

M. Ceria*, T. Mora†, M. Sala‡

ZECH TABLEAUX AS TOOLS FOR SPARSE DECODING

Abstract. Within the framework of Groebner-free Solving, we introduce the notion of Zech tableau as a tool for producing a linear error locator polynomials for cyclic codes.

1. Introduction

In the Late Nineties, the classical approach on BCH decoding based on Berlekamp's *key equation* was upsetted by the application of Gröbner bases to the problem; it appeared a series of papers which terminated with two different proposals: Orsini-Sala general error locator polynomial [30] and Augot *et al.* Newton-Based decoder [3]; both approaches payed not only the hard pre-computation of a Gröbner basis but (mainly) the density of their decoders.

A recent work-in-progress [7, 8, 9] reconsidered the same problem within the frame of *Gröbner-free solving*, explicitly expressed and sponsored in the book [26, Vol.3,40.12,41.15]; such approach aims to avoid the computation of a Gröbner basis of a (0-dimensional) ideal $J \subset \mathcal{P}$ in favour of combinatorial algorithms describing instead the structure of the algebra \mathcal{P}/J .

The consequence is a preprocessing which is quadratic (and a decoding which is linear) on the length of the code.

The approach requires to describe and produce a monomial basis of the syndrome algebra; such description forced us to introduce the notion of *Zech tableau* which is the argument of this note.

2. Notations

\mathbb{F} denotes an arbitrary field, $\overline{\mathbb{F}}$ denotes its algebraic closure and \mathbb{F}_q denotes a finite field of size q (so q is implicitly understood to be a power of a prime) and $\mathcal{P} := \mathbb{F}[X] := \mathbb{F}[x_1, \dots, x_n]$ the polynomial ring over the field \mathbb{F} .

Let \mathcal{T} be the set of terms in \mathcal{P} , *id est*

$$\mathcal{T} := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}.$$

If $t = x_1^{\gamma_1} \cdots x_n^{\gamma_n} \in \mathcal{T}$, then $\deg(t) = \sum_{i=1}^n \gamma_i$ is the *degree* of t and, for each $h \in \{1, \dots, n\}$, $\deg_h(t) := \deg_{x_h}(t) := \gamma_h$ is the *h-degree* of t .

*Department of Computer Science, University of Milan.

†Department of Mathematics, University of Genoa.

‡Department of Mathematics, University of Trento.

A *semigroup ordering* $<$ on \mathcal{T} is a total ordering such that

$$t_1 < t_2 \Rightarrow st_1 < st_2, \text{ for each } s, t_1, t_2 \in \mathcal{T}.$$

For each semigroup ordering $<$ on \mathcal{T} , we can represent a polynomial $f \in \mathcal{P}$ as a linear combination of terms arranged w.r.t. $<$, with coefficients in the base field \mathbb{F} :

$$f = \sum_{t \in \mathcal{T}} c_t t = \sum_{t \in \mathcal{T}} c(f, t) t = \sum_{i=1}^s c(f, t_i) t_i : c(f, t_i) \in \mathbb{F} \setminus \{0\}, t_i \in \mathcal{T}, t_1 > \dots > t_s.$$

For each such f its *support* is $\text{supp}(f) := \{\tau \in \mathcal{T} : c(f, \tau) \neq 0\}$, its *leading term* is the term $\mathbf{T}_{<}(f) := \max_{<}(\text{supp}(f)) = t_1$, its *leading coefficient* is $\text{lc}_{<}(f) := c(f, t_1)$ and its *leading monomial* is $\mathbf{M}_{<}(f) := \text{lc}_{<}(f) \mathbf{T}_{<}(f) = c(f, t_1) t_1$. When $<$ is understood we will drop the subscript, as in $\mathbf{T}(f) = \mathbf{T}_{<}(f)$.

A *term ordering* is a semigroup ordering such that 1 is lower than every variable or, equivalently, such that it is a *well ordering*.

In all paper, we consider the *lexicographical ordering* induced by $x_1 < \dots < x_n$, i.e:

$$x_1^{\gamma_1} \cdots x_n^{\gamma_n} <_{\text{Lex}} x_1^{\delta_1} \cdots x_n^{\delta_n} \Leftrightarrow \exists j \mid \gamma_j < \delta_j, \gamma_i = \delta_i, \forall i > j,$$

which is a term ordering. Since we do not consider any term ordering other than Lex, we drop the subscript and denote it by $<$ instead of $<_{\text{Lex}}$.

The assignment of a finite set of terms

$$\mathbf{G} := \{\tau_1, \dots, \tau_\nu\} \subset \mathcal{T}, \tau_i = x_1^{a_1^{(i)}} \cdots x_n^{a_n^{(i)}}$$

defines a partition $\mathcal{T} = \mathbf{T} \sqcup \mathbf{N}$ of \mathcal{T} in two parts:

- $\mathbf{T} := \{\tau_i : \tau \in \mathcal{T}, 1 \leq i \leq \nu\}$ which is a *semigroup ideal*, id est a subset $\mathbf{T} \subset \mathcal{T}$ such that

$$\tau \in \mathbf{T}, t \in \mathcal{T} \implies t\tau \in \mathbf{T};$$

- the *normal set* $\mathbf{N} := \mathcal{T} \setminus \mathbf{T}$ which is an *order ideal*, id est a subset $\mathbf{N} \subset \mathcal{T}$ such that

$$\tau \in \mathbf{N}, t \in \mathcal{T}, t \mid \tau \implies t \in \mathbf{N},$$

For any set $F \subset \mathcal{P}$, write

- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\}$;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\}$;
- $\mathbf{T}(F) := \{\tau \mathbf{T}(f) : \tau \in \mathcal{T}, f \in F\}$, a semigroup ideal;
- $\mathbf{N}(F) := \mathcal{T} \setminus \mathbf{T}(F)$, an order ideal;
- $\mathbb{I}(F) = \langle F \rangle$ the ideal generated by F .

$$- \mathbb{F}[\mathbf{N}(F)] := \text{Span}_{\mathbb{F}}(\mathbf{N}(F)).$$

Given an ideal $J \subset \mathcal{P}$, denote G the minimal set of generators of the semigroup ideal $\mathbf{T} := \mathbf{T}(J)$; we denote by $\mathbf{N} := \mathbf{N}(J) = \mathcal{T} \setminus \mathbf{T}(J)$ the order ideal introduced by the partition $\mathcal{T} = \mathbf{T}(J) \sqcup \mathbf{N}(J) = \mathbf{T} \sqcup \mathbf{N}$; \mathbf{N} will be called the *Groebner escalier* of J .

Let $\mathbf{X} = \{P_1, \dots, P_N\} \subset \mathbb{F}^m$ be a finite set of simple points

$$P_i := (a_{1,i}, \dots, a_{n,i}), i = 1, \dots, N.$$

We call

$$I(\mathbf{X}) := \{f \in \mathcal{P} : f(P_i) = 0, \forall i\},$$

the *ideal of points* of \mathbf{X} .

If we are interested in the *ordered set*, instead of its support \mathbf{X} , we denote it by $\underline{\mathbf{X}} = [P_1, \dots, P_N]$.

For any (0-dimensional, radical) ideal $J \subset \mathcal{P}$ and any extension field E of \mathbb{F} , let $\mathcal{V}_E(J)$ be the (finite) rational points of J over E . We also write $\mathcal{V}(J) = \mathcal{V}_{\mathbb{F}}^J(J)$. We have the obvious duality between I and $\mathcal{V} = \mathcal{V}_{\mathbb{F}}^J$.

Definition 1. For an ideal $J \subset \mathcal{P}$, a finite set $G \subset J$ will be called a *Groebner basis* of J if $\mathbf{T}(G) = \mathbf{T}(J)$, that is, $\mathbf{T}\{G\} := \{\mathbf{T}(g) : g \in G\}$ generates $\mathbf{T}(J) = \mathbf{T}\{J\}$.

We give now a brief recap on Cerlienco-Mureddu algorithm, introduced in [11, 12, 13], which is the first combinatorial algorithm that, given a finite set of simple points $\mathbf{X} = \{P_1, \dots, P_N\}$ computes the lexicographical Groebner escalier $\mathbf{N}(I(\mathbf{X}))$ for the ideal of points of \mathbf{X} .

In particular, in [11], they consider an *ordered* finite set of simple points in \mathbf{k}^n , $\underline{\mathbf{X}} = [P_1, \dots, P_N]$, and prove that there is a one-to-one correspondence between $\underline{\mathbf{X}}$ and the terms of the lexicographical Groebner escalier of $I(\mathbf{X})$:

$$\Phi : \underline{\mathbf{X}} \rightarrow \mathbf{N}(I(\mathbf{X}))$$

$$P_i \mapsto x_1^{\alpha_1^{(i)}} \cdots x_n^{\alpha_n^{(i)}}.$$

They find Φ using only combinatorics on the coordinates of the elements in \mathbf{X} . In particular, only comparisons among the coordinates of the points are needed. The algorithm is iterative on the points and recursive on the variables, thus it pays the price of a rather bad complexity: a straightforward implementation of the algorithm is proportional to $n^2 N^2$. Another iterative algorithm [10] gives the same result by eliminating recursion and keeping iterativity on the points, via the introduction of a data structure (the Bar Code) that stores the information on the terms needed to perform the algorithm.

We conclude this section briefly recalling the standard notation on cyclic codes, needed to understand what follows.

Let C be an $[n, k, d]_q$ q -ary cyclic code with length n , dimension k and distance d . We denote by $g(x) \in \mathbb{F}_q[x]$ its *generator polynomial*, remarking that $\deg(g) = n - k$ and

$g \mid x^n - 1$. Let \mathbb{F}_{q^m} be the splitting field of $x^n - 1$ over \mathbb{F}_q .

If a is a primitive n -th root of unity, the *complete defining set* of C is

$$S_C = \{j \mid g(a^j) = 0, 0 \leq j \leq n-1\}.$$

This set is completely partitioned in cyclotomic classes, so we can pick an element for each such class, getting a set $S \subset S_C$, uniquely identifying the code. This set S is a *primary defining set* of C .

If H is a parity-check matrix of C , \mathbf{c} is a codeword (i.e. $\mathbf{c} \in C$), $\mathbf{e} \in (\mathbb{F}_q)^n$ an error vector and $\mathbf{v} = \mathbf{c} + \mathbf{e}$ a received vector, the vector $\mathbf{s} \in (\mathbb{F}_{q^m})^{n-k}$ such that its transpose \mathbf{s}^T is $\mathbf{s}^T = H\mathbf{v}^T$ is called *syndrome vector*. We call *correctable syndrome* a syndrome vector corresponding to an error of weight $\mu \leq t$, where t is the *error correction capability* of the code, i.e. the maximal number of errors that the code can correct.

3. Cooper Philosophy

In 1990 Cooper [17, 18] suggested to use Gröbner basis computations in order to decode cyclic codes. Let C be a binary BCH code correcting up to t errors, $\bar{s} = (s_1, \dots, s_{2t-1})$ be the syndrome vector associated to a received word. Cooper's idea consisted in interpreting the error locations z_1, \dots, z_t of C as the roots of the syndrome equation system:

$$f_i := \sum_{j=1}^t z_j^{2i-1} - s_{2i-1} = 0, \quad 1 \leq i \leq t,$$

and, consequently, the plain error locator polynomial as the monic generator $g(z_1)$ of the principal ideal

$$\left\{ \sum_{i=1}^t g_i f_i, g_i \in \mathbb{F}_2(s_1, \dots, s_{2t-1})[z_1, \dots, z_t] \right\} \cap \mathbb{F}_2(s_1, \dots, s_{2t-1})[z_1],$$

which was computed via the elimination property of lexicographical Gröbner bases.

In a series of papers [14, 15, 16] Chen et al. improved and generalized Cooper's approach to decoding. In particular, for a q -ary $[n, k, d]$ cyclic code, with error correction capability t , they made the following alternative proposals:

1. denoting, for an error with weight μ , z_1, \dots, z_μ the error locations, y_1, \dots, y_μ the error values, $s_1, \dots, s_{n-k} \in \mathbb{F}_{q^m}$ the associated syndromes, they interpreted [14] the coefficients of the plain error locator polynomial as the elementary symmetric functions σ_j and the syndromes as the *Waring functions*, $s_i = \sum_{j=1}^\mu y_j z_j^i$, and suggested to deduce the σ_j 's from the (known) s_i 's via a Gröbner basis computation of the ideal generated by the Newton identities; a similar idea was later developed in [2, 3].
2. They considered [15] the *syndrome variety*, namely the variety

$$V := \left\{ (s_1, \dots, s_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t) \in (\mathbb{F}_{q^m})^{n-k+2t} : s_i = \sum_{j=1}^\mu y_j z_j^i, 1 \leq i \leq n-k \right\}$$

and proposed to deduce via a Groebner basis pre-computation in

$$\mathbb{F}_q[x_1, \dots, x_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t]$$

a series of polynomials $g_\mu(x_1, \dots, x_{n-k}, Z), \mu \leq t$ such that, for any error with weight μ and associated syndromes $s_1, \dots, s_{n-k} \in \mathbb{F}_{q^m}$, $g_\mu(s_1, \dots, s_{n-k}, Z)$ in $\mathbb{F}_{q^m}[Z]$ is the plain error locator polynomial. This approach was improved in a series of paper [4, 22] culminating with [30] which, specializing Gianni-Kalkbrener Theorem [20, 21], stated in Theorem 6 below.

For a survey of this *Cooper Philosophy* see [29] and on Sala-Orsini locator [5].

4. Syndrome Variety and spurious roots

The notion of *syndrome variety* was formalized in [15] in its approach to decoding q -ary $[n, k, d]$ cyclic codes, with error correction capability t .

Definition 2. For such a cyclic code, the *syndrome variety* is the set of points $\mathbf{V} := \left\{ (s_1, \dots, s_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t) \in (\mathbb{F}_{q^m})^{n-k+2t} : s_l = \sum_{j=1}^{\mu} y_j z_j^l, 1 \leq l \leq n-k \right\}$ where for an error $(s_1, \dots, s_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t) \in \mathbf{V}$ with weight $\mu \leq t$ and

$$y_{\mu+1} = \dots = y_t = 0, \quad z_{\mu+1} = \dots = z_t = 0,$$

z_1, \dots, z_μ represent the *error locations*, y_1, \dots, y_μ the *error values*, $s_1, \dots, s_{n-k} \in \mathbb{F}_{q^m}$ the *associated syndromes*.

Definition 3. For such a cyclic code, and $\mu \leq t$ the *plain error locator polynomial* is the polynomial $\prod_{j=1}^{\mu} (X - z_j)$

Definition 4. [15, 30] A point $(s_1, \dots, s_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t) \in \mathbf{V}$ is said *spurious* if there are at least two values $z_i, z_j, 1 \leq i \neq j \leq \mu$, such that $z_i = z_j \neq 0$.

Denote $\mathbf{V}_{OS} \subset \mathbf{V}$ the set of the non-spurious points of the syndrome variety and consider the polynomial set

$$\mathcal{F}_{OS} = \{f_i, h_j, \chi_i, \lambda_j, p_{l\bar{l}}, 1 \leq l < \bar{l} \leq t, 1 \leq i \leq n-k, 1 \leq j \leq t\} \subset \mathcal{P},$$

where

$$f_i := \sum_{l=1}^t y_l z_l^i - x_i, \quad p_{l\bar{l}} := z_l z_{\bar{l}} \frac{z_l^n - z_{\bar{l}}^n}{z_l - z_{\bar{l}}},$$

$$h_j := z_j^{n+1} - z_j, \quad \lambda_j := y_j^{q-1} - 1, \quad \chi_i := x_i^{q^m} - x_i.$$

Theorem 5. [30] It holds $\mathbb{I}(\mathcal{F}_{OS}) = I(\mathbf{V}_{OS})$.

5. General error locator polynomial

Let G be the reduced Gröbner basis of $\mathbb{I}(\mathcal{F}_{OS}) = I(\mathbf{V}_{OS})$ w.r.t. the lex ordering with $x_1 < \dots < x_{n-k} < z_t < \dots < z_1 < y_1 < \dots < y_t$ and let us denote, for each $\iota \leq t$ and each $\ell \in \mathbb{N}$

$$G_\iota := G \cap \mathbb{F}_q[x_1, \dots, x_{n-k}, z_\iota, \dots, z_1] \text{ and } G_{\iota\ell} := \{g \in G_\iota \setminus G_{\iota+1} : \deg_{x_\iota}(g) = \ell\}.$$

Moreover, we enumerate each $G_{\iota\ell}$ as

$$G_{\iota\ell} := \{g_{\iota\ell 1}, \dots, g_{\iota\ell j_\ell}\}, \mathbf{T}(g_{\iota\ell 1}) < \dots < \mathbf{T}(g_{\iota\ell j_\ell}).$$

Theorem 6. [30] *With the present notation we have*

1. $G \cap \mathbb{F}_q[x_1, \dots, x_{n-k}, z_1, \dots, z_t] = \cup_{i=1}^t G_i$;
2. $G_i = \sqcup_{\delta=1}^i G_{i\delta}$ and $G_{i\delta} \neq \emptyset$, $1 \leq i \leq t$, $1 \leq \delta \leq i$;
3. $G_{ii} = \{g_{ii1}\}$, $1 \leq i \leq t$, i.e. exactly one polynomial exists with degree i w.r.t. the variable z_i in G_i ;
4. $\mathbf{T}(g_{ii1}) = z_i^i$, $\text{lc}(g_{ii1}) = 1$;
5. if $1 \leq i \leq t$ and $1 \leq \delta \leq i-1$, then $\forall g \in G_{i\delta}, z_1 \mid g$.

Definition 7. [30] The unique polynomial

$$g_{tt1} = z_t^t + \sum_{l=1}^t a_{t-l}(s_1, \dots, s_{n-k}) z_t^{t-l}$$

with degree t w.r.t. the variable z_t in G_t , which is labelled the *general error locator polynomial*, is such that the following properties are equivalent for each syndrome vector $s = (s_1, \dots, s_{n-k}) \in (\mathbb{F}_{q^m})^{n-k}$ corresponding to an error with weight bounded by t :

- there are exactly $\mu \leq t$ errors $\zeta_1, \dots, \zeta_\mu$;
- $a_{t-l}(s_1, \dots, s_{n-k}) = 0$ for $l > \mu$ and $a_{t-\mu}(s_1, \dots, s_{n-k}) \neq 0$;
- $g_{tt1}(s_1, \dots, s_{n-k}, z_t) = z_t^{t-\mu} \prod_{i=1}^{\mu} (z_t - \zeta_i)$.

This means that the general error locator polynomial g_{tt1} is the monic polynomial in $\mathbb{F}_q[x_1, \dots, x_{n-k}, z]$ which satisfies the following property:

given a syndrome vector $s = (s_1, \dots, s_{n-k}) \in (\mathbb{F}_{q^m})^{n-k}$ corresponding to an error with weight $\mu \leq t$, then its t roots are the μ error locations plus zero counted with multiplicity $t - \mu$.

Theorem 8 ([30]). *Every cyclic code possesses a general error locator polynomial.*

6. Degroebnerizing Error Correcting Codes (1)

Recently the same problem has been reconsidered in a group of papers [7, 9, 8] within the frame of *Groebner-free Solving* [23, 28, 23, 27], explicitly expressed and sponsored in the book [26, Vol.3,40.12,41.15]; such approach aims to avoid the computation of a Gröbner bases of a (0-dimensional) ideal $J \subset \mathcal{P}$ in favour of combinatorial algorithms, describing instead the structure of the algebra \mathcal{P}/J .

In particular, given the syndrome variety⁵

$$Z = \{(c + d, c^3 + d^3, c, d), c, d \in \mathbb{F}_{2^m}^*, c \neq d\}$$

of a BCH $[2^m - 1, 2]$ -code C over \mathbb{F}_{2^m} , and denoted $I(Z)$ the ideal of points of Z , [7] is able with good complexity to produce, via Cerlienco-Mureddu Algorithm [11, 12, 13] and Lazard Theorem [19], the set $\mathbf{N} := \mathbf{N}(I(Z))$ and proves that the related Gröbner basis has the shape

$$G = (x_1^n - 1, g_2, z_2 + z_1 + x_1, g_4)$$

where (see [30])

$$g_2 = \frac{x_2^{\frac{n+1}{2}} - x_1^{\frac{n+1}{2}}}{x_2 - x_1} = x_2^{\frac{n-1}{2}} + \sum_{i=1}^{\frac{n-1}{2}} \binom{\frac{n-1}{2}}{i} x_1^i x_2^{\frac{n-1}{2}-i}$$

and $g_4 = z_1^2 - \sum_{t \in \mathbf{N}} c_t t$ is Sala-Orsini general error locator polynomial.

Such result allowed [7] to remark (applying Marinari-Mora Theorem [25, 1, 6]) that, for decoding, it is sufficient to compute a particular polynomial – the *half error locator polynomial* (HELP) – that is, a polynomial of the form

$$h(x_1, x_2, z_1) := z_1 - \sum_{t \in \mathbf{H}} c_t t \text{ where } \mathbf{H} := \{x_1^i x_2^j, 0 \leq i < n, 0 \leq j < \frac{n-1}{2}\}$$

which satisfies

$$h(c(1 + a^{2j+1}), c^3(1 + a^{3(2j+1)}), z_1) = z_1 - c, \text{ for each } c \in \mathbb{F}_{2^m}^*, 0 \leq j < \frac{n-1}{2},$$

the other error location ca^{2j+1} been computable via the polynomial $z_2 + z_1 + x_1 \in G$ as $z_2 := x_1 - z_1 = (c + ca^{2j+1}) - c = ca^{2j+1}$.

In other words, once the HELP $h(x_1, x_2, z_1)$ is known, in order to decode a received vector \mathbf{v} , one should:

1. compute the syndrome vector $\mathbf{s} = (s_1, s_2)$ from \mathbf{v} ;
2. evaluate the HELP in \mathbf{s} , namely compute $h(s_1, s_2, z_1)$;

⁵We remark that the variables y_i , corresponding to the error values (see Definition **D**) will be omitted in this paper, because talking about error values in a binary code is completely useless. Therefore $s_1 = x_1 = c + d$, $s_2 = x_2 = c^3 + d^3$ represent the two syndromes and $z_1 = c$, $z_2 = d$ represent the error locations.

3. find the unique root of $h(s_1, s_2, z_1)$ in z_1 , i.e. $z_1 = c$; being an element of \mathbb{F}_{2^m} , it can be expressed either as $c = a^i$, $i \in \{1, \dots, n\}$, in terms of a fixed primitive n -th root of unity $a \in \mathbb{F}_{2^m}$ or as $c = 0$;
4. evaluate the polynomial $z_2 + z_1 + x_1$ in (\mathbf{s}, c) , namely compute $z_2 + c + s_1$;
5. solve $z_2 + c + s_1 = 0$, getting $z_2 = c + s_2 =: d$; being an element of \mathbb{F}_{2^m} , it can be expressed either as $d = a^j$, $j \in \{1, \dots, n\}$, again in terms of a , or as $d = 0$;
6. c, d are the two error locations, so that, if they are different from zero, they identify the position of an error. For $c = a^i, d = a^j \neq 0$, two errors occurred, exactly in positions i, j . Flipping the bits in that positions, we recover the correct sent codeword. If some of c, d are zero, it means that less than two errors occurred.

The HELP can be easily obtained with good complexity via Lundqvist interpolation formula [23] on the set of points

$$\{(c + ca^{2j+1}, c^3 + c^3 a^{3(2j+1)}, c), c \in \mathbb{F}_{2^m}^*, 0 \leq j < \frac{n-1}{2}\}.$$

Experimental showed that in that setting HELP has a very sparse formula, which has been proved in [7]:

$$h(x_1, x_2, z_1) = z_1 + \sum_{i=1}^{\frac{n-1}{2}} a_i x_1^{(4-3i) \bmod n} x_2^{(i-1) \bmod \frac{n+1}{2}}$$

where the unknown coefficients can be deduced by Lundqvist interpolation on the set of points

$$\{(1 + a^{2j+1}, 1 + a^{3(2j+1)}, 1), 0 \leq j < \frac{n-1}{2}\}$$

and on the monomials $\{x_1^{(4-3i) \bmod n} x_2^{(i-1) \bmod \frac{n+1}{2}}, 1 \leq i < \frac{n+1}{2}\}$.

Knowing the structure of the lexicographical Groebner escalier associated to the syndrome variety is a crucial step, in order to find the HELP and efficiently decode a binary cyclic code.

This suggested [9] to consider a binary cyclic code C over $GF(2^m)$, with length $n \mid 2^m - 1$ and *primary* defining set $S_C = \{1, l\}$. Thus it denoted by

- a a primitive $(2^m - 1)$ th root of unity so that $\mathbb{F}_{2^m} = \mathbb{Z}_2[a]$, $\alpha := \frac{2^m - 1}{n}$ and
- $b := a^\alpha$ a primitive n th root of unity,
- $\mathcal{R}_n := \{e \in \mathbb{F}_{2^m} : e^n = 1\}$
- $\mathcal{S}_n := \mathcal{R}_n \sqcup \{0\}$;

considered the following sets of points

$$\mathcal{Z}_2 := \{(c + d, c^l + d^l, c, d), c, d \in \mathcal{R}_n, c \neq d\}, \#\mathcal{Z}_2^\times = n^2 - n;$$

$$Z_+ := \{(c+d, c^l + d^l, c, d), c, d \in \mathcal{S}_n, c \neq d\}, \#Z_+^\times = n^2 + n,$$

$$Z_{ns} := \{(c+d, c^l + d^l, c, d), c, d \in \mathcal{S}_n\} \setminus \{(0, 0, c, c), c \in \mathcal{R}_u\}, \#Z_{ns}^\times = n^2 + n + 1,$$

$$Z_e := \{(c+d, c^l + d^l, c, d), c, d \in \mathcal{S}_n\}, \#Z_e^\times = (n+1)^2,$$

and denoted, for $*$ $\in \{e, ns, +, 2\}$,

- $J_* := I(Z_*)$,
- $N_* := \mathbf{N}(J_*)$ the Gröbner escalier of J_* w.r.t. the lex ordering with $x_1 < x_2 < z_1 < z_2$ and
- $\Phi_* : Z_* \rightarrow N_*$ a Cerlienco-Mureddu correspondence.

Then it assumed to know

- (a). the structure of the order ideal N_2 , $\#N_2 = n^2 - n$, i.e. a minimal basis $\{t_1, \dots, t_r\}, t_i := x_1^{a_i} x_2^{b_i}$, of the monomial ideal $\mathcal{T} \setminus N_2 = \mathbf{T}(\mathcal{J}(Z_2))$,
- (b). a Cerlienco Mureddu Correspondence $\Phi_2 : N_2 \rightarrow Z_2$

and deduced with elementary arguments N_* and Φ_* for $*$ $\in \{e, ns, +\}$.

7. Zech Tableaux

We observe that the parameters of a minimal basis $G = \{t_1, \dots, t_r\}, t_i := x_1^{\gamma_i} x_2^{\delta_i}$, of a monomial ideal

$$\mathcal{T} \subset \mathcal{T} = \{x_1^\gamma x_2^\delta : (\gamma, \delta) \in \mathbb{N}^2\}$$

satisfy relations

- $\gamma_1 > \gamma_2 > \dots > \gamma_r$
- $\delta_1 < \delta_2 < \dots < \delta_r$
- and \mathcal{T} is 0-dimensional if and only if $\delta_1 = 0 = \gamma_r$.

Indeed, the γ_i can be ordered so that $\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_r$

If $\gamma_i = \gamma_{i+1}$ and without loss of generality, $\delta_i \geq \delta_{i+1}$ then $t_{i+1} | t_i$, contradicting the minimality of G . Moreover, if $\delta_i \geq \delta_{i+1}$, $t_{i+1} | t_i$ contradicting the minimality of G .

The corresponding escalier $N = \mathcal{T}/\mathcal{T}$, in the zerodimensional case, is

$$N := \bigsqcup_{i=1}^{r-1} \{x_1^\gamma x_2^\delta : 0 \leq \gamma < \gamma_i, 0 \leq \delta < \delta_{i+1}\}.$$

Definition 9. Consider the field $\mathbb{F}_{2^m} = \mathbb{Z}_2[a]$, a denoting a primitive $(2^m - 1)$ th root of unity; for a value $n \mid (2^m - 1)$ we denote $\alpha := \frac{2^m - 1}{n}$ and $b := a^\alpha$ a primitive n th root of unity.

Denote, for $i, 0 \leq i < \alpha$, $Z_i := \{j, 1 \leq j \leq n : 1 + b^j = 1 + a^{j\alpha} \equiv a^{i \bmod n}\}$, set $z(i) = \#Z_i$; for any set $H \subset \{j, 1 \leq j \leq n\}$ we consider also the values $\zeta(i) = \#(H \cap Z_i)$.

The $(2^m - 1, n; H)$ -Zech Tableau is the assignment of

- an ordered sequence $S := [j_0, \dots, j_{r-1}] \subset \{i, 0 \leq i < \alpha\}$ which satisfies
 - $\zeta(j_0) \geq \dots \geq \zeta(j_{r-1}) > 0$,
 - $\zeta(j) = 0$ for each $j \notin S$.
- the minimal basis $G = \{t_1, \dots, t_r\}, t_i := x_1^{a_i} x_2^{b_i}$, of the monomial ideal $T = \mathcal{T} \setminus N$ corresponding to the escalier

$$N := \bigsqcup_{i=1}^{r-1} \{x_1^a x_2^b : 0 \leq a < a_i, 0 \leq b < b_{i+1}\}.$$

Example 10. Let us consider the values $n = 21, m = 6, \alpha = \frac{63}{21} = 3$ and $O := \{2i - 1, 1 \leq i \leq 10\}$. Let the primary defining set of our code be $S = \{1, 3\}$. The three classes induced by the 21-st roots of unity are divided in this way:

$[0] = \{1 + a^{21}, 1 + a^{45}, 1 + a^9, 1 + a^{27}\}, [1] = \{1 + a^{51}, 1 + a^{15}, 1 + a^3\}, [2] = \{1 + a^{39}, 1 + a^{57}, 1 + a^{33}\}$, so that $\zeta(0) = 4 > \zeta(1) = \zeta(2) = 3$ and the $(63, 21; O)$ -Zech Tableau is given by the sequence $[0, 1, 2]$ and by the minimal basis $\{x_1^3, x_1 x_2^3, x_2^4\}$.

Example 11. Let us consider the value $n = 35, m = 12, \alpha = \frac{4095}{35} = 117$ and $O := \{2i - 1, 1 \leq i \leq 17\}$. Let the primary defining set of our code be $S = \{1, 3\}$. The 35-th roots of unity, namely the powers of a^{117} : $\mathcal{R}_{35} = \{a^{117}, a^{234}, \dots, a^{3978}, a^{4095} = 1\}$. The 117 classes induced by the 35-st roots of unity are divided in this way:

$[0] = \{1 + a^{2925}, 1 + a^{585}, (1 + a^{1755})\}$ and for each $u' \in \mathcal{R}_{35} \setminus \{a^{2925}, a^{585}, a^{1755}, a^{4095}\}, \{1 + u'\} = [k]$ where $1 + u = a^k, k \equiv u \pmod{117}$.

The $(4095, 35; O)$ -Zech Tableau is given by the sequence

$$[0, 113, 106, 78, 116, 29, 58, 115, 53, 39, 73, 85, 95, 101, 109]$$

with $\zeta(0) = 3, \zeta(113) = \zeta(106) = \zeta(78) = \zeta(116) = \zeta(29) = \zeta(58) = \zeta(115) = \zeta(53) = \zeta(39) = \zeta(73) = \zeta(85) = \zeta(95) = \zeta(101) = \zeta(109) = 1$ and the minimal basis $\{x_1^{15}, x_1 x_2, x_2^3\}$.

8. Degroebnerizing Error Correcting Codes (2)

In this section, we deal with the case of codes such that $n \mid 2^m - 1$ with primary defining set $S_C = \{1, l\}$.

The escalier's shape is far from being trivial, and Zech tableaux will be used to study the escalier's shape.

Experiments showed that, for binary cyclic codes C over $GF(2^m)$, with length $n \mid 2^m - 1$ and *primary* defining set $S_C = \{1, l\}$, the $(2^m - 1, n; O)$ -Zech Tableaux – with $O := \{2i - 1, 1 \leq i \leq \frac{n-1}{2}\}$ – describe the structure of Z_2 thus making effective the results of [9] and allowing to extend those of [7]. In particular [8] reports (and proves) the following result. Still denoting a a primitive $(2^m - 1)^{\text{th}}$ root of unity, $\alpha := \frac{2^m - 1}{n}$ and $b := a^\alpha$ a primitive n^{th} root of unity, we consider the $(2^m - 1, n; O)$ -Zech Tableaux with

- ordered sequence $S := [j_0, \dots, j_{r-1}] \subset \{i, 0 \leq i < \alpha\}$,
- minimal basis $G = \{t_1, \dots, t_r\}$, $t_i := x_1^{a_i} x_2^{b_i}$,

and let us enumerate

- each Z_{j_i} as $Z_{j_i} = [\beta_{i1}, \dots, \beta_{i\zeta(i)}]$

Then it holds.

- (A). the minimal basis of $\mathbf{T}(J_2)$ is $G_2 = \{\tau_1, \dots, \tau_r\}$, $\tau_i := x_1^{na_i} x_2^{b_i}$, so that
- (B). $N_2 := \bigsqcup_{i=1}^{r-1} \{x_1^a x_2^b : 0 \leq a < na_i, 0 \leq b < b_{i+1}\}$ correlated to Z_2 via
- (C). the Cerlienco-Mureddu correspondence

$$\Phi_2 \left(b^\ell (1 + b^{\beta_n}), b^{\ell\ell} (1 + b^{\beta_n}), b^\ell, b^{\ell + \beta_n} \right) = (x_1^{(i-1) + \ell} x_2^1).$$

- (D). Also in this more general frame the HELP has still a very sparse formula:

$$h(z_1, x_1, x_2) = z_1 - \sum_{j=0}^{\alpha-1} x_1^{nj+1} \sum_{i=0}^{\zeta(i)-1} a_{ji} (x_1^{-l} x_2)^i,$$

- (E). where the unknown coefficient can be deduced by Lundqvist interpolation on the set of points

$$\left\{ \left((1 + b^{\beta_n}), (1 + b^{\beta_n}), 1 \right) \right\}.$$

Example 10 (cont.). We have

$$N_2 = \{1, x_1, \dots, x_1^{62}, x_2, x_1 x_2, \dots, x_1^{62} x_2, x_2^2, x_1 x_2^2, \dots, x_1^{62} x_2^2, x_2^3, x_1 x_2^3, \dots, x_1^{20} x_2^3\}$$

corresponding to $G_2 = \{x_1^{63}, x_1^{21} x_2^3, x_2^4\}$ and HELP

$$z_1 + a^{47} x_1^{13} x_2^3 + a^{33} x_1^{58} x_2^2 + a^{47} x_1^{37} x_2^2 + a^{12} x_1^{16} x_2^2 + a^{41} x_1^{61} x_2 + a^{32} x_1^{40} x_2 + a^{47} x_1^{19} x_2 + a^{27} x_1^{43} + a^{42} x_1^{22} + a^9 x_1$$

Example 11 (cont.). We have

$$N_2 = \{1, x_1, \dots, x_1^{524}, x_2, x_1 x_2, \dots, x_1^{34} x_2, x_2^2, x_1 x_2^2, \dots, x_1^{34} x_2^2\}$$

corresponding to $G_2 = \{x_1^{525}, x_1^{35} x_2, x_2^3\}$ and HELP

$$z_1 + a^{3510} x_1^{30} x_2^2 a^{2340} x_1^{33} x_2 + a^{3381} x_1^{491} + a^{1140} x_1^{456} + a^{608} x_1^{421} + a^{56} x_1^{386} + a^{3477} x_1^{351} + a^{2238} x_1^{316} + a^{3445} x_1^{281} + a^{3709} x_1^{246} + a^{2260} x_1^{211} + a^{3761} x_1^{176} + a^{510} x_1^{141} + a^{400} x_1^{106} + a^{1044} x_1^{71} + a^{141} x_1^{36} + a^{1663} x_1$$

References

- [1] M.E. Alonso, M.G. Marinari, T. Mora, *The Big Mother of All the Dualities, II: Macaulay Bases*, *Appl. Algebra Engrg. Comm. Comput.* **17** (2006) 409–451.
- [2] D. Augot, M. Bardet, J.C. Faugere, Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases, *Proc. IEEE Int. Symp. Information Theory 2003*, (2003) .
- [3] D. Augot, M. Bardet, J.C. Faugere, On formulas for decoding binary cyclic codes, *Proc. IEEE Int. Symp. Information Theory 2007*, (2007) .
- [4] M. Caboara, T. Mora The Chen-Reed-Helleseth-Truong Decoding Algorithm and the Gianni-Kalkbrenner Gröbner Shape Theorem, *Appl. Algebra Engrg. Comm. Comput.*, **13** (2002)
- [5] F. Caruso, E. Orsini, C. Tinnirello and M. Sala *On the shape of the general error locator polynomial for cyclic codes* *IEEE Trans. Inform. Theory* 63.6 (2017): 3641-3657.
- [6] M. Ceria, *A proof of the "Axis of Evil theorem" for distinct points*, *Rend. Semin. Mat. Univ. Politec. Torino*, Vol. 72 No. 3-4, pp. 213-233 (2014)
- [7] M. Ceria, T. Mora, M. Sala, *HELP: a sparse error locator polynomial for BCH codes*, submitted.
- [8] M. Ceria, *Half error locator polynomials for efficient decoding of binary cyclic codes*, in preparation.
- [9] M. Ceria, *Macaulay, Lazard and the Syndrome Variety*, arxiv preprint arXiv:1910.13189 [math.CO].
- [10] M. Ceria, T. Mora, *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game*, arxiv preprint arXiv:1805.09165.
- [11] L. Cerlienco, M. Mureddu, *Algoritmi combinatori per l'interpolazione polinomiale in dimensione ≥ 2* , *Sém. Lothar. Combin*, B34e (1995).
- [12] L. Cerlienco, M. Mureddu, *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, *Discrete Math.* **139**, (1995) 73-87.
- [13] L. Cerlienco, M. Mureddu, *Multivariate Interpolation and Standard Bases for Macaulay Modules*, *J. Algebra* **251** (2002), 686-726.
- [14] X. Chen, I. S. Reed, T. Helleseth, K. Truong, Use of Gröbner Bases to Decode Binary Cyclic Codes up to the True Minimum Distance, *IEEE Trans. Inform. Theory*, **40** (1994) , 1654–1661.
- [15] X. Chen, I. S. Reed, T. Helleseth, K. Truong, General Principles for the Algebraic Decoding of Cyclic Codes, *IEEE Trans. Inform. Theory*, **40** (1994) , 1661–1663.

- [16] X. Chen, I. S. Reed, T. Helleseht, K. Truong, Algebraic decoding of cyclic codes: A polynomial Ideal Point of View, *Contemp. Math.*, **168** (1994), 15–22
- [17] A.B. III Cooper, Direct solution of BCH decoding equations, In E. Arikan (Ed.) *Comm. Control and Signal Processing*, 281–286, Elsevier (1990)
- [18] A.B. III Cooper, Finding BCH error locator polynomials in one step *Electron. Letters*, **27** (1991) 2090–2091
- [19] D. Lazard, *Ideal Bases and Polynomial Decomposition: Case of Two Variables*, *J. Symbolic Comput.* **1** (1985), 261–270
- [20] P. Gianni, Properties of Gröbner bases under specialization, step *Lecture Notes in Comput. Sci.*, **378** 293–297, (1991)
- [21] M. Kalkbrenner, Solving systems of algebraic equations using Gröbner bases, step *Lecture Notes in Comput. Sci.*, **378** 282–292, (1991)
- [22] P. Loustau, E.V. York, On the decoding of cyclic codes using Gröbner bases, *Appl. Algebra Engrg. Comm. Comput.*, **8** (1997) 469–483.
- [23] S. Lundqvist, *Vector space bases associated to vanishing ideals of points*, *J. Pure Appl. Algebra* **214** (2010), 309–321.
- [24] M.G. Marinari, T. Mora, H.M. Moeller, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, *Appl. Algebra Engrg. Comm. Comput.* **4** (1993), 103–145.
- [25] M.G. Marinari, T. Mora, *A remark on a remark by Macaulay or Enhancing Lazard Structural Theorem*, *Bull. of the Iranian Math. Soc.* **29** n 1 (2003), 103–145;
- [26] T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016)
- [27] T. Mora, *An FGLM-like algorithm for computing the radical of a zero-dimensional ideal*. *J. Algebra Appl.*, **17**(01) (2018).
- [28] B. Mourrain, *A New Criterion for Normal Form Algorithms* In: Fossorier M., Imai H., Lin S., Poli A. (eds) *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAEECC 1999. Lecture Notes in Comput. Sci.*, **1719**. Springer, Berlin, Heidelberg (1999)
- [29] E. Orsini, T. Mora., *Decoding cyclic codes: the Cooper Philosophy*. in M.Sala et al., *Groebner Bases, Coding, and Cryptography*. Springer (2009), 62–92
- [30] E. Orsini, M. Sala, *Correcting errors and erasures via the syndrome variety*, it *J. Pure Appl. Algebra*, **200** (2005), 191–226.

AMS Subject Classification: 05E40, 14G50, 11T71

M. Ceria, T. Mora, M. Sala

Lavoro pervenuto in redazione il 31.07.2019.