[F : K] = m$ and let $n, k \in \mathbb{N}$ such as $k \leqslant n \leqslant m$. Let $g = (g_1, \ldots, g_n) \in K^n$ such as g_i are linearly independant over F and let $c \in K$. Gabidulin code is the set of words :*

$$Gab_c[n, k, g] = \{ev_c(f)(g_1), \ldots, ev_c(f)(g_n) \mid f \in K[X, \theta, \partial] \textbf{ and } \deg(f) < k\},$$

it's a code of length n and dimension k.

For this code's family, the Hamming distance isn't the most adapted distance, so it is better to use the rank metric.

Definition 4 (Rank weight). *Let $a = (a_1, \ldots, a_n) \in K^n$, the rank weight of a is the dimension of the F-vector space generated by a.*

For metric rank code, there is an equivalent of perfect codes.

Proposition 3. *Gabidulin codes are Maximal Rank Distance code (MRD code) i.e. the minimum rank distance $d = n - k + 1$.*

Proof. Let $Gab_c[n, k, g]$ a Gabidulin code and let $a = (a_1, \ldots, a_n) \in Gab_c[n, k, g]$ a non-zero word as rank weight w. So, there is a Ore polynomial P as $\deg(P) = w$ and $\mathrm{ev}_c(P)(a_i) = 0$ for all $i \in \{1, \ldots, n\}$. However, a is a word of Gabidulin Code, so there is a Ore polynomial Q as $\deg(Q) \leqslant k - 1$ and $a_i = \mathrm{ev}_c(Q)(g_i)$. We known that $\mathrm{ev}_c(PQ)(g_i) = \mathrm{ev}_c(P)(a_i) = 0$ and thus the Ore polynomial PQ is an annihilator polynomial of n elements linearly independant over F. So, we have $\deg(PQ) \geqslant n$. Moreover, by construction we have $\deg(PQ) = w + k - 1$, so we have $n \leqslant w + k - 1$ i.e. $w \geqslant n - k + 1$. The equality is given by Singleton bound.

To decode Gabidulin codes, we have a generalized Gao algorithm. Let $Gab_c[n, k, g]$ a gabidulin code and $b = \{b_1, \ldots, b_n\} \in K^n$ a received vector. To decode b we proceed as follows.

- Step 0, Annihilator : Find the unique Ore polynomial G_0 as $\mathrm{ev}_c(G_0)(g_i) = 0$ for all $i \in \{1, \ldots, n\}$.

- Step 1, Interpolation : Find the unique Ore polynomial G_1 as $\mathrm{ev}_c(G_1)(g_i) = b_i$ and $\deg(G_1) \leqslant n-1$.
- Step 2, Partial gcd : Apply the extend Euclidian algorithm to G_0 and G_1. Stop when the remainder G has degree $< \frac{n+k}{2}$. If we have to this step $uG_0 + vG_1 = G$.
- Step 3, Long left division : Apply a left division to G by v, say $G = vf_1 + r$. If $r = 0$ and $\deg(f_1) < k$ then the word is f_1 else, that more than $\frac{d-1}{2}$ errors occurred.

- donner des exemples : 1) sur les corps finis et 2) avec des dérivations

4 Implementation

- dire ce qu'on a implémenté
- donner quelques benchmarks