On Gröbner basis for certain one-point AG codes

Guilherme Chaud Tizziotti
Based on joint work with F. Fornasiero

FAMAT - UFU
guilhermect@ufu.br

CIMPA - Research School Algebraic Methods in Coding Theory

Objective

- Gröbner basis for certain one-point AG codes.
- Why? - Input to an encoding algorithm to certain AG codes.

Idea

- Linear code $C \subset \mathbb{F}_q^n$.
- S_n symmetric group.
- $\sigma \in S_n$, $(c_1, \ldots, c_n) \in \mathbb{F}_q^n \rightsquigarrow$
$\sigma(c_1, \ldots, c_n) = (c_{\sigma(1)}, \ldots, c_{\sigma(n)})$.
- $\mathrm{Aut}(C) = \{\sigma \in S_n : \sigma(C) = C\}$, automorphism group of C.
- Code C + automorphism $\rightsquigarrow$ module $\overline{C} \leq \mathbb{F}_q[t]^r \rightsquigarrow$
encoding algorithm.

Encoding AG codes via Gröbner basis

• J. Little, C. Heegard and K. Saints, 1995, Systematic encoding via Gröbner bases for a class of algebraic geometric Goppa codes, IEEE Trans. Infor. Theory 41(6), 1752-1761.

• J. Little, C. Heegard and K. Saints, 1997, On the structure of Hermitian codes, J. Pure Appl. Algebra 121, 293-314.

Gröbner basis for $\mathbb{F}_q[t]$-modules

• Every submodule $M \subseteq \mathbb{F}_q[t]^n$ has a Gröbner basis $\mathcal{G}$, which induces a a division algorithm: given $\mathbf{f} \in \mathbb{F}_q[t]^r$ there exist $\mathbf{a}_1, \ldots, \mathbf{a}_s, \mathbf{R}_{\mathcal{G}} \in \mathbb{F}_q[t]^r$ such that $\mathbf{f} = \mathbf{a}_1\mathbf{g}_1 + \ldots + \mathbf{asg}_s + \mathbf{R}_{\mathcal{G}}$.

• Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ be the standard basis in $\mathbb{F}_q[t]^r$, with $\mathbf{e}_1 > \ldots > \mathbf{e}_r$. The POT ordering on $\mathbb{F}_q[t]^r$ is defined by

$$t^i\mathbf{e}_j > t^k\mathbf{e}_\ell$$

if $j < \ell$, or $j = \ell$ and $i > k$.

AG codes

$$C_{\mathcal{X}}(D, G) := \{(f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n : f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G)$ is the space of rational functions f on $\mathcal{X}$ such that $f = 0$ or $\text{div}(f) + G \geq 0$.

• If $G = \lambda P$, for some rational point P on $\mathcal{X}$, and D is the sum of the all others rational points on $\mathcal{X}$, the AG code $C_{\mathcal{X}}(D, \lambda P)$ is called *one-point AG code*.

AG codes

Proposition (Goppa): Let $\mathrm{Aut}(\mathcal{X})$ be the automorphism group of $\mathcal{X}$ over $\mathbb{F}_q$ and consider the subgroup

$$Aut_{D,G}(\mathcal{X}) = \{\sigma \in \mathrm{Aut}(\mathcal{X}) : \sigma(D) = D \text{ and } \sigma(G) = G\} .$$

Each $\sigma \in \mathrm{Aut}_{D,G}(\mathcal{X})$ induces an automorphism of $C_{\mathcal{X}}(D, G)$ by

$$\widehat{\sigma}(f(P_1), \ldots, f(P_n)) = (f(\sigma(P_1)), \ldots, f(\sigma(P_n))) .$$

Linking AG codes and $\mathbb{F}_q[t]$-modules

Lemma: Let $C_{\mathcal{X}}(D, G)$ be an AG code arising from $\mathcal{X}$ over $\mathbb{F}_q$. Suppose that $\mathcal{X}$ has a nontrivial automorphism $\sigma \in Aut_{D,G}(\mathcal{X})$. If $Supp(D) = O_1 \cup \ldots \cup O_r$ is the decomposition of the support of D into disjoint orbits under the action of σ, then there is an one-to-one correspondence between $C_{\mathcal{X}}(D, G)$ and a submodule $\overline{C}$ of the free module $\mathbb{F}_q[t]^r$.

Linking AG codes and $\mathbb{F}_q[t]$-modules

Proof. Suppose that $Supp(D) = O_1 \cup \ldots \cup O_r$ is the decomposition of the support of D into disjoint orbits under the action of σ. For each $i = 1, \ldots, r$, let $O_i = \{P_{i,0}, \ldots, P_{i,|O_i|-1}\}$, where for each $P_{i,j} \in O_i$ we have that $P_{i,j} = \sigma^j(P_{i,0})$ be as above, and let $h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$.
The r-tuples $(h_1(t), \ldots, h_r(t))$ can be seen also as an element of the $\mathbb{F}_q[t]$-module $A = \bigoplus_{i=1}^r \mathbb{F}_q[t]/\langle t^{|O_i|} - 1\rangle$. So, the collection $\tilde{C}$ of r-tuples obtained from all $f \in \mathcal{L}(G)$ is closed under sum and multiplication by t. Define $\overline{C} := \pi^{-1}(\tilde{C})$, where π is the natural projection from $\mathbb{F}_q[t]^r$ onto $\bigoplus_{i=1}^r \mathbb{F}_q[t]/\langle t^{|O_i|} - 1\rangle$. Thus, we get an one-to-one correspondence between $C_{\mathcal{X}}(D, G)$ and $\overline{C} \leq \mathbb{F}_q[t]^r$. $\square$

The root diagram

• Suppose that the one-point AG code $C = C_{\mathcal{X}}(D, \lambda P)$ ($\mathcal{X}$ over $\mathbb{F}_q$) has an automorphism σ that fixing the divisors D and $G = \lambda P$.

• Suppose also that the order of σ is equal to s, with $s = d(q-1)$ for some $d \in \mathbb{N}$.

• Let $\overline{C}$ be the submodule of $\mathbb{F}_q[t]^r$ associated to C by the automorphism σ.

• Using the POT ordering we can get that a Gröbner basis $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\}$ for $\overline{C}$ such that $\mathbf{g}_i = (0, \ldots, 0, g_i^{(i)}(t), g_i^{(i+1)}(t), \ldots, g_i^{(r)}(t))$, for all $i = 1, \ldots, r$.

• If $deg(g_i^{(i)}(t)) = d_i$, then $g_i^{(i)}(t)$ has d_i distinct roots in $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

The root diagram

- For $i = 1, \ldots, r$, let $\mathcal{R}_i \subseteq \mathbb{F}_q^*$ be the set of roots of $t^{|O_i|} - 1$.

By a *root diagram* $\mathcal{D}_C$ for the code C, we mean a table with r rows. For each i, the boxes on the i-th row correspond to the elements of $\mathcal{R}_i$. We mark the roots of $g_i^{(i)}(t)$ on the i-th row with a X in the corresponding box.

Proposition (Saints, Heegard and Little): The dimension of the code C is equal to the number of empty boxes in the root diagram $\mathcal{D}_C$.

Gröbner basis for certain AG codes

• Let $\mathcal{X}_{a,b}$ be the curve defined over $\mathbb{F}_q$ by affine equation $f(y) = g(x)$, where $f(T), g(T) \in \mathbb{F}_q[T]$, $deg(f) = a$ and $deg(g) = b$, with $a < b$ and $gcd(a, b) = 1$.

• Consider the one-point AG code $C_{\mathcal{X}_{a,b}}(D, \lambda P)$.

• Suppose that $div_\infty(x) = aP$ and $div_\infty(y) = bP$, for some point on $\mathcal{X}_{a,b}$, and that there exists $\sigma \in Aut_{D,G}(\mathcal{X}_{a,b})$, given by $\sigma(x) = \alpha x$ and $\sigma(y) = \alpha^t y$, for some positive integer t and some $\alpha \in \mathbb{F}_q^*$ with order equal to $ord(\alpha) := \nu$.

• Assume that $H(P) = \langle a, b \rangle$.

Gröbner basis for certain AG codes

• Assume that there exists polynomials $M_i(y)$ such that the orbit O_i is the intersection of $\mathcal{X}$ with the curve $M_i(y) = 0$ and, for all i, $M_i(y)$ is a non-zero constant when restricted to each of the orbits O_k, $k \neq i$.

• Assume also that there are polynomials $B_{i,j}(x, y)$ such that $B_{i,j}(x, y)$ vanishes at each point of O_i except $P_{i,j}$.

Gröbner basis for certain AG codes

Lemma: $div_\infty(M_i) = (\rho_1 b)P$ and $div_\infty(B_{i,j}) = (\rho_2 a + \rho_3 b)P$, where ρ_1, ρ_2 and ρ_3 are non-negative integers.

Gröbner basis for certain AG codes

Proposition: Let $C_{\mathcal{X}_{a,b}}(D, \lambda P)$ and σ be as above. Let $\mathcal{D}_C$ be the root diagram for $C_{\mathcal{X}_{a,b}}(D, \lambda P)$. Fix i, $1 \leq i \leq r$, and let ρ_1, ρ_2 and ρ_3 be as above. Therefore,
1) if $\lambda \geq (i-1)(\rho_1 b)$, then the i-th row of $\mathcal{D}_C$ is not full, in the sense that not every boxes composing the i-th row are marked with X;
2) if $\lambda \geq (\rho_2 a + \rho_3 b) + (i-1)(\rho_1 b)$, then the row is empty, in the sense that none of the boxes composing the i-th row is marked with X.

Theorem

Let $\mathcal{D}_C$ be the root diagram for $C_{\mathcal{X}_{a,b}}(D, \lambda P)$. If there is $i \in \{1, \ldots, r\}$ such that

$$(i-1)(\rho_1 b) \leq \lambda < (\rho_2 a + \rho_3 b) + (i-1)(\rho_1 b),$$

then the i-th row of $\mathcal{D}_C$ is neither full, nor empty, and the complement of the set of roots marked on row i of the diagram is the set $E_i = \{\alpha^{-(\beta+\gamma b)} \in \mathbb{F}_q^* \mid 0 \leq \beta \leq b-1,\ 0 \leq \gamma \leq \rho_1 - 1,\ (i-1)(\rho_1 b) + \beta a + \gamma b \leq \lambda\}$.

Gröbner basis for certain AG codes

Input: the root diagram $\mathcal{D}_C$, the N rational points $P_{i,j}$ of $Supp(D) = O_1 \cup \ldots \cup O_r \cup O_{r+1} \cup O_{r+s}$.

Output: a non-reduced Gröbner basis $\mathcal{G} = \{\mathbf{g}^{(1)}, \mathbf{g}^{(2)}, \ldots, \mathbf{g}^{(r+s)}\}$ of $\overline{C}$.

$\mathcal{G} := \{\}$
for i from 1 to $r+s$ **do**
    if |RootDiagram[i]|<Boxes[i] **then**
        for k from 1 to $r+s$ **do**
            $g_k^{(i)} := 0$
            if $k \geq i$ **then**
                for j from 0 to Boxes[k] $- 1$ **do**
                    $g_k^{(i)} := g_k^{(i)} +$ Evaluate[$i, P_{k,j}$] $t^j\, \mathbf{e}_k$
                end for
            end if
        end for
    else
        $\mathbf{g}^{(i)} := (t^{\texttt{Boxes}[i]} - 1)\, \mathbf{e}_i$
    end if
    $\mathcal{G} := \mathcal{G} \cup \{\mathbf{g}^{(i)}\}$
end for
return $\mathcal{G}$

Examples

- The curve $\mathcal{X}_{q^{2r}}$ defined over $\mathbb{F}_{q^{2r}}$ by the affine equation

$$y^q + y = x^{q^r+1},$$

where q is a prime power and r an odd integer.

- The curve $\mathcal{X}_m$ defined over $\mathbb{F}_{q^2}$ by the affine equation

$$y^q + y = x^m,$$

where q is a prime power and $m > 2$ is a divisor of $q + 1$.

Referência

F. Fornasiero and G. Tizziotti, On Gröbner basis for certain one-point AG codes, 2017, arxiv.org/abs/1703.06899

MUITO OBRIGADO!