The Chen-Reed-Helleseth-Truong Decoding Algorithm and the Gianni-Kalkbrenner Gröbner Shape Theorem

Massimo Caboara
DIMA, Univ. Genova,
Viale Dodecaneso 35, 16146 Genova, Italy,
caboara@dima.unige.it

Teo Mora
DISI, Univ. Genova,
Viale Dodecaneso 35, 16146 Genova, Italy,
theomora@dima.unige.it

March 17, 2003

Abstract

In a paper from Chen, Reed, Helleseth and Truong, [4] (cf. also Loustaunau and York [10]) Gröbner bases are applied as a preprocessing tool in order to devise an algorithm for decoding a cyclic code over $GF(q)$ of length n. The Gröbner basis computation of a suitable ideal allows us to produce two finite ordered lists of polynomials over $GF(q)$,

$$\{\Gamma_i(X_1,\dots,X_s)\} \text{ and } \{\mathrm{G_i}(\mathrm{X_1},\dots,\mathrm{X_s},\mathrm{Z})\};$$

upon the receipt of a codeword, one needs to compute the syndromes $\{\mathsf{s}_1,\dots,\mathsf{s}_s\}$ and then to compute the maximal value of the index i s.t. $\Gamma_i(\mathsf{s}_1,\dots,\mathsf{s}_s)=0$; the error locator polynomial is then

$$\gcd(G_i(\mathsf{s}_1,\dots,\mathsf{s}_s,Z),Z^n-1).$$

The algorithm proposed in [4] needs the assumption that the computed Gröbner basis associated to a cyclic code has a particular structure; this assumption is not satisfied by every cyclic code. However the structure of the Gröbner basis of a 0-dimensional ideal has been deeply analyzed by Gianni [7] and Kalkbrenner [8]. Using these results we were able to generalize the idea of Chen, Reed, Helleseth and Truong to all cyclic codes.

Introduction

This paper has the following structure:

In the first section, we describe the coding theory problem we are dealing with and the tools from Gröbner basis theory we need. We give a very brief introduction (mainly notational) to both cyclic code and Gröbner bases theory, to the extent necessary for the non-conversant in one of the subjects to follow the algorithm description.

In the second section, we describe the Chen-Reed-Helleseth-Truong decoding algorithm, with the modifications due to Loustaunau and York.

In the third section, we describe the structure of the Gröbner basis of a zero-dimensional ideal, i.e. the Gianni-Kalkbrenner Shape Theorem.

In the fourth section, we give the correct and optimized version of the Chen-Reed-Helleseth-Truong decoding algorithm, based on the Shape Theorem.

A full example, taken from [4, 10], is provided in the fifth section, while in the sixth (and last) section we present some conclusions and some remarks on the complexity.

*Acknowledgments This paper, whose results were informally presented at the Conference AAECC-11, has been written while the second author was visiting Prof. Cannon (University of Sydney) and during his sabbatical visit at Florida State University.

1 The setting

We introduce here the notations and hypothesis from Coding Theory and Gröbner bases theory that we need in the remained of this paper. Since the repetition of these notations and hypothesis is often unwieldy, in the following sections, when not explicitly stated, they are taken for granted, especially in the stating of propositions and theorems.

1.1 Decoding a cyclic code

Let $\mathcal{C} \subset \mathrm{GF}(q)[X]/(X^n - 1) =: GF(q)[x]$ be a cyclic code over $\mathrm{GF}(q)$ of length n, minimum distance d, dimension k and generator polynomial $g(x) \in \mathrm{GF}(q)[x]$. We assume $\gcd(n, q) = 1$.

The splitting field of $X^n - 1$ containing all the n^{th} roots of unity over $\mathrm{GF}(q)$ is $\mathrm{GF}(q^D) = \mathrm{GF}(q)[\alpha]$ where D is the multiplicative order of $q \bmod n$, i.e.

$$D := Min\{m \in \mathbb{N} \mid q^m \equiv 1 \mod n)\}$$

and α is any primitive n^{th} root of unity. Note that $D \leq n$.

Let $\alpha \in \mathrm{GF}(q^D)$ be a primitive n^{th} root of unity and $\phi_i(x)$, $0 \leq i < n$, the minimal polynomials of α^i over $\mathrm{GF}(q)$; therefore there are indices $\{i_1, \ldots i_s\}$

such that

$$g(x) = \prod_{j=1}^{s} \phi_{i_j}(x)$$

Let $r(x) \in GF(q)[x]$ be a word received through a noisy channel; there is at most one error pattern

$$e(x) = \sum_{l=1}^{\mu} a_l x^{k_l} \in GF(q)[x]$$

s.t. $c(x) := r(x) - e(x) \in \mathcal{C}$ and whose weight μ satisfies

$$\mu \leq \mathsf{t} := \lfloor \frac{\mathsf{d}-1}{2} \rfloor;$$

the magnitudes and locations of this error pattern are, respectively,

$$\{a_1, \ldots, a_\mu\} \subset \mathrm{GF}(q)$$

and

$$\{k_1, \ldots, k_\mu\}, 1 \leq k_1 < k_2 \cdots < k_\mu \leq n$$

The locations of the error pattern are coded within the error locator polynomial

$$L(z) := \prod_{l=1}^{\mu} (z - \alpha^{k_l}).$$

Once the locations are detected, the error magnitudes may be found using the Forney formula [6].

For $1 \leq j \leq s$, let us consider the syndromes $\mathsf{s}_j \in \mathrm{GF}(q)[\alpha] = \mathrm{GF}(q^D)$ (remember that by construction $c(\alpha^{i_j}) = 0$)

$$\mathsf{s}_j = r(\alpha^{i_j}) = e(\alpha^{i_j}) = \sum_{l=1}^{\mu} a_l \ (\alpha^{i_j})^{k_l} = \sum_{l=1}^{\mu} a_l \ (\alpha^{k_l})^{i_j} = \sum_{l=1}^{j} a_l \beta_l^{i_j}$$

where $\mu \leq j \leq \mathsf{t}$ and

$$\beta_l := \begin{cases} \alpha^{k_l} & \text{if } l \leq \mu \\ 0 & \text{if } \mu < l \leq j \end{cases}$$

Since it is well-known that the syndromes are unique for each error pattern of weight $\mu \leq \mathsf{t}$, our aim is to find such error pattern $e(X)$ in order to decode the received word $r(x)$ as $c(x) := r(x) - e(x) \in \mathcal{C}$; all we need is to compute the weight μ and the error locator polynomial $L(z)$.

To do that,[4] proposed to compute the roots of the polynomials

$$\sum_{l=1}^{j} a_l \beta_l^{i_j} - s_j, \qquad 1 \le j \le s \tag{1}$$

w.r.t. the indeterminates a_l's and β_l's, keeping the syndromes s_j as parameters. In practice, [4] computes a special form (a Gröbner basis) of the system comprising equations (1) plus some other auxiliary equations. Once the word $r(x)$ is received and the syndromes s_j are computed, it is just sufficient to evaluate such system at them in order to deduce μ and $L(z)$ and so computing the maximum likelihood decoded word $c(x)$.

1.2 Gröbner tools

Throughout this subsection, P stands for $K[x_1, \dots, x_n]$, where K is a field, and $\mathbf{T}$ denotes the commutative semigroup generated by $x_1, \dots, x_n$ i.e.

$$\mathbf{T} := \{x_1^{a_1} \cdots x_n^{a_n}, a_i \in \mathbb{N}\}.$$

A *term-ordering* on P is any semigroup well-ordering $<$ on $\mathbf{T}$, i.e. any total ordering $<$ such that

$t > t' \Longrightarrow mt > mt'$ for any $m, t, t' \in \mathbf{T}$

$t > 1$ for any $t \in \mathbf{T}, t \neq 1$.

All over the paper, we will use only the *lexicographic term ordering induced by* $x_1 < \cdots < x_n$ defined by

$$x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n} \iff \exists j : b_i = a_i, \forall i > j, \text{and } b_j > a_j,$$

i.e.

$$\begin{cases} a_n < b_n & \text{or} \\ a_n = b_n, a_{n-1} < b_{n-1} & \text{or} \\ \qquad \vdots & \\ a_n = b_n, \dots, a_2 = b_2 & \text{and } a_1 < b_1 \end{cases}$$

Once a term-ordering $<$ is fixed, each element $f \in P$ can be uniquely expressed as

$$f = \sum c_i \tau_i, c_i \in K \setminus \{0\}, \tau_i \in \mathbf{T}, \tau_1 > \tau_2 > \cdots$$

and we will denote $\mathbf{T}(f) := \tau_1$ its *leading term* (w.r.t. $<$); for each set $G \subset P$, $\mathbf{T}(G)$ denotes the set $\{\mathbf{T}(g) : g \in G\}$.

Example 1.1 *Let $<$ be the lexicographic term ordering induced by $x < y < z$ on $\mathbb{Q}[x, y, z]$. The following polynomials of $\mathbb{Q}[x, y, z]$ are written in descending $<$ order.*

$$z + y^2 + x^2y + x + 1$$
$$z^2 + z + x^5y^3 + x^7y^2 + y + x^5 + 1$$

and their leading terms are z and z^2 respectively.

Definition 1.2 Let $\mathcal{F} = \{f_1, \ldots, f_t\}$ be a set of polynomials of P, I the ideal generated by $\mathcal{F}$ and $<$ a term-ordering on P. If the ideal $(\mathbf{T}(f_1), \ldots, \mathbf{T}(f_t))$ is equal to the ideal generated by $\{\mathbf{T}(f) \mid f \in I\}$ then $\mathcal{F}$ is a *Gröbner basis* of I with respect to $<$.

Remark 1.3 Given any $\{f_1, \ldots, f_t\} \subset P$, a system of generators of the ideal I, and any term-ordering $<$ on P, Gröbner basis of I with respect to $<$ can be computed by means of Buchberger Algorithm.

Remark 1.4 Given a multivariate polynomial ring $P = K[x_1, .., x_n]$ over a field, Buchberger Theory of Gröbner bases considers each polynomial as a linear combination of terms in $\mathbf{T}$ with coefficients on the field K.

In order to describe the structure of the Gröbner basis of an ideal, one needs to consider P also as a univariate polynomial with coefficients in the polynomial ring $K[x_1, .., x_{n-1}]$ i.e. as $P = K[x_1, .., x_{n-1}][x_n]$.

In this context each element $f \in P$ can be uniquely expressed as

$$f = \sum_{i=0}^{d} g_i(x_1, .., x_{n-1})x_n^i, g_i(x_1, .., x_{n-1}) \in K[x_1, .., x_{n-1}], g_d(x_1, .., x_{n-1}) \neq 0.$$

$Lp(f) := g_d(x_1, .., x_{n-1})$ and $Tp(f) := g_0(x_1, .., x_{n-1})$ will denote respectively the *leading polynomial* and the *trailing polynomial* of f.

For example, the leading and trailing polynomials of

$$f = xz^2 + yz^2 + x^3z + x^2 + y = z^2(x + y) + (x^3)z + (x^2 + y) \in \mathbb{Q}[x, y][z]$$

are $Lp(f) = x + y \in \mathbb{Q}[x, y]$ and $Tp(f) = x^2 + y \in \mathbb{Q}[x, y]$.

We recall that

Definition 1.5 For any ideal $I \subset K[x_1, \ldots, x_n]$, denoting $\mathcal{K}$ the algebraic closure of K, and

$$\mathcal{Z}(I) := \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{K}^n : f(\alpha_1, \ldots, \alpha_n) = 0, \forall f \in I\},$$

the following conditions

1. the set $\mathcal{Z}(I)$ of all the roots of I is finite;
2. $\forall i, \exists p_i \in I \cap K[x_i]$;
3. $K[x_1, \ldots, x_n]/I$ is a finite dimensional K-vector space;
4. $\forall i, \exists d_i$ s.t. $X_i^{d_i} \in \mathbf{T}(I)$ (w.r.t. any ordering)

are equivalent and an ideal satisfying them is called *0-dimensional*.

1.3 Notation

As we said above, in order to decode a received word $r(x)$, [4] proposed to evaluate the Gröbner basis of the polynomial equation system comprising the equations (1) plus some other auxiliary equations at the syndromes s_j, in order to deduce μ and $L(z)$ and so computing the maximum likelihood decoded word $c(x)$.

Let us choose a value $\nu \leq \mathtt{t}$ and consider the polynomial rings

$$\begin{aligned}
\mathcal{P}_{XZY} &:= \mathrm{GF}(q)[X_1, X_2, \ldots, X_s, Z_\nu, Z_{\nu-1}, \ldots, Z_1, Y_1, \ldots, Y_\nu], \\
\mathcal{P}_{XZ} &:= \mathrm{GF}(q)[X_1, X_2, \ldots, X_s, Z_\nu, Z_{\nu-1}, \ldots, Z_1], \\
\mathcal{P}_{X} &:= \mathrm{GF}(q)[X_1, X_2, \ldots, X_s].
\end{aligned}$$

where

X_j stands for the syndrome s_j, $1 \leq j \leq s$;

Z_l represents the algebraic number β_l, $1 \leq l \leq \nu$;

Y_l stands for the magnitude a_l, $1 \leq l \leq \nu$.

The equations (1) give the polynomials

$$f_j \quad := \quad \sum_{l=1}^{j} Y_l Z_l^{i_j} - X_j, \quad 1 \leq j \leq s$$

and the variables $\mathbf{X}$,$\mathbf{Y}$ and $\mathbf{Z}$ satisfy the relations

$$\begin{array}{lll}
\sigma_j := X_j^D - X_j, & 1 \leq j \leq s, & \text{since } s_j \in \mathrm{GF}(q^D); \\
h_i := Z_i^{n+1} - Z_i, & 1 \leq i \leq \nu; & \text{since } \beta_l \text{ are } n\text{-root of unity or zero ;} \\
\lambda_i := Y_i^{q-1} - 1, & 1 \leq i \leq \nu, & \text{since } a_l \in \mathrm{GF}(q) \setminus \{0\}.
\end{array}$$

The polynomial equation system introduced by [4] is then

$$\mathcal{F} := \{f_j, \sigma_j, h_i, \lambda_i : 1 \leq j \leq s, 1 \leq i \leq \nu\}.$$

$I \subset \mathcal{P}_{XZY}$ will denote the ideal generated by $\mathcal{F}$ and will be called the *syndrome ideal*; $\mathcal{G}$ will denote its Gröbner basis w.r.t. the lexicographical order induced by

$$X_1 < X_2 < \ldots < X_s < Z_\nu < Z_{\nu-1} < \ldots < Z_1 < Y_1 < \ldots < Y_\nu.$$

Remark 1.6 Consider the subsystem

$$\mathcal{F}' := \{f_j, h_i, \lambda_i : 1 \le j \le s, 1 \le i \le \nu\}$$

and the ideal I' generated by it. Since, under the lexicographical order induced by

$$Z_\nu < Z_{\nu-1} < \ldots < Z_1 < Y_1 < \ldots < Y_\nu < X_1 < \ldots < X_{s-1} < X_s$$

one has

$$\mathbf{T}(f_j) = X_j, \mathbf{T}(\lambda_i) = Y_i^{q-1}, \mathbf{T}(h_i) = Z_i^{n+1}$$

we can immediately deduce that I', and hence I, are 0-dimensional.

In [4] the syndrome ideal considered is the one generated by $\mathcal{F}'$ and the polynomials σ_j are not considered.

In fact, they are not even necessary to guarantee that I is 0-dimensional in order to apply Gianni-Kalkbrenner result as we will do in § 4, but, on the other side, it is sufficient to compare the computation proposed in [10] with the one performed in § 5 to realize the crucial role of the σ_j's to simplify the output and the corresponding decoding algorithm.

The effective rôle of the polynomials σ_j, λ_i, h_i is essentially that of removing among the roots of the systems, those which live in algebraic extensions and stripping the other roots of their multiplicity – and so giving a "simpler" polynomial system – according to the following

Fact 1.7 *Let $\mathcal{K}$ be the algebraic closure of $GF(q)$. For any 0-dimensional ideal $I \subset GF(q)[x_1, \ldots, x_n]$ denote*

$$\mathcal{Z}(I) := \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{K}^n : f(\alpha_1, \ldots, \alpha_n) = 0, \forall f \in I\}.$$

and

$$\forall m \in \mathbb{N}, I_m := I + (x_i^{q^m} - x_i : 1 \le i \le n).$$

Then, $\forall m \in \mathbb{N}$, all the roots of I_m are simple and they are

$$\mathcal{Z}(I_m) = \mathcal{Z}(I) \cap GF(q^m)^n.$$

Proof. Cf. [2] □

2 The Chen-Reed-Helleseth-Truong Decoding Algorithm

In the paper [4] a decoding algorithm for the code $\mathcal{C}$ is presented based on the following

Theorem 2.1 *Assume that*

$$\mathcal{G} = \mathcal{G}_X \cup \{g_\nu, g_{\nu-1}, \dots, g_1\} \cup \mathcal{G}_Y,$$

where

– $\forall g \in \mathcal{G}_X, g \in P_X$;

– $\forall i, \nu \geq i \geq 1$, $g_i \in P_X[Z_\nu, \dots, Z_{i+1}][Z_i] \setminus P_X[Z_\nu, \dots, Z_{i+1}]$, *so that*

- $g_i = \sum_{\delta=0}^{\Delta_i} \gamma_{i\delta} Z_i^\delta$,
- $\gamma_{i\delta} \in P_X[Z_\nu, \dots, Z_{i+1}]$, $\forall \delta$;

– $\forall g \in \mathcal{G}_Y, g \in \mathcal{P}_{XZY} \setminus \mathcal{P}_{XZ}$.

Then, setting μ *to be the value s.t.*

* $\gamma_{i0}(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0) = 0, i > \mu$,

* $\gamma_{\mu 0}(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0) \neq 0$,

it holds:

- *there are exactly* μ *errors in the received word* $r(x)$;
- *the error locator polynomial is*

$$L(z) := \gcd\left(g_\mu(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, z), z^n - 1\right). \quad \square$$

Exploiting theorem 2.1, it is easy the develop an algorithm for the computation of the error locator polynomial.

The CRHT algorithm consists of the following steps :

- precomputing the Gröbner basis $\mathcal{G}$ of I,
- storing $\forall i, \nu \geq i \geq 1$, the polynomials

$$\begin{aligned} \Gamma_i(X_1, \dots, X_s) &:= \gamma_{i0}(X_1, \dots, X_s, 0, \dots, 0) = \\ &= Tp(g_i)(X_1, \dots, X_s, 0, \dots, 0), \\ G_i(X_1, \dots, X_s, Z_i) &:= g_i(X_1, \dots, X_s, 0, \dots, 0, Z_i) \end{aligned}$$

- and, for any received word $r(x)$,
  - computing the syndromes $\mathsf{s}_j, 1 \leq j \leq s$,
  - and applying the algorithm in Fig. 1.

Figure 1: The CRHT decoding algorithm

Input $\{\Gamma_i\}$, $\{G_i\}$

$\mu := \nu$

While $\Gamma_\mu(\mathsf{s}_1, \ldots, \mathsf{s}_s) = 0$ **do** $\mu := \mu - 1$

$L(z) := \gcd\left(G_\mu(\mathsf{s}_1, \ldots, \mathsf{s}_s, z), z^n - 1\right)$

Output μ, $L(z)$

Remark 2.2
Clearly (cf. [4]), $\forall i$ if $g_i(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z) \neq 0$ then it is annihilated by each $\alpha^{k_j}, 1 \leq j \leq \mu$, and in case $i > \mu$ it is also satisfied by 0.

Therefore it holds

- $g_i(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z) = 0, \forall i < \mu;$
- $g_\mu(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z) = L(z);$
- $g_{\mu+1}(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z) = zL(z);$
- $g_i(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z)$ is multiple of $zL(z), \forall i > \mu + 1$.

This implies also that the following conditions

1. $\deg(L) \leq m$
2. $Tp(g_i)(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) = \gamma_{i0}(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) = 0, \forall i > m$

are equivalent.

3 The Gianni-Kalkbrenner Gröbner Shape Theorem

The shape of the Gröbner basis $\mathcal{G}$ is usually not the one which Theorem 2.1 assumes. Gröbner bases shape has been completely described by Gianni [7] and

Kalkbrenner [8] (but cf. also the seminal paper [9] by Lazard), whose result can be summarized in the following

Theorem 3.1 *Let $I \subset \mathcal{P} := K[T_1, \ldots, T_n]$ be a 0-dimensional ideal and let $\mathcal{G}$ be a Gröbner basis of I with respect to the lexicographical ordering induced by $T_1 < \ldots < T_n$. Then*

$$\mathcal{G} = \bigcup_{i=1}^{n} \mathcal{G}_i = \bigcup_{i=1}^{n} \bigcup_{\partial=1}^{\Delta_i} \mathcal{G}_{i\partial}$$

and:

1. *For each i, ∂, if $g \in \mathcal{G}_{i\partial}$, we have that*
   - *$g \in K[T_1, \ldots, T_{i-1}][T_i] \setminus K[T_1, \ldots, T_{i-1}]$,*
   - *the degree of g w.r.t. T_i is ∂, $\deg_{T_i}(g) = \partial > 0$,*

   and if we order $\mathcal{G}_{i\partial} := \{g_{i\partial j}, 1 \leq j \leq j_{i\partial}\}$ in such a way that

   $$J < j \iff \mathbf{T}(g_{i\partial J}) < \mathbf{T}(g_{i\partial j})$$

   we obtain

   $$\mathbf{T}(g_{IDJ}) < \mathbf{T}(g_{i\partial j}) \iff \begin{cases} I < i, & or \\ I = i, D < \partial, & or \\ I = i, D = \partial, J < j. & \end{cases} \tag{2}$$

2. *Let $(\tau_1, \ldots, \tau_{i-1}) \in \mathcal{K}^{i-1}$ be a root of $I \cap K[T_1, \ldots, T_{i-1}]$ – where $\mathcal{K}$ denotes the algebraic closure of K. We have*

   $$g(\tau_1, \ldots, \tau_{i-1}) = 0 \ \forall\ g \in \mathcal{G}_I, I < i$$

   and on $\mathcal{G}_i$ there is the following structure:

   let us order the polynomials in $\mathcal{G}_i$ by increasing leading terms, i.e. using (2). Then, if $g_{i\partial j}$ is the first polynomial in $\mathcal{G}_i$ s.t.

   $$Lp(g_{i\partial j})(\tau_1, \ldots, \tau_{i-1}) \neq 0$$

   i. e. whose leading polynomial evaluated in $(\tau_1, \ldots, \tau_{i-1})$ is non null, then $g_{i\partial j}$ is the first polynomial in $\mathcal{G}_i$ s.t.

   $$g_{i\partial j}(\tau_1, \ldots, \tau_{i-1}, T_i) \neq 0$$

   i.e. whose evaluation in $(\tau_1, \ldots, \tau_{i-1}, T_i)$ is non null.

   Moreover if $(g_{iDJ}) \in \mathcal{G}_i$ is s.t. $\mathbf{T}(g_{iDJ}) > \mathbf{T}(g_{i\partial j})$ then

   $$g_{i\partial j}(\tau_1, \ldots, \tau_{i-1}, T_i) \text{ divides } g_{iDJ}(\tau_1, \ldots, \tau_{i-1}, T_i).$$

We can describe more explicitly the structure of $\mathcal{G}_i$ in the following way: let ∂, j, with $1 \le \partial \le \Delta_i$, $1 \le j \le j_{iD}$ be such that

- $Lp(g)(\tau_1, \dots, \tau_{i-1}) = 0\ \forall\ g \in \mathcal{G}_{i,D}, \forall D < \partial$;
- $Lp(g_{i\partial J})(\tau_1, \dots, \tau_{i-1}) = 0\ \forall J < j$;
- $Lp(g_{i\partial j})(\tau_1, \dots, \tau_{i-1}) \neq 0$

Then

- $g(\tau_1, \dots, \tau_{i-1}, T_i) = 0\ \forall\ g \in \mathcal{G}_{i,D}, \forall D < \partial$;
- $g_{i\partial J}(\tau_1, \dots, \tau_{i-1}, T_i) = 0\ \forall J < j$;
- $g_{i\partial j}(\tau_1, \dots, \tau_{i-1}, T_i) \neq 0$;
- $g_{i\partial j}(\tau_1, \dots, \tau_{i-1}, T_i)$ *divides* $g_{i\partial J}(\tau_1, \dots, \tau_{i-1}, T_i)\ \forall J > j$;
- $g_{i\partial j}(\tau_1, \dots, \tau_{i-1}, T_i)$ *divides* $g(\tau_1, \dots, \tau_{i-1}, T_i)\ \forall\ g \in \mathcal{G}_{i,D}, \forall D > \partial$.

Proof. For a proof we refer to [7, 8]. □

Example 3.2 To illustrate Theorem 3.1, which gives, in fact, a much, much more complex Gröbner Basis characterization than Theorem 2.1, we consider the ideal $I \subset \mathbb{Z}_2[T_1, T_2, T_3, T_4]$ generated by (f_1, f_2, f_3, f_4) where

$$f_1 := T_4 + T_3 + T_2, f_2 := T_4^3 + T_3^3 + T_1, f_3 := T_3^{16} + T_3, f_4 := T_4^{16} + T_4,$$

whose Gröbner basis is $\{h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8\}$ where

$$\begin{array}{lcl}
h_1 := g_{1\ 16\ 1} &=& \mathbf{1}T_1^{16} + T_1, \\
h_2 := g_{2\ 3\ 1} &=& (\mathbf{T_1^{11}} + \mathbf{T_1^6} + \mathbf{T_1})T_2^3 + T_1^{12} + T_1^7 + T_1^2, \\
h_3 := g_{2\ 9\ 1} &=& \mathbf{T_1}T_2^9 + T_1^2T_2^6 + T_1^8T_2^3 + T_1^4, \\
h_4 := g_{2\ 16\ 1} &=& \mathbf{1}T_2^{16} + T_2, \\
h_5 := g_{3\ 2\ 1} &=& \mathbf{T_1}T_3^2 + (T_1T_2)T_3 + \\
 & & +T_2^8T_1^9 + T_2^8T_1^4 + T_2^5T_1^{10} + T_2^5T_1^5 + T_2^2T_1^6 + T_2^2T_1, \\
h_6 := g_{3\ 2\ 2} &=& \mathbf{T_2}T_3^2 + T_2^2T_3 + T_2^3 + T_1, \\
h_7 := g_{3\ 16\ 1} &=& \mathbf{1}T_3^{16} + T_3, \\
h_8 := g_{4\ 1\ 1} &=& \mathbf{1}T_4 + T_3 + T_2T_3^{16} + T_3.
\end{array}$$

and the **bold** term of each h_i is its leading polynomials $Lp(h_i)$. Note that an (incomplete) factorization of $g_{1\ 16\ 1} = T_1^{16} + T_1$ is

$$g_{1\ 16\ 1} = T_1(T_1^{10} - T_1^5 + 1)(T_1^5 + 1).$$

Among the 16 roots of $g_{1\ 16\ 1}$:

– $\tau_1 = 0$ is s.t.

- $Lp(h_4)(0) \neq 0$;
- $h_i(0, T_2) = 0, \forall i \leq 3$,

- each root τ_1 of $T_1^{10} + T_1^5 + 1 = \frac{Lp(h_2)}{Lp(h_3)}$ is s.t.
  - $Lp(h_3)(\tau_1) \neq 0$,
  - $h_1(\tau_1, T_2) = h_2(\tau_1, T_2) = 0$,
  - $h_4(T_2) = \tau_1^{-1} h_3(\tau_1, T_2)(T_2^7 + \tau_1 T_2^4 + \tau_1^{12} T_2)$;
- each root τ_1 of $T_1^5 + 1 = \frac{h_1}{Lp(h_2)}$ is s.t.
  - $Lp(h_2)(\tau_1) \neq 0$,
  - $h_1(\tau_1, T_2) = 0$,
  - $h_3(\tau_1, T_2) = h_2(\tau_1, T_2)(T_2^6 + \tau_1^2)$,
  - $h_4(T_2) = \tau_1^{-1} h_2(\tau_1, T_2)(T_2^{13} + \tau_1 T_2^{10} + \tau_1^2 T_2^7 + \tau_1^3 T_2^4 + \tau_1^4 T_2)$.

Therefore the roots (τ_1, τ_2) of $I \cap K[T_1, T_2]$ are

- $\{(0, \beta) : \beta^{16} + \beta = 0\}$,
- $\{(\zeta, \delta) : \zeta^{10} + \zeta^5 + 1 = \delta^9 + \zeta\delta^6 + \zeta^7\delta^3 + \zeta^3 = 0\}$,
- $\{(\epsilon, \eta) : \epsilon^5 + 1 = \eta^3 + \epsilon = 0\}$.

Among these roots:

- $(\tau_1, \tau_2) := (0, 0)$ is s.t.
  - $Lp(h_7)(0, 0) \neq 0$,
  - $h_i(0, 0, T_3) = 0, \forall i \leq 6$;
- each root $(\tau_1, \tau_2) := \{(0, \beta) : \beta^{15} + 1 = 0\}$ is s.t.
  - $Lp(h_6)(0, \beta) \neq 0$,
  - $h_i(0, \beta, T_3) = 0, \forall i \leq 5$;
  - $\beta^{-1} h_7(T_3) = (\beta^{-1} T_3)^{16} - (\beta^{-1} T_3)$ is obviously a multiple of
  $$(\beta^{-1} T_3)^2 + (\beta^{-1} T_3) + 1 = \beta^{-2} h_6(0, \beta, T_3);$$
- while for the other roots (τ_1, τ_2)
  - $Lp(h_5)(\tau_1, \tau_2) \neq 0$
  - $\delta h_5(\zeta, \delta) = \zeta h_6(\zeta, \delta)$,
  - $\exists h(\zeta, \delta, T_3) : \zeta h_7(T_3) = h_5(\zeta, \delta) h(\zeta, \delta, T_3)$,
  - $\eta h_5(\epsilon, \eta) = \epsilon h_6(\epsilon, \eta)$,

– $\exists h(\epsilon, \eta, T_3) : \epsilon h_7(T_3) = h_5(\epsilon, \eta)h(\epsilon, \eta, T_3)$. $\square$

Example 3.3 A more elementary example which somehow explains better the relation between the different polynomials in $\mathcal{G}_{i\partial}$ is the ideal $I \subset \mathbb{Z}_2[T_1, T_2, T_3]$ generated by Gröbner basis $(f_1, f_2, f_3, f_4, f_5, f_6)$ where

$$f_1 := T_1^2 - T_1, f_2 := T_1T_2, f_3 := T_2^2 - T_2, f_4 := T_1T_3, f_5 := T_2T_3 - T_2, f_6 := T_3^2 - T_3$$

in which

- $I \cap \mathbb{Z}_2[T_1] = (T_1^2 - T_1)$ whose roots are $\{0, 1\}$:
  - for $\tau_1 = 0$ we have $I \cap \mathbb{Z}_2[0, T_2] = (0, 0, T_2^2 - T_2) = (T_2^2 - T_2)$ whose roots are $\{0, 1\}$:
    - for $(\tau_1, \tau_2) = (0, 0)$ we have
      $$I \cap \mathbb{Z}_2[0, 0, T_3] = (0, 0, 0, 0, 0, T_3^2 - T_3) = (T_3^2 - T_3)$$
      whose roots are $\{0, 1\}$;
    - for $(\tau_1, \tau_2) = (0, 1)$ we have
      $$I \cap \mathbb{Z}_2[0, 1, T_3] = (0, 0, 0, 0, T_3 - 1, T_3^2 - T_3) = (T_3 - 1)$$
      whose root is 1;
  - for $\tau_1 = 1$ we have $I \cap \mathbb{Z}_2[1, T_2] = (0, T_2, T_2^2 - T_2) = (T_2)$, whose root is 0 for which:
    - $I \cap \mathbb{Z}_2[1, 0, T_3] = (0, 0, 0, 0, T_3, 0, T_3^2 - T_3) = (T_3)$ whose root is 0.

4 Revisiting the CRHT Algorithm

Since Theorem 3.1 introduces the *degree* of the polynomials in the Gröbner basis, we can improve the result of Remark 2.2 by

Lemma 4.1 *Assume the weight of the error pattern of the received word $r(x)$ is exactly μ; let us fix $i, \mu \le i \le \nu$, and let us choose any element $g \in \mathcal{G}$ s.t.*

$$g \in \mathcal{P}_X[Z_\nu, \dots, Z_{i+1}][Z_i] \setminus \mathcal{P}_X[Z_\nu, \dots, Z_{i+1}].$$

Denoting $G(z) := g(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, z)$ (there are $\nu - i$ zeros) and $\delta := \deg(G)$, we have that:

1. *if $\delta < \mu$ then $G(z) = 0$;*
2. *if $\delta = \mu$ then*
   - *if $\mu = i$ then $G(z) = L(z)$;*
   - *if $\mu < i$ then $G(z) = 0$;*

3. *if* $\delta = \mu + 1$ *then* $G(z) = zL(z)$,
4. *if* $\delta > \mu + 1$ *then* $G(z)$ *is a multiple of* $zL(z)$.

Proof. In fact Remark 2.2 proves that the following statements are equivalent

- $G(z) \neq 0$,
- $G(z)$ is annihilated by all the $\alpha^{k_j}, 1 \leq j \leq \mu$ and is also satisfied by 0 in case $i > \mu$;
- $G(z)$ is a multiple of $L(z)$ (and also of $zL(z)$ in case $i > \mu$).

This implies that $\delta \geq \mu$, where equality holds only in case $\mu = i$.
The statement is then obvious. $\square$

Recalling that I is 0-dimensional (cf. Rem.1.6), Theorem 3.1 allows us to give a precise description of the Gröbner basis $\mathcal{G}$ of the ideal I discussed in Theorem 2.1. Using it and Lemma 4.1 we can state a result analogous of the one of Theorem 2.1.

Theorem 4.2 *The following properties hold for the Gröbner basis* $\mathcal{G}$ *of the syndrome ideal* I *w.r.t. the lexicographical order induced by*

$$X_1 < X_2 < \ldots < X_s < Z_\nu < Z_{\nu-1} < \ldots < Z_1 < Y_1 < Y_2 < \ldots < Y_\nu.$$

1. $\mathcal{G} = \mathcal{G}_X \bigcup \left(\bigcup_{i=1}^{\nu} \bigcup_{\partial=1}^{\Delta_i} \mathcal{G}_{i\partial} \right) \bigcup \mathcal{G}_Y$, *where*
   - $\forall g \in \mathcal{G}_X, g \in \mathcal{P}_X$;
   - $\forall i, \partial$, $\mathcal{G}_{i\partial} \subset \mathcal{P}_X[Z_\nu, \ldots, Z_{i+1}][Z_i] \setminus \mathcal{P}_X[Z_\nu, \ldots, Z_{i+1}]$,
   - $\mathcal{G}_{i\partial} := \{g_{i\partial j} \mid 1 \leq j \leq j_{i\partial}\}$ *is ordered in such a way that*
     $$J < j \iff \mathbf{T}(g_{i\partial J}) < \mathbf{T}(g_{i\partial j})$$
     then (2) is satisfied;
   - $\forall g \in \mathcal{G}_Y, g \in \mathcal{P}_{XZY} \setminus \mathcal{P}_{XZ}$.
2. *For each* i, *let* $g_i := g_{i\partial j}$ *be the first polynomial in* $\mathcal{G}_i$ *whose leading polynomial evaluated in* $(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0)$ *(with* $\nu - i$ *zeros) is non null, i.e.*
   - $Lp(g)(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) = 0 \;\forall\; g \in \mathcal{G}_{iD}, D < \partial$;
   - $Lp(g_{i\partial J})(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) = 0 \;\forall J < j$;
   - $Lp(g_{i\partial j})(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) \neq 0$.

Denote

$$\begin{aligned}\Gamma_i(X_1,\ldots,X_s) &:= Lp(g_i)(X_1,\ldots,X_s,0,\ldots,0),\\ G_i(X_1,\ldots,X_s,Z_i) &:= g_i(X_1,\ldots,X_s,0,\ldots,0,Z_i).\end{aligned}$$

Then it holds

(a) If μ is the value s.t.

- $\Gamma_i(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)=0, i>\mu,$
- $\Gamma_\mu(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)\neq 0,$

then:

- *there are exactly μ errors in the received word $r(x)$;*
- *the error locator polynomial is $L(z):=G_\mu(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,z)$.*

(b) $g_i = g_{i\partial j}$ is the first polynomial in $\mathcal{G}_i$ which doesn't vanish when evaluated in $(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)$. More precisely

- $g(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)=0\ \forall\ g\in\mathcal{G}_{iD}, D<\partial;$
- $g_{i\partial J}(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)=0\ \forall J<j;$
- $g_i(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)\neq 0;$
- $g_i(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)$ *divides* $g_{i\partial J}(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)$, $\forall J>j;$
- $g_i(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)$ *divides* $g(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_i)\ \forall\ g\in\mathcal{G}_{iD},\forall D>\partial.$

3. *Under the assumption that there are at most μ errors, then either*

- $\forall j, 1\le j\le j_{\mu\mu},\ Lp(g_{\mu\mu j})(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)=0$, *in which case*
  - $g(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,Z_\mu)=0,\forall g\in\mathcal{G}_{\mu\mu};$
  - *there are at most $\mu-1$ errors;*
- *or there is a minimal value J s.t.* $Lp(g_{\mu\mu J})(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)\neq 0$ *in which case* $g_{\mu\mu J}(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)\neq 0$ *and*
  - *either*
    - $Tp(g_{\mu\mu J})(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)\neq 0,$
    - *there are exactly μ errors, and*
    - $L(z)=g_{\mu\mu J}(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0,z);$
  - *or*
    - $Tp(g_{\mu\mu J})(\mathsf{s}_1,\ldots,\mathsf{s}_s,0,\ldots,0)=0,$
    - *there are at most $\mu-1$ errors.*

Proof. 1. and 2.(b) follow directly by Theorem 3.1.

The proof of 2.(a) is the same as the one of Theorem 2.1 (cf. [4], Th.3.1); there is no need to compute the gcd of $G_\mu(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, z)$ with $z^n - 1$ because there is no algebraic solution among the roots of syndrome ideal (thanks to Rem. 1.6 and to the introductions of the equation σ and, a fortiori, of $G_\mu(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, z)$.

3. follows by Lemma 4.1: since there are at most μ errors, Lemma 4.1 then guarantees that

$$G_\mu(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, Z_\mu) \neq 0 \Longrightarrow \deg_{Z_\mu}(G_\mu) \geq \mu;$$

therefore it is just sufficient to check whether there exists a polynomial

$$g \in \mathcal{G} \cap \mathcal{P}_X[Z_\nu, \dots, Z_{\mu+1}][Z_\mu]$$

s.t. $\deg_{Z_\mu}(g) = \mu$ and $g(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, Z_\mu) \neq 0$. If this is not the case we know that there are less than μ errors. In the other case then

$$g(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, Z_\mu) = G_\mu(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0, Z_\mu) =: G(Z_\mu)$$

and $G(z) = \begin{cases} L(z) & \iff Tp(G)(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0) \neq 0 \\ zL(z) & \iff Tp(G)(\mathsf{s}_1, \dots, \mathsf{s}_s, 0, \dots, 0) = 0. \end{cases}$ □

On the basis of this result, the algorithm of Fig. 1 can be modified as in Fig. 2 making correct the CHRT Decoding Algorithm.

5 A full example

Let us apply the algorithm to the same example discussed in [4] and [10]. We are working in $GF(2)[\mathbf{X}, \mathbf{Z}]$ for which the syndrome ideal is:

$$\begin{aligned} I = \{ & Z_1 + Z_2 + Z_3 + X_1, \\ & Z_1^3 + Z_2^3 + Z_3^3 + X_2, \\ & Z_1^5 + Z_2^5 + Z_3^5 + X_3, \\ & X_1^{16} - X_1, \\ & X_2^{16} - X_2, \\ & X_3^{16} - X_3, \\ & Z_1^{16} - Z_1, \\ & Z_2^{16} - Z_2, \\ & Z_3^{16} - Z_3 \} \end{aligned}$$

Remark that the $\mathbf{Y}$ indeterminates are not necessary here since the possible error magnitudes in $GF(2)$ are either 0 or 1.

The Gröbner basis of the syndrome ideal with respect to the lexicographic term-ordering induced by $X_1 < X_2 < X_3 < Z_3 < Z_2 < Z_1$ is $\mathcal{G}$, structured as shown in Corollary 4.2 and whose component $\left(\bigcup_{i=1}^{\nu} \bigcup_{\partial=1}^{\Delta_i} \mathcal{G}_{i\partial} \right)$ is

Figure 2: The revised CRHT decoding algorithm

Input $\mathcal{G}$ Gröbner basis.

$\mu := \nu$, $L := 1$,

Repeat

> $j := 0$
>
> **Repeat**
>
> > j := j+1
>
> **Until** $Lp(g_{\mu\mu j})(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) \neq 0$ **or** $j > j_{\mu\mu}$
>
> **If** $j > j_{\mu\mu}$ **then**
>
> > $\mu := \mu - 1$
>
> **else**
>
> > **If** $Tp(g_{\mu\mu j})(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) = 0$ **do**
> >
> > > $\mu := \mu - 1$
> >
> > **else**
> >
> > > $L := g_{\mu\mu j}(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0, z)$;
> > >
> > > **Output** μ, $L(z)$

Until $L \neq 1$ **or** $\mu = 0$

Output μ, $L(z)$

$$
\begin{aligned}
g_{3\ 3\ 1} &= Z_3^3(\mathbf{X_2X_3^3}+\mathbf{X_2})+Z_3^2X_1X_2X_3^3+Z_3^2X_1X_2+Z_3X_1^{11}X_2^3+\\
&\quad +Z_3X_1^8X_2^4X_3^3+Z_3X_1^7X_2X_3^2+Z_3X_1^6X_2^3X_3+Z_3X_1^5X_2^{10}+\\
&\quad +Z_3X_1^5X_2^5X_3^3+Z_3X_1^5X_3^3+Z_3X_1^4X_2^2X_3^2+Z_3X_1^3X_2^4X_3+\\
&\quad +Z_3X_1^2X_2^{11}X_3^3+Z_3X_1^2X_2^{11}+Z_3X_1^2X_2^6X_3^3+Z_3X_1^2X_2^6+\\
&\quad +Z_3X_1X_2^8X_3^2+Z_3X_1X_2^3X_3^2+Z_3X_2^{10}X_3+Z_3X_2^5X_3+Z_3X_3+\\
&\quad +X_1^{12}X_2^3+X_1^8X_2X_3^2+X_1^7X_2^8X_3+X_1^7X_2^3X_3+X_1^6X_2^{10}+\\
&\quad +X_1^6X_3^3+X_1^5X_2^{12}X_3^2+X_1^4X_2^9X_3+X_1^3X_2^{11}+X_1^3X_2^6X_3^3+\\
&\quad +X_1^3X_2^6+X_1^3X_2X_3^3+X_1^3X_2+X_1^2X_2^{13}X_3^2+X_1X_2^{15}X_3+\\
&\quad +X_1X_2^{10}X_3+X_1X_3+X_2^{12}X_3^3+X_2^7X_3^3+X_2^2,\\
g_{3\ 3\ 2} &= Z_3^3(\mathbf{X_2^5}+\mathbf{X_3^3})+Z_3^2X_1X_2^5+Z_3^2X_1X_3^3+Z_3X_1^{11}X_2^2+\\
&\quad +Z_3X_1^8X_2^{13}X_3^3+Z_3X_1^8X_2^8+Z_3X_1^8X_2^3+Z_3X_1^7X_2^5X_3^2+\\
&\quad +Z_3X_1^6X_2^7X_3+Z_3X_1^5X_2^{14}X_3^3+Z_3X_1^5X_2^9X_3^3+Z_3X_1^5X_2^9+\\
&\quad +Z_3X_1^4X_2X_3^2+Z_3X_1^3X_2^{13}X_3+Z_3X_1^2X_2^{10}X_3^3+\\
&\quad +Z_3X_1^2X_2^5X_3^3+Z_3X_1^2X_2^5+Z_3X_1^2+Z_3X_1X_2^{12}X_3^2+\\
&\quad +Z_3X_1X_2^7X_3^2+Z_3X_2^9X_3+X_1^{12}X_2^2+X_1^8X_2^5X_3^2+\\
&\quad +X_1^7X_2^{12}X_3+X_1^7X_2^2X_3+X_1^6X_2^9X_3^3+X_1^6X_2^4+X_1^5X_2X_3^2+\\
&\quad +X_1^4X_2^{13}X_3+X_1^3X_2^{15}+X_1^3X_2^{10}X_3^3+X_1^3X_2^{10}+\\
&\quad +X_1^3X_3^3+X_1^3+X_1^2X_2^2X_3^2+X_1X_2^9X_3+X_2^{11},\\
g_{3\ 3\ 3} &= Z_3^3(\mathbf{X_1}+\mathbf{X_2^2X_3^2})+Z_3^2X_1^2+Z_3^2X_1X_2^2X_3^2+Z_3X_1^{12}X_2^2+\\
&\quad +Z_3X_1^8X_2^5X_3^2+Z_3X_1^8X_3^2+Z_3X_1^7X_2^{12}X_3+Z_3X_1^7X_2^7X_3+\\
&\quad +Z_3X_1^7X_2^2X_3+Z_3X_1^6X_2^{14}X_3^3+Z_3X_1^6X_2^9X_3^3+Z_3X_1^6X_2^9+\\
&\quad +Z_3X_1^5X_2^{11}X_3^2+Z_3X_1^5X_2X_3^2+Z_3X_1^4X_2^{13}X_3+\\
&\quad +Z_3X_1^4X_2^8X_3+Z_3X_1^4X_2^3X_3+Z_3X_1^3X_2^{10}X_3^3+Z_3X_1^3X_2^{10}+\\
&\quad +Z_3X_1^3X_2^5X_3^3+Z_3X_1^3X_2^5+Z_3X_1^2X_2^{12}X_3^2+Z_3X_1X_2^4X_3+\\
&\quad +Z_3X_2^{11}X_3^3+Z_3X_2^6X_3^3+X_1^{10}X_2^3+X_1^8X_2^{12}X_3+\\
&\quad +X_1^8X_2^7X_3+X_1^7X_2^4X_3^3+X_1^6X_2^{11}X_3^2+X_1^6X_2^6X_3^2+X_1^5X_2^8X_3+\\
&\quad +X_1^5X_2^3X_3+X_1^4X_2^{15}+X_1^4X_2^{10}+X_1^4X_2^5X_3^3+\\
&\quad +X_1^3X_2^7X_3^2+X_1^2X_2^4X_3+X_1X_2^{11}+X_1X_2^6X_3^3+X_1X_2^6+\\
&\quad +X_2^{13}X_3^2+X_2^8X_3^2,
\end{aligned}
$$

$$
\begin{aligned}
g_{3\ 16\ 1} &= Z_3^{16}+Z_3,\\
g_{2\ 2\ 1} &= Z_2^2(\mathbf{X_2X_3^3}+\mathbf{X_2})+Z_2Z_3X_2X_3^3+Z_2\\
&\quad +Z_3X_2+Z_2X_1X_2X_3^3+Z_2X_1X_2+
\end{aligned}
$$

$$
\begin{aligned}
& +Z_3^2X_2X_3^3+Z_3^2X_2+Z_3X_1X_2X_3^3+Z_3X_1X_2+X_1^{11}X_2^3+\\
& +X_1^8X_2^4X_3^3+X_1^7X_2X_3^2+X_1^6X_2^3X_3+X_1^5X_2^{10}+\\
& +X_1^5X_2^5X_3^3+X_1^5X_3^3+X_1^4X_2^2X_3^2+X_1^3X_2^4X_3+\\
& +X_1^2X_2^{11}X_3^3+X_1^2X_2^{11}+X_1^2X_2^6X_3^3+X_1^2X_2^6+X_1X_2^8X_3^2+\\
& +X_1X_2^3X_3^2+X_2^{10}X_3+X_2^5X_3+X_3,\\
g_{2\ 2\ 2} &= Z_2^2(\mathbf{X_2^5}+\mathbf{X_3^3})+Z_2Z_3X_2^5+Z_2Z_3X_3^3+Z_2X_1X_2^5+Z_2X_1X_3^3+\\
& +Z_3^2X_2^5+Z_3^2X_3^3+Z_3X_1X_2^5+Z_3X_1X_3^3+X_1^{11}X_2^2+\\
& +X_1^8X_2^{13}X_3^3+X_1^8X_2^8+X_1^8X_2^3+X_1^7X_2^5X_3^2+X_1^6X_2^7X_3+\\
& +X_1^5X_2^{14}X_3^3+X_1^5X_2^9X_3^3+X_1^5X_2^9+X_1^4X_2X_3^2+\\
& +X_1^3X_2^{13}X_3+X_1^2X_2^{10}X_3^3+X_1^2X_2^5X_3^3+X_1^2X_2^5+\\
& +X_1^2+X_1X_2^{12}X_3^2+X_1X_2^7X_3^2+X_2^9X_3,\\
g_{2\ 2\ 3} &= Z_2^2(\mathbf{X_1}+\mathbf{X_2^2X_3^2})+Z_2Z_3X_1+Z_2Z_3X_2^2X_3^2+Z_2X_1^2+\\
& +Z_2X_1X_2^2X_3^2+Z_3^2X_1+Z_3^2X_2^2X_3^2+Z_3X_1^2+Z_3X_1X_2^2X_3^2+\\
& +X_1^{12}X_2^2+X_1^8X_2^5X_3^2+X_1^8X_3^2+X_1^7X_2^{12}X_3+X_1^7X_2^7X_3+\\
& +X_1^7X_2^2X_3+X_1^6X_2^{14}X_3^3+X_1^6X_2^9X_3^3+X_1^6X_2^9+\\
& +X_1^5X_2^{11}X_3^2+X_1^5X_2X_3^2+X_1^4X_2^{13}X_3+X_1^4X_2^8X_3+\\
& +X_1^4X_2^3X_3+X_1^3X_2^{10}X_3^3+X_1^3X_2^{10}+X_1^3X_2^5X_3^3+\\
& +X_1^3X_2^5+X_1^2X_212X_3^2+X_1X_2^4X_3+X_2^{11}X_3^3+X_2^6X_3^3,\\
g_{2\ 2\ 4} &= Z_2^2(\mathbf{Z_3}+\mathbf{X_2^2X_3^2})+Z_2Z_3^2+Z_2Z_3X_1+Z_2Z_3X_2^2X_3^2+\\
& +Z_2X_1X_2^2X_3^2+Z_3^2X_2^2X_3^2+Z_3X_1X_2^2X_3^2+X_1^{12}X_2^2+\\
& +X_1^8X_2^5X_3^2+X_1^8X_3^2+X_1^7X_2^{12}X_3+X_1^7X_2^7X_3+\\
& +X_1^7X_2^2X_3+X_1^6X_2^{14}X_3^3+X_1^6X_2^9X_3^3+X_1^6X_2^9+X_1^5X_2^{11}X_3^2+\\
& +X_1^5X_2X_3^2+X_1^4X_2^{13}X_3+X_1^4X_2^8X_3+X_1^4X_2^3X_3+\\
& +X_1^3X_210X_3^3+X_1^3X_2^{10}+X_1^3X_2^5X_3^3+X_1^3X_2^5+X_1^3+\\
& +X_1^2X_2^{12}X_3^2+X_1X_2^4X_3+X_211X_3^3+X_2^6X_3^3+X_2,\\
g_{2\ 16\ 1} &= Z_2^{16}+Z_2,\\
g_{1\ 1\ 1} &= Z_1+Z_2+Z_3+X_1.
\end{aligned}
$$

Note that

$$
\begin{aligned}
Lp(g_{3\ 3\ 1}) &= Lp(g_{2\ 2\ 1}),\\
Lp(g_{3\ 3\ 2}) &= Lp(g_{2\ 2\ 2}),\\
Lp(g_{3\ 3\ 3}) &= Lp(g_{2\ 2\ 3}).
\end{aligned}
$$

and remark that

$$\begin{aligned}
g_{3\ 3\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z) &= z g_{2\ 2\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z) + Tp(g_{3\ 3\ 1}), \\
g_{3\ 3\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z) &= z g_{2\ 2\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z) + Tp(g_{3\ 3\ 2}), \\
g_{3\ 3\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z) &= z g_{2\ 2\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z) + Tp(g_{3\ 3\ 3}).
\end{aligned}$$

Such behavior is quite common, and it is due to the structure described by the Gianni-Kalkbrenner Theorem; see Remark 2.2 and Lemma 4.1.

Hence, we have that

1.1 if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 \neq 0, Tp(g_{3\ 3\ 1}) \neq 0$$

then

$$L = g_{3\ 3\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z),$$

1.2 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 \neq 0, Tp(g_{3\ 3\ 1}) = 0, Tp(g_{2\ 2\ 1}) \neq 0$$

then

$$L = g_{2\ 2\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z),$$

1.3 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 \neq 0, Tp(g_{3\ 3\ 1}) = 0, Tp(g_{2\ 2\ 1}) = 0$$

then

$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, 0, z),$$

2.1 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 \neq 0, Tp(g_{3\ 3\ 2}) \neq 0$$

then

$$L = g_{3\ 3\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z),$$

2.2 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 \neq 0, Tp(g_{3\ 3\ 2}) = 0, Tp(g_{2\ 2\ 1}) \neq 0$$

then

$$L = g_{2\ 2\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z),$$

2.3 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 \neq 0, Tp(g_{3\ 3\ 2}) = 0, Tp(g_{2\ 2\ 1}) = 0$$

then

$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, 0, z),$$

3.1 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{3\ 3\ 3}) \neq 0$$
then
$$L = g_{3\ 3\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, z),$$

3.2 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{3\ 3\ 3}) = 0, Tp(g_{2\ 2\ 3}) \neq 0$$
then
$$L = g_{2\ 2\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z),$$

3.3 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{3\ 3\ 3}) = 0, Tp(g_{2\ 2\ 3}) = 0$$
then
$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, 0, z),$$

3.4 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0$$
then
$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, 0, z),$$

4.1 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0, \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{2\ 2\ 4}) \neq 0$$
then
$$L = g_{2\ 2\ 4}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z),$$

4.2 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = \mathsf{s}_2^5 + \mathsf{s}_3^3 = \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0,\ \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{2\ 2\ 4}) = 0, Tp(g_{1\ 1\ 1}) \neq 0$$
then
$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, 0, z),$$

4.3 else if
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = \mathsf{s}_2^5 + \mathsf{s}_3^3 = \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0, \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0, Tp(g_{2\ 2\ 4}) = Tp(g_{1\ 1\ 1}) = 0$$
then
$$L = 1,$$

4.4 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0, \mathsf{s}_2^2\mathsf{s}_3^2 = 0, Tp(g_{1\ 1\ 1}) \neq 0$$

then

$$L = g_{1\ 1\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, z),$$

4.5 else if

$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0, \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0, \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0, \mathsf{s}_2^2\mathsf{s}_3^2 = 0, Tp(g_{1\ 1\ 1}) = 0$$

then

$$L = 1.$$

6 Complexity and First Conclusions

The complexity of both algorithms Figs. 1 and 2 depends

- on the cost of the evaluation of the generic polynomials

  $$Lp(f), Tp(f) \in K[X_1, \ldots, X_s] :$$

  since for each variable X_j it holds $\deg_{X_j}(f) < D$, the cost of this evaluation is $\mathcal{O}(s^n)$;

  and

- on the number of needed evaluations: for Fig. 1 they are $\mathcal{O}(\mathsf{d})$, while for Fig. 2 they are $\mathcal{O}(s^n \mathsf{d}^n)$, which is the numbers of monomials in $\mathcal{P}_{XZ}$.

On the other side, the precomputing of the Gröbner basis, being a precomputation does not effect the decoding procedure. Of course the effectiveness of the proposed approach depends on the *practical* effectiveness of the method used to compute the Gröbner bases; from this point of view the suggestion of [10] of using some variants of the FGLM algorithm (see [5]) is very worthwhile, but not for the argument expounded there. In fact, from the representation of quotients $\mathcal{P}/I$ where I is 0-dimensional which is discussed in [11] (see also [1]) it follows easily that the complexity of computing the Gröbner basis $\mathcal{G}$ is the same using either the FGLM algorithm or the Buchberger Algorithm: that paper proposed to use the finite vector-space structure of $\mathcal{P}/I$ in order to reduce the Gröbner basis computation to a linear algebra computation in a style mimicking Zharkov ([13]) and Border Bases computation. We are personally convinced that this is the most efficient way to compute Gröbner bases for syndrome ideals.

7 Further improvements

The decoding tree at the end of section 5 gives the decoding algorithm, but it may appear cumbersome. Recently, in cooperation with M. Sala [3], we are investigating the effect of some possible improvements to the rough algorithm sketched above. Here is a very brief sketch of some of the material contained in that work, which already gives a nicer (and faster) decoding tree.

We begin by remarking that $\mathcal{S} := \mathcal{G} \cap \mathcal{P}_X$ is the Gröbner basis of the ideal $I \cap \mathcal{P}_X$ of all the polynomial relations satisfied by the syndromes s_j, and that the algorithm gives us in each **If** branch two sets $\mathbf{C}_0$, $\mathbf{C}_1$ of polynomials for which it holds

$$p(\mathsf{s}_1, \ldots, \mathsf{s}_s, 0, \ldots, 0) \begin{cases} = 0 & \iff p \in \mathbf{C}_0 \\ \neq 0 & \iff p \in \mathbf{C}_1 \end{cases}$$

a new polynomial P to be tested, and a possible locator polynomial L; in each branch we can denote by S, $I \cap \mathcal{P}_X \subset \mathsf{S} \subset \mathcal{P}_X$, the ideal generated by $\mathcal{S} \cup \mathbf{C}_0$.

Among the improvements we can quote the following:

- each new polynomial P whose vanishing must be tested, can be factorized (for instance
$$\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = \mathsf{s}_2(\mathsf{s}_3^3 + 1)$$
producing more branches, each with possibly less depth;
- both the polynomial P and L can be Gröbner reduced modulo S, thus giving sparser polynomials to be tested;
- moreover one can test, by Gröbner redaction, whether $\exists p \in \mathbf{C}_1 : p \in \mathsf{S}$, in which case we get an obvious contradiction, thus pruning the potential branches;
- the refinement of Gianni-Kalhbrenner Theorem conjectured in [12] implies that for each locator polynomial $L = g_{\mu\mu j}$ there should be an easy-to-compute polynomial ℓ s.t. $g_{\mu\mu j} - Lp(g_{\mu\mu j})\ell \in \mathsf{S}$. It is therefore worthwhile to computationally verify the existence of s.t. ℓ and eventually return ℓ (resp. $Lt(\ell)$) instead of $g_{\mu\mu j}$ (resp.$Lt(g_{\mu\mu j})$) if shorter.

These improvements are already sufficient to trim the result of the algorithm in our example to the following decoding tree:

$$\begin{aligned} \mathsf{s}_2^5 = 0, \mathsf{s}_3 \neq 0 &\implies L = \mathsf{s}_3^3 Z^2 + \mathsf{s}_1 Z + \mathsf{s}_1^2, \\ \mathsf{s}_2^5 = 0, \mathsf{s}_3 = 0 &\implies L = 1, \\ \mathsf{s}_2^5 = 1, \mathsf{s}_3^3 = 1, \mathsf{s}_1 \neq \mathsf{s}_2^2\mathsf{s}_3^2 &\implies L = h_1(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) \end{aligned}$$

$$
\begin{array}{rcl}
\mathsf{s}_2^5 = 1, \mathsf{s}_3^3 = 1, \mathsf{s}_1 = \mathsf{s}_2^2\mathsf{s}_3^2, & \Longrightarrow & L = z + \mathsf{s}_1. \\
\mathsf{s}_2^5 \neq 0, \mathsf{s}_3^3 \neq 1, \mathsf{s}_1 = 0 & \Longrightarrow & L = h_2(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z), \\
\mathsf{s}_2^5 \neq 0, \mathsf{s}_3^3 \neq 1, \mathsf{s}_1 \neq 0, & \Longrightarrow & L = Z^2 + \mathsf{s}_1 Z + \mathsf{s}_1^2\mathsf{s}_2^5, \\
\mathsf{s}_2^5 \notin \{0,1\}, \mathsf{s}_3^3 = 1, q_1(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) \neq 0 & \Longrightarrow & L = h_3(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) \\
\mathsf{s}_2^5 \notin \{0,1\}, \mathsf{s}_3^3 = 1, q_1(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) = 0 & \Longrightarrow & L = Z^2 + \mathsf{s}_1 Z + \mathsf{s}_1^2 + \mathsf{s}_1\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2^4\mathsf{s}_3
\end{array}
$$

where

$$
\begin{array}{rcl}
h_1(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) & = & Z^3 + \mathsf{s}_1 Z^2 + (\mathsf{s}_1^7\mathsf{s}_3^2 + \mathsf{s}_1^5\mathsf{s}_2^4 + \mathsf{s}_1^2 + \mathsf{s}_1\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2^4\mathsf{s}_3^3)Z + \\
& + & \mathsf{s}_1^7\mathsf{s}_2^2\mathsf{s}_3 + \mathsf{s}_1^6\mathsf{s}_2^4 + \mathsf{s}_1^5\mathsf{s}_2\mathsf{s}_3^2 + \mathsf{s}_1^4\mathsf{s}_2^3\mathsf{s}_3 + \mathsf{s}_1^3 + \mathsf{s}_1^2\mathsf{s}_2^2\mathsf{s}_3^2, \\
h_2(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) & = & Z^3 + \mathsf{s}_1 Z^2 + \left(\mathsf{s}_1^{11}\mathsf{s}_2^2 + \mathsf{s}_1^5\mathsf{s}_2^9 + \mathsf{s}_1^2\mathsf{s}_2^{10} + \mathsf{s}_1^2\mathsf{s}_2^5\right) Z + \\
& + & \mathsf{s}_1^{12}\mathsf{s}_2^2 + \mathsf{s}_1^6\mathsf{s}_2^9 + \mathsf{s}_1^3\mathsf{s}_2^{10} + \mathsf{s}_1^3\mathsf{s}_2^5 + \mathsf{s}_1^3 + \mathsf{s}_2, \\
h_3(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) & = & Z^3 + \mathsf{s}_1 Z^2 + \\
& + & \left(\mathsf{s}_1^8\mathsf{s}_2^8 + \mathsf{s}_1^7\mathsf{s}_3^2 + \mathsf{s}_1^6\mathsf{s}_2^2\mathsf{s}_3 + \mathsf{s}_1^5\mathsf{s}_2^4 + \mathsf{s}_1^3\mathsf{s}_2^8\mathsf{s}_3\right) Z + \\
& + & \left(\mathsf{s}_1^3\mathsf{s}_2^3\mathsf{s}_3 + \mathsf{s}_1^2\mathsf{s}_2^{10} + \mathsf{s}_1\mathsf{s}_2^7\mathsf{s}_3^2 + \mathsf{s}_1\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2^9\mathsf{s}_3 + \mathsf{s}_2^4\mathsf{s}_3\right) Z + \\
& + & \mathsf{s}_1^8\mathsf{s}_3^2 + \mathsf{s}_1^7\mathsf{s}_2^7\mathsf{s}_3 + \mathsf{s}_1^6\mathsf{s}_2^9 + \mathsf{s}_1^6\mathsf{s}_2^4 + \mathsf{s}_1^5\mathsf{s}_2^6\mathsf{s}_3^2 + \mathsf{s}_1^5\mathsf{s}_2\mathsf{s}_3^2 + \\
& + & \mathsf{s}_1^4\mathsf{s}_2^8\mathsf{s}_3 + \mathsf{s}_1^3\mathsf{s}_2^5 + \mathsf{s}_1^3 + \mathsf{s}_1^2\mathsf{s}_2^7\mathsf{s}_3^2 + \mathsf{s}_1^2\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2
\end{array}
$$

and

$$
\begin{array}{rcl}
q_1(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) & = & \mathsf{s}_1^8\mathsf{s}_3^2 + \mathsf{s}_1^7\mathsf{s}_2^7\mathsf{s}_3 + \mathsf{s}_1^6\mathsf{s}_2^9 + \mathsf{s}_1^6\mathsf{s}_2^4 + \mathsf{s}_1^5\mathsf{s}_2^6\mathsf{s}_3^2 + \mathsf{s}_1^5\mathsf{s}_2\mathsf{s}_3^2 + \\
& + & \mathsf{s}_1^4\mathsf{s}_2^8\mathsf{s}_3 + \mathsf{s}_1^3\mathsf{s}_2^5 + \mathsf{s}_1^3 + \mathsf{s}_1^2\mathsf{s}_2^7\mathsf{s}_3^2 + \mathsf{s}_1^2\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2
\end{array}
$$

Recently we have developed an alternative and quite promising strategy to the one we have exposed throughout the present paper, i.e. the computation and processing of the Gröbner basis $\mathcal{G}$ of the syndrome ideal I encoding the case in which there are *at most* ν *errors*.

Using this new strategy we compute and process, $\forall\mu, 1 \leq \mu \leq \nu$, the Gröbner basis $\mathcal{G}_\mu$ of the μ^{th} syndrome ideal I_μ encoding only the case in which there are *exactly* μ *errors*.

Remark that, with the notation previously introduced such Gröbner basis encoding the ideal I_μ is the one generated by

$$\{\phi_{j\mu}, \sigma_j, g_i, \lambda_i : 1 \leq j \leq s, 1 \leq i \leq \mu\}.$$

where

$$
\begin{array}{rcll}
h_i & := & Z_i^n - 1, & 1 \leq i \leq \mu, \\
\phi_j & := & \sum_{l=1}^{\mu} Y_l Z_l^{i_j} - X_j, & 1 \leq j \leq s
\end{array}
$$

We recently performed this investigation on the same example and the results are quite promising. The decoding tree can be summarized in the table :

$$
\begin{array}{llllrcl}
\mathsf{s}_2 = 0 & \mathsf{s}_3 = 0 & & \Longrightarrow & L & = & 1 \\
\mathsf{s}_2 = 0 & \mathsf{s}_3 \neq 0 & & \Longrightarrow & L & = & Z^2 + Z_2\mathsf{s}_1 + \mathsf{s}_1^2 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 = 0 & \mathsf{s}_1 = 0 & \Longrightarrow & L & = & Z^3 + \mathsf{s}_2 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 = 0 & \mathsf{s}_1 \neq 0 & \Longrightarrow & L & = & Z^3 + Z^2\mathsf{s}_1 + Z\left(\mathsf{s}_1^{11}\mathsf{s}_2^2 + \mathsf{s}_1^5\mathsf{s}_2^4\right) + \mathsf{s}_1^9\mathsf{s}_2^3 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 \neq 0 & \sigma = 0 & \Longrightarrow & L & = & Z + \mathsf{s}_1 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 \neq 0 & \sigma \neq 0 & \Longrightarrow & L & = & Z^3 + Z^2\mathsf{s}_1 + \\
 & & & & & + & Z\left(\mathsf{s}_1^2 + \mathsf{s}_2^4\mathsf{s}_3^4\right)\left(\mathsf{s}_1^5\mathsf{s}_3^2 + \sigma^{-1}\right) + \\
 & & & & & + & \mathsf{s}_1^2\mathsf{s}_2^2\mathsf{s}_3\left(\mathsf{s}_1^5 + \mathsf{s}_2^{10}\mathsf{s}_3^{10}\right)\sigma^{-1} \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3 = 0 & & \Longrightarrow & L & = & Z^2 + Z\mathsf{s}_1 + \mathsf{s}_1^2\mathsf{s}_2^5 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0 & \mathsf{s}_1 = 0 & \Longrightarrow & L & = & Z^3 + Z\mathsf{s}_2^{-1}\mathsf{s}_3 + \mathsf{s}_2 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0 & \rho = 0 & \Longrightarrow & L & = & Z^2 + Z_2\mathsf{s}_1 + \mathsf{s}_2^9\mathsf{s}_3 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0 & \mathsf{s}_1\rho \neq 0 & \Longrightarrow & L & = & Z^3 + Z^2\mathsf{s}_1 + \\
 & & & & & + & Z\left(\mathsf{s}_1^5\mathsf{s}_2^8\mathsf{s}_3 + \mathsf{s}_1^3\mathsf{s}_2^2\mathsf{s}_3^2\right)\rho^{-1} + \\
 & & & & & + & Z\left(\mathsf{s}_1^2\mathsf{s}_2^9\mathsf{s}_3 + \mathsf{s}_2^{13}\mathsf{s}_3^2\right)\rho^{-1} + \\
 & & & & & + & \mathsf{s}_1^4\mathsf{s}_2^3\mathsf{s}_3 + \mathsf{s}_1^3\mathsf{s}_2^5 + \mathsf{s}_1\mathsf{s}_2^{-1}\mathsf{s}_3 + \mathsf{s}_2^{-4}
\end{array}
$$

where

$$
\begin{array}{rcl}
\rho & := & \mathsf{s}_1^2 + \mathsf{s}_1\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2^{-1}\mathsf{s}_3 \\
\sigma & := & \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2.
\end{array}
$$

References

[1] Alonso M.E., M.G. Marinari and T. Mora. *The big mother of all dualities: Möller algorithm*, Communications in Algebra, to appear (2002).

[2] Caboara M. and Mora F., *Some notes on solving polynomial equation systems over a finite field*, Draft (2002).

[3] Caboara, M., T. Mora and M. Sala, *Fast decoding of cyclic codes via the syndrome variety*, Preprint (2002).

[4] Chen, X., I.S. Reed, T. Helleseth and T.K. Truong, , *Algebraic Decoding of Cyclic Codes: a Polynomial Ideal Point of View*, Cont. Math. **168** (1994) 15–22.

[5] Faugère J.C., P. Gianni, D. Lazard and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Journal of Symbolic Computation, **16**(4) (1993) 329–344.

[6] Forney G.D. Jr., *On Decoding BCH Codes*, IEEE Trans. on Information Theory, IT-10,(1965), 549–557.

[7] Gianni P., *Properties of Gröbner Bases under Specialization*, Lect.N. Comp. Sci. **378**, Springer, 1989, 293–297.

[8] Kalkbrenner M., *Solving Systems of Algebraic Equations Using Gröbner Bases*, Lect.N. Comp. Sci. **378**, Springer, 1989, 282–292.

[9] Lazard D., *Ideal bases and Primary Decomposition: Case of two Variables*. J. Symb. Comp. **1** (1985) 261–270.

[10] Loustaunau P. and York, E.V., *On the Decoding of Cyclic Codes Using Gröbner Bases*. J. AAECC, **8** (1997).

[11] Mora T. and C. Traverso. Preprint (1992).

[12] Mora, F., *Some remarks around a remark by Macaulay*, invited lecture in Rhine Workshop on Computer Algebra, Karlsruhe, March 2002.

[13] Zharkov A.Yu. and Yu.A. Blinkov, *Involutive approach to solving systems of algebraic equations*, Proc. IMACS '93, 11–16.