Decoding cyclic codes: the Cooper philosophy

Teo Mora[*] Emmanuela Orsini[†]

October 19, 2007

Abstract

In 1990 Cooper [10, 11] suggested to use Gröbner basis computations in order to deduce error locator polynomials of cyclic codes.

The aim of this tutorial is to show, with illuminating examples, how Cooper's approach has been refined [6, 7, 8, 9, 14] up to give both an *online decoder* [2, 3] and *general error locator polynomials* [15, 16, 17].

1 Introduction

In 1990 Cooper [10, 11] suggested to use Gröbner basis computations in order to correct 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 interpretating the error locators of C as the roots of the syndrome equation system:

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

and, consequently, let $\mathbb{F}_{2^m}$ be some extension field of $\mathbb{F}_2$, the plain error locator polynomial as the monic generator $g(z_1)$ of the principal ideal

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

[*] T. Mora, DISI, Università di Genova, Via Dodecaneso 35, I-16100 Genova, Italy. E-mail: `theomora@disi.unige.it`.

[†] E. Orsini, Department of Mathematics, University of Milan, Milan, Italy. E-mail: `orsini@posso.dm.unipi.it`.

which can be directly computed via the elimination property of lexicographical Gröbner bases.

In a series of papers [7, 8, 9] Chen et al. improved and generalized Cooper's approach to decoding. In particular, for a q-ary $[n, k, d]$ cyclic codes, with correction capability t, they made the following alternative proposals:

1. denoting, for an error with weight μ, $z_1, \ldots, z_\mu$ the error locators, $y_1, \ldots, y_\mu$ the error values, $s_1, \ldots, s_{n-k} \in \mathbb{F}_{q^m}$ the associated syndromes, they interpreted ([7]) the coefficients of the plain error locator polynomial as the elementary symmetric functions
$$\sigma_j(z_1, \ldots, z_\mu) = (-1)^j \sum_{1 \le l_1 \le \cdots \le l_\mu \le \mu} z_{l_1} \cdots z_{l_\mu},\ 1 \le j \le \mu,$$
and the syndromes as the *power sum 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;

2. they considered ([8]) the *syndrome variety*
$$\left\{ (s_1, \ldots, s_{n-k}, y_1, \ldots, y_t, z_1, \ldots, z_t) \in (\mathbb{F}_{q^m})^{n+2t} : s_i = \sum_{j=1}^{\mu} y_j e_j^i,\ 1 \le i \le n-k \right\}$$
and proposed to deduce via a Gröbner basis pre-computation in
$$\mathbb{F}_q[x_1, \ldots, x_{n-k}, y_1, \ldots, y_t, z_1, \ldots, z_t]$$
a series of polynomials $g_\mu(x_1, \ldots, x_{n-k}, Z), \mu \le t$ such that, for any error with weight μ and associated syndromes $s_1, \ldots, s_{n-k} \in \mathbb{F}_{q^m}$, $g_\mu(s_1, \ldots, s_{n-k}, Z)$ in $\mathbb{F}_{q^m}[Z]$ is the plain error locator polynomial.

Their suggestions were improved and refined in (respectively) [2] and [6, 14]; remark that

1. requires to perform for each received vector up to t Gröbner basis computations; the μ^{th} computation deducing the unknown $\sigma_1, \ldots, \sigma_\mu$ in terms of the known syndromes $s_1, \ldots, s_n \in GF(q^m)$;

2. requires a pre-computation of a Gröbner basis into a polynomial ring in $2t + n - k$ variables.

Both computations are therefore not-necessarily feasible, the first since it requires an *on line* computation, the second since the syndrome variety has too many roots so that the Gröbner basis is less feasable to compute.

The investigation on the structure of the syndrome variety and on its Gröbner basis shows that most of its roots are spurious [8] and that the pre-computed polynomials $g_\mu(x_1, \ldots, x_n, Z)$ have the telescopical relations [5, 6]

$$g_\mu = Z g_{\mu-1} + c(x_1, \ldots, x_n).$$

To improve ([15]) the pre-computation it was sufficient to add equations removing the spurious roots. This new idea permitted to prove the existence of a computable *general error locator polynomial*, that is, a polynomial that satisfies the following property:

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

In this tutorial we assume that the reader is familiar with the notation for linear and cyclic codes adopted in [4]. In particular, we will use without comments concepts like: generator polynomial, defining set, correctable syndrome, error polynomial, classical error locator polynomial and plain error locator polynomial.
This tutorial has the following structure. In the second section we present the Cooper's idea of using Gröbner bases to decode binary BCH codes. In the third and fourth sections we describe Chen et *al.* ideas and we introduce the syndrome variety. The fifth section applies the Gianni–Kalkbrener Gröbner shape theorem to describe the structure of the syndrome variety. Section six introduces the general error locator polynomial for cyclic codes. Section seven is devoted to the *on line decoder* due to Augot et *al.* based on Newton's identities and Waring formulas.

2 Decoding binary BCH codes

We now describe the decoding algorithm proposed by Cooper in [10] and [11] to correct a primitive binary BCH codes of length $n = 2^m - 1$.

Let $\alpha \in \mathbb{F}_{2^m}$ be a primitive n-th root of unity and C a primitive BCH code over $\mathbb{F}_2$, with defining set $S = \{2i+1, 0 \leq i < t\}$. From the BCH bound we know that C can correct at least t errors.

We analyze the decoding process. Once the decoder receives a vector $v \in (\mathbb{F}_2)^n$, it computes the associated syndrome $\mathbf{s} \in (\mathbb{F}_{2^m})^{2t}$ and then uses it to find the unknown error locations α^j. We introduce the variables $Z =$

$(z_1, \dots, z_t)$, where z_j stands for the error locator α^j, $j = 1, \dots, t$. Thus we obtain the following system of t polynomials in $\mathbb{F}_{2^m}[Z]$:

$$\mathcal{F}_C : \left\{ f_i : \sum_{j=1}^{t} z_j^{2i-1} - s_{2i-1},\ i = 1, \dots, t \right\}.$$

The error locators form a solution $(\xi_1, \dots, \xi_t) \in (\mathbb{F}_{2^m})^t$ of $\mathcal{F}_C$. In this way an error correction procedure is a method of solving the nonlinear polynomial system $\mathcal{F}_C$ for $z_1, \dots, z_t$. Sometimes finding this solution could be difficult and ineffective. Cooper's idea is to transform the system $\mathcal{F}_C$ to another simpler system of equations having the same roots. Let I be the ideal generated by $\mathcal{F}_C$ in $\mathbb{F}_{2^m}[Z]$ and $\mathcal{V}(I)$ the set of its roots. Let G be the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $z_1 < \cdots < z_t$; we denote by $g \in \mathbb{F}_{2^m}[z_1]$ the unique polynomial such that $G \cap \mathbb{F}_{2^m}[z_1] = \{g\}$. To find the error locations, it is useful to define E to be the set of error locators:

$$\mathsf{E} = \{\xi_1, \dots, \xi_\mu\} \tag{1}$$

and Z the set of all components of the zeros of $\mathcal{F}_C$:

$$\mathsf{Z} = \{\xi \mid (\xi, a_2, \dots, a_t) \in \mathcal{V}(I)\}. \tag{2}$$

Theorem 2.1 ([11]). *Let G, I and g be as above. The following hold:*

a) $\mathsf{E} = \mathsf{Z} = \{\xi \mid g(\xi) = 0\}$;

b) $|\mathsf{E}| = \mu = \deg(g) \le t$;

c) $L_e(z) = g(z) = \prod_{\xi \in \mathsf{Z}} (z - \xi)$, *i.e. g is the polynomial whose roots are the error locators;*

d) $\sigma(z) = z^\mu g(z^{-1})$.

Remark 2.2. *There is in Cooper a designed ambiguity; the arithmetic is performed on the s_i in $\mathbb{F}_2[\mathsf{s}_i, i \in S]$ but are interpreted as performed on $s_i = \mathsf{s}_i(\alpha)$ in $\mathbb{F}_{2^m}$. All over this section we have deliberately maintained this ambiguity which will be solved in the next section; we have done so based on the interpretation of error locator polynomials suggested in [5]: an error locator polynomial is a cascade of devices, each evaluating a rational function $a_l(\mathsf{s}_i) \in \mathbb{F}_2(\mathsf{s}_i)$ and connected by gates activated by the value of polynomials $\beta(\mathsf{s}_i) \in \mathbb{F}_2[\mathsf{s}_i]$; at arrival of the word, the devices are properly connected, by evaluation of $\beta(s_i) \in \mathbb{F}$ producing an expression $\sum_{l=1}^{\mu} a_l(\mathsf{s}_i) z \in \mathbb{F}_2(\mathsf{s}_i)[z]$, whose evaluation returns the error locator polynomial $\sum_{l=1}^{\mu} a_l(s_i) z \in \mathbb{F}_2(\mathsf{s}_i)[z]$.* □

Example 2.3 ([11])**.** *Let C be a BCH code over $\mathbb{F}_2$ and defining set $S = \{1,3\}$. We want to find the classical error locator polynomial $\sigma(z)$. As $t = 2$, we set $\mathcal{P} := \mathbb{F}_2[\mathsf{s}_1,\mathsf{s}_3][z_1,z_2]$. Then*

$$\mathsf{I} := \mathbb{I}(z_1 + z_2 + \mathsf{s}_1, z_1^3 + z_2^3 + \mathsf{s}_3) \subset \mathcal{P}$$

and the reduced Gröbner basis w.r.t. the lex ordering is

$$G = \{z_1^2\mathsf{s}_1 + z_1\mathsf{s}_1^2 + \mathsf{s}_1^3 + \mathsf{s}_3, z_2 + z_1 + \mathsf{s}_1\}.$$

*So $g(z) = z^2\mathsf{s}_1 + z\mathsf{s}_1^2 + \mathsf{s}_1^3 + \mathsf{s}_3$, id est (*cf. [5] *Example* 5.6 *pp.*$138 - 139$*)*

$$\sigma(z) = 1 + z\mathsf{s}_1 + z^2\left(\frac{\mathsf{s}_1^3 + \mathsf{s}_3}{\mathsf{s}_1}\right).$$

Example 2.4 ([11])**.** *Let C be a BCH code over $\mathbb{F}_2$, defining set $S = \{1,3,5\}$ and $t = 3$. As in the previous example we set $\mathcal{P} := \mathbb{F}_2[\mathsf{s}_1,\mathsf{s}_3,\mathsf{s}_5][z_1,z_2,z_3]$. Then*

$$\mathsf{I} := \mathbb{I}(z_1 + z_2 + z_3 + \mathsf{s}_1, z_1^3 + z_2^3 + z_3^3 + \mathsf{s}_3, z_1^5 + z_2^5 + z_3^5 + \mathsf{s}_5) \subset \mathcal{P}$$

and the reduced Gröbner basis w.r.t. the lex ordering, with $z_1 < z_2 < z_3$, is

$G = \{z_1^3\mathsf{s}_1^3 + z_1^3\mathsf{s}_3 + z_1^2\mathsf{s}_1^4 + z_1^2\mathsf{s}_1\mathsf{s}_3 + z_1\mathsf{s}_1^2\mathsf{s}_3 + z_1\mathsf{s}_5 + \mathsf{s}_1^6 + \mathsf{s}_1^3\mathsf{s}_3 + \mathsf{s}_1\mathsf{s}_5 + \mathsf{s}_3^2,\ \ z_2^2\mathsf{s}_1^3 + z_2^2\mathsf{s}_3 + z_2z_1\mathsf{s}_1^3 + z_2z_1\mathsf{s}_3 + z_2\mathsf{s}_1^4 + z_2\mathsf{s}_1\mathsf{s}_3 + z_1^2\mathsf{s}_1^3 + z_1^2\mathsf{s}_3 + z_1\mathsf{s}_1^4 + z_1\mathsf{s}_1\mathsf{s}_3 + \mathsf{s}_1^2\mathsf{s}_3 + \mathsf{s}_5,\ \ z_2^2z_1 + z_2^2\mathsf{s}_1 + z_2z_1^2 + z_2\mathsf{s}_1^2 + z_1^2\mathsf{s}_1 + z_1\mathsf{s}_1^2 + \mathsf{s}_1^3 + \mathsf{s}_3,\ \ z_3 + z_2 + z_1 + \mathsf{s}_1\}$*, so that*

$$g(z) = z^3(\mathsf{s}_1^3 + \mathsf{s}_3) + z^2(\mathsf{s}_1^4 + \mathsf{s}_1\mathsf{s}_3) + z(\mathsf{s}_1^2\mathsf{s}_3 + \mathsf{s}_5) + \mathsf{s}_1^6 + \mathsf{s}_1^3\mathsf{s}_3 + \mathsf{s}_1\mathsf{s}_5 + \mathsf{s}_3^2$$

and $\sigma(z) = 1 + z\mathsf{s}_1 + z^2\left(\frac{\mathsf{s}_1^2\mathsf{s}_3+\mathsf{s}_5}{\mathsf{s}_1^3+\mathsf{s}_3}\right) + z^3\left(\frac{\mathsf{s}_1^6+\mathsf{s}_1^3\mathsf{s}_3+\mathsf{s}_1\mathsf{s}_5+\mathsf{s}_3^2}{\mathsf{s}_1^3+\mathsf{s}_3}\right)$.

In the following example we perform decoding.

Example 2.5. *Let C be the binary BCH $[15,5,7]$ code. This code has defining set $\{1,3,5\}$. If we set $\beta_1 := \mathsf{s}_1^3 + \mathsf{s}_3$, $\beta_2 := \mathsf{s}_1^2\mathsf{s}_3 + \mathsf{s}_5$, and*

$$\beta_3 := \mathsf{s}_1^6 + \mathsf{s}_1^3\mathsf{s}_3 + \mathsf{s}_1\mathsf{s}_5 + \mathsf{s}_3^2 = \mathsf{s}_1\beta_2 + \beta_1^2,$$

we obtain:

$$\sigma(z) = 1 + z\mathsf{s}_1 + z^2\beta_2\beta_1^{-1} + z^3\beta_3\beta_1^{-1}.$$

i) Suppose that the error polynomial is $e(x) = x^3$. Obviously the decoder does not know the error polynomial, but it receives a vector in $(\mathbb{F}_2)^{15}$ and it calculates the syndrome components, which in this case are:

$$\mathsf{s}_1 = \alpha^3,\ \mathsf{s}_3 = \alpha^9,\ \mathsf{s}_5 = 1.$$

So $\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$ and $\sigma(z) = 1 + z\alpha^3$. The decoder correctly concludes that the error locator is α^3.

ii) *If the error polynomial is $e(x) = x^3 + x^2$, the syndromes are:*

$$\mathsf{s}_1 = \alpha^6,\ \mathsf{s}_3 = \alpha^5,\ \mathsf{s}_5 = \alpha^5,$$

that is, $\beta_1 = \alpha^{11}, \beta_2 = \alpha, \beta_3 = 0$ and

$$\sigma(z) = 1 + z\alpha^6 + z^2\alpha^5 = (1 + z\alpha^2)(1 + z\alpha^3).$$

iii) *Let $e(x) = x^3 + x^2 + x$ be the error polynomial, then we have:*

$$\mathsf{s}_1 = \alpha^{11},\ \mathsf{s}_3 = \alpha^{11},\ \mathsf{s}_5 = 0,$$

that is, $\beta_1 = \alpha^5, \beta_2 = \alpha^3, \beta_3 = \alpha^{11}$ and then

$$\sigma(z) = 1 + z\alpha^{11} + z^2\alpha^{13} + z^3\alpha^6 = (1 + z\alpha)(1 + z\alpha^2)(1 + z\alpha^3).$$

3 Gröbner bases for cyclic codes

3.1 Decoding binary cyclic codes

In [7], Chen et al. generalize the Cooper's idea of using Gröbner techniques to decoding binary cyclic codes.

We consider a cyclic code C over $\mathbb{F}_2$ with length n and defining set S. As usual we denote by μ the number of errors which occurred and we name v an integer such that $0 < v \leq t$ and $\mu \leq v$. Using the z_j's variables for the error locators (which are n–th roots of unity), we can consider the following system where each syndrome s_i represents a *value* ($s_i \in \mathbb{F}_{2^m}$):

$$\mathcal{F}_{CRHT_2} : \left\{ \left\{ \sum_{j=1}^{v} z_j^i - s_i, i \in S \right\} \bigcup \left\{ z_j^{n+1} - z_j, 1 \leq j \leq v \right\} \right\} \subset \mathbb{F}_{2^m}[z_1, \ldots, z_v]$$

Let E and Z be as in (1) and (2). The system $\mathcal{F}_{CHRT_2}$ defines an ideal $I = \mathbb{I}(\mathcal{F}_{CHRT_2})$ in $\mathbb{F}_{2^m}[z_1, \ldots, z_v]$. The zero set of this ideal gives the error locators and, consequently, the error vector that occurred in the transmission. Gröbner basis computation can be used to find the solutions of this system.

Let μ be the number of errors really occurred during the transmission, $G \subset \mathbb{F}_{2^m}[z_1, \ldots, z_v]$ be the reduced Gröbner basis of I w.r.t. the lex ordering with $z_1 < \cdots < z_v$, and $g(z_1) \in \mathbb{F}_{2^m}[z_1]$ such that $g(z_1) = G \cap \mathbb{F}_{2^m}[z_1]$.

Proposition 3.1 ([7]). *We have:*

a) $\mathsf{E} \subseteq \mathsf{Z} = \{\xi : g(\xi) = 0\}$;

b) $|\mathsf{E}| = \mu \leq v = \deg(g)$.

Compare Theorem 2.1 *a)*–*b)* and Proposition 3.1, which is a generalization of the previous. As regards *c)* and *d)* the following theorem describes the relation between g and the plain error locator polynomial $L_e(z)$ in function of μ (the weight of the error) and hence implies a decoding algorithm for any binary cyclic code up to its true minimum distance.

Theorem 3.2 ([7]). *We have:*

i) If $v = \mu$ then $\mathcal{V}(I)$ consists of all coordinate permutations of the root $(\xi_1, \dots, \xi_\mu)$, $\mathsf{E} = \mathsf{Z}$, $L_e(z) = g(z)$ and $\sigma(z) = z^\mu g(z^{-1})$.

ii) If $v = \mu + 1$ then $(0, \xi_1, \dots, \xi_\mu) \in \mathcal{V}(I)$, $\mathsf{E} = \mathsf{Z} \cup \{0\}$, and $g(z) = z\left(z^\mu \sigma(z^{-1})\right) = zL_e(z)$.

iii) If $v \geq \mu + 2$ then $(\zeta, \zeta, \xi_1, \dots, \xi_\mu, 0 \cdots, 0) \in \mathcal{V}(I)$, $\forall \zeta \in \mathbb{F}_{2^m}$, $\mathsf{E} = \mathbb{F}_{2^m}$ and $g(z) = z^{n+1} - z$.

iv) If $v < \mu$ then $G = \{1\}$.

From this theorem we easily deduce a decoding algorithm for all binary cyclic codes. We will see some examples.

Example 3.3. *Let C be the binary cyclic code $[21, 6, 7]$ with defining set $S = \{1, 5, 9\}$. The splitting field is $\mathbb{F}_{2^6}$ and $t = 3$.*

1. *We first suppose that two errors occurred with the error polynomial $e(x) = 1 + x$. Obviously the decoder does not know μ and $e(x)$, but it calculates the syndrome components, which are $s_1 = 1 + \alpha$, $s_5 = 1 + \alpha^5$ and $s_9 = 1 + \alpha^9$. We set $v = 2$. Then the associated polynomial system $\mathcal{F}_{CRHT_2}$ is*

   $\{z_1 + z_2 + (1 + \alpha), z_1^5 + z_2^5 + (1 + \alpha^5), z_1^9 + z_2^9 + (1 + \alpha^9), z_1^{22} - z_1, z_2^{22} - z_2\}$

   We obtain $g(z) = z^2 + (1 + \alpha)z + \alpha = (z + 1)(z + \alpha) = L_e(z)$.

2. *Let $e(x) = 1 + x + x^3$ be the error polynomial. The syndrome components are $s_1 = 1 + \alpha + \alpha^3$, $s_5 = 1 + \alpha^3 + \alpha^{15}$ and $s_9 = 1 + \alpha^9 + \alpha^{27}$. We set $v = 2$. Then $\mathcal{F}_{CRHT_2}$ is*

   $$\{z_1 + z_2 + s_1, z_1^5 + z_2^5 + s_5, z_1^9 + z_2^9 + s_9, z_1^{22} - z1, z_2^{22} - z_2, z_3^{22} - z_3\}$$

   and the reduced Gröbner basis of $I(\mathcal{F}_{CRHT_2})$ is $G = \{1\}$. So we set $v = 3$, the associated polynomial system $\mathcal{F}_{CRHT_2}$ is

   $\{z_1 + z_2 + z_3 + s_1, z_1^5 + z_2^5 + z_3^5 + s_5, z_1^9 + z_2^9 + z_3^9 + s_9, , z_1^{22} - z_1, z_2^{22} - z_2, z_3^{22} - z_3\}$

   and $g(z) = z^3 + (\alpha^3 + \alpha + 1)z^2 + (\alpha^4 + \alpha^3 + \alpha)z + \alpha^4 = (z + 1)(z + \alpha)(z + \alpha^3) = L_e(z)$.

3.2 Decoding cyclic codes over $GF(q)$

In [8], Chen, Reed, Helleseth and Troung generalize Cooper's approach to q-adic codes proposing a solution for decoding an error whose weight μ is assumed known and they give an alternative approach via Newton's identities.

If we consider a cyclic code over $\mathbb{F}_q$, we use the variables $y = (y_1, \dots, y_\mu)$ for the error values. We suppose that we know the number of errors μ. As before, our goal is to find the error locations and the corresponding error values from the known syndromes $s_i \in \mathbb{F}_{q^m}$, $i \in S_C$. So we consider the polynomial system in $\mathbb{F}_{q^m}[z_1, \dots, z_\mu, y_1, \dots, y_\mu]$:

$$\mathcal{F}_{CHRT_q} : \left\{ \left\{ \sum_{j=1}^{\mu} y_j z_j^i - s_i, i \in S_C \right\} \bigcup \left\{ z_j^{n+1} - z_j, 1 \leq j \leq \mu \right\} \bigcup \left\{ y_j^{q-1} - 1, 1 \leq j \leq \mu \right\} \right\}.$$

Let I be the ideal in $\mathbb{F}_{q^m}[z_1, \dots, z_\mu, y_1, \dots, y_\mu]$ generated by $\mathcal{F}_{CHRT_q}$, and G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $z_1 < \cdots < z_\mu < y_1 < \cdots < y_\mu$. Then we generalize the definitions (1) and (2). Let $\mathcal{V}(I) \subset (\mathbb{F})^{2\mu}$ be the roots of I, we set

$$\mathsf{Z} := \{\xi : (\xi, a_2, \dots, a_\mu, e_1, \dots, e_\mu) \in \mathcal{Z}(\mathsf{I})\}, \quad \mathsf{E} := \{\xi_1, \dots, \xi_\mu\}$$

the set of the error locators of an error with weight μ.

Theorem 3.4 ([8]). *Let g be the monic polynomial in $G \cap \mathbb{F}[x_1]$. We have:*

- $\mathsf{E} = \mathsf{Z} = \{\xi : g(\xi) = 0\}$;
- $\#\mathsf{E} = \mu = \deg(g) \leq t$;
- $L_e(z) = g(z) = \prod_{\xi \in \mathsf{Z}}(z - \xi)$;
- $\sigma(z) = z^\mu g(z^{-1})$.

3.3 A new system with the Newton identities

Denoting $\sigma_j, 1 \leq j \leq \mu$, the j–th elementary symmetric function on the z_i's, the plain error locator polynomial is $L_e(z) = 1 + \sum_{j=1}^{\mu} \sigma_j z^j$. The second decoding scheme proposed in [8] is based on the relations among all syndromes s_i, $i = 1, \dots, n$, and coefficients σ_j of $L_e(z)$, given by the following theorem.

Theorem 3.5 (Newton identities). *Let $s_i = \sum_{j=1}^{\mu} y_j z_j^i$ (as in $\mathcal{F}_{CHRT_q}$), then the following identities hold:*

$$(3) \qquad \begin{cases} s_i + \sum_{j=1}^{i-1} (-1)^j \sigma_j s_{i-j} + (-1)^i i \sigma_i = 0 & 1 \leq i \leq \mu \\ s_i + \sum_{j=1}^{\mu} \sigma_j s_{i-j} = 0 & \mu < i < n \end{cases}$$

Remark 3.6. *If $2\mu \leq n$, polynomial $L_e(z)$ can be uniquely determined from the equations* (3)*.*

We now need some more notation. We denote by $R = \{\ell_1, \dots, \ell_r\}$ a set of representatives for the cyclotomic cosets of $\{i, 1 \leq i \leq n, i \notin S_C\}$. We use variables $(T_1, \dots, T_\mu)$ and we set that T_i stands for σ_i, $1 \leq i \leq \mu$, and variables $(U_1, \dots, U_r)$ for $(s_{\ell_1}, \dots, s_{\ell_r})$. Then let $\mathcal{P} := \mathbb{F}[T_1, \dots, T_\mu, U_1, \dots, U_r]$ and let π be the evaluation defined by

$$\pi : K[T_1, \dots, T_\mu, X_1, \dots, X_n] \longrightarrow \mathcal{P}, \quad \pi(X_i) := \begin{cases} s_i \in \mathbb{F} & i \in S_C \\ U_j^{2^\alpha} & i = 2^\alpha \ell_j \notin S_C \end{cases}$$

We consider the set $\mathcal{F}_N$ of polynomials in $\mathcal{P}$:

$$\left\{\pi(X_i + \sum_{j=1}^{\mu} T_j X_{i-j}), \mu < i < n\right\} \bigcup \left\{U_j^{q^m} - U_j, 1 \leq j \leq r\right\} \bigcup \left\{T_l^{q^m} - T_l, 1 \leq l \leq \mu\right\}$$

Theorem 3.7 ([8])**.** *For each $l, 1 \leq l \leq \mu$, let $g_l \in \mathbb{F}[T_l]$ be the monic generator polynomial of $I(\mathcal{F}_N) \cap \mathbb{F}[T_l]$. Then $g_l = T_l - \sigma_l$.*

Remark 3.8. *Any g_l can be found in an appropriate Gröbner basis.*

4 The CRHT syndrome variety

In the decoding algorithms presented up to now, we have to do, for any word to be decoded, a Gröbner basis computation with syndromes considered as parameters, which are calculated from the received word and substituted into the system. Moreover, different Gröbner basis computations must be performed for different potential error weights, until the true weight of the actual error is obtained.

In [9] a new method is described in which we calculate the Gröbner basis as a "preprocessin", with the syndromes taken as variables x_i. In this way the system has more variables, but we have to calculate the Gröbner basis only once and then simply evaluate it at the actual syndromes each time a word is received.

We use the variables x, z and y with the usual meaning (syndromes, locators, values) and consider system $\mathcal{F}_{CRHT} \subset \mathbb{F}_q[x_1, \dots, x_{n-k}, z_t, \dots, z_1, y_1, \dots, y_t]$:

$$\left\{\left\{\sum_{j=1}^{t} y_j z_j^i - x_i, \ i \in S\right\} \cup \left\{z_j^{n+1} - z_j, 1 \leq j \leq t\right\} \cup \left\{y_j^{q-1} - 1, 1 \leq j \leq t\right\}\right\}.$$

Let $\mathcal{V}(I) \subset (\mathbb{F}_{q^m})^{2\mu}$ and G be the reduced Gröbner basis of $I = \mathbb{I}(\mathcal{F}_{CRHT})$ w.r.t. lex $<$ with $x_1 < \dots < x_{n-k} < z_t < \dots < z_1 < y_1 < \dots < y_t$.

Remark 4.1. *The ideal I is zero–dimensional. From now on we refer to I as the* **syndrome ideal** *and to $\mathcal{V}(I)$ as the* **syndrome variety**.

The decoding algorithm presented in [9] is build on this claim: *the Gröbner basis G contains for each $i, 1 \leq i \leq t$, a* single *element*

$$g_i \in \mathbb{F}_q[x_1, \ldots, x_{n-k}, z_t, \ldots, z_{t-i+1}]$$

with positive *degree in z_{t-i+1}* .

Remark 4.2. *This claim is clearly not true, as shown in [14].*

Theorem 4.3. [9] *Let e be the error vector of weight $\mu' \leq t$ and $\mathbf{s} = (s_1, \ldots, s_{n-k})$ the syndrome vector.*

Under the assumption above and setting

$$g_i(x_1, \ldots, x_{n-k}, 0, \ldots, 0, z_{t-i+1}) = \sum_{j=0}^{n_i} c_{i,j} z_{t-i+1}^j,$$

we have that

1. *The following conditions are equivalent:*
   - *a) there are exactly μ errors;*
   - *b) $c_{1,0}(\mathbf{s}) = \cdots = c_{t-\mu,0}(\mathbf{s}) = 0 \neq c_{t-\mu+1,0}(\mathbf{s})$;*
2. *$L_e(z) = \gcd\left(g_{t-\mu}(\mathbf{s}, 0, z), z^n - 1\right)$.*

From the theorem we directly design the following decoding algorithm:

```
$\mu := 1$
**While** $c_{\mu,0}(s_1, \ldots, s_{n-k}) = 0$ **do** $\mu := \mu + 1$
  $g := \gcd(g_\mu(s_1, \ldots, s_{n-k}, 0, \ldots, 0, z), z^n - 1)$
  $\sigma(z) := z^\mu g(z^{-1})$
```

Table 1: CHRT decoding algorithm

The proposed algorithm needs the assumption that the related Gröbner basis has a particular structure, but in [14] Loustaunau and York remark that the CRHT assumption, in general, does not hold and they make a weak proposal to correct the CRHT algorithm. Moreover, they observe that the suggested Gröbner computation cannot be performed by the best software and hardware of the period (1997), therefore suggest to use the FGLM algorithm (the ideal is 0-dimensional). Their remark is particular significant, since the same software/hardware is able to compute Cooper's ideal Example 2.5 within 18 secs.

5 The Gianni–Kalkbrenner shape theorem

The structure of the Gröbner basis of a zero–dimensional ideal has been deeply analyzed in [12] and [13]. [6] gives a correct and optimized version of the CRHT decoding algorithm, based on the Gianni–Kalkbrenner Gröbner shape theorem.

Let $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ its algebraic closure. We set $\mathcal{P} = \mathbb{F}[x_1, \ldots, x_n]$. For any $f \in \mathcal{P}$, we will denote by $\mathbf{T}(f)$ the *leading term* of f (w.r.t. a fixed term ordering); and, for any set $H \subset \mathcal{P}$, $\mathbf{T}\{H\}$ denotes the set $\{\mathbf{T}(h) \mid h \in H\}$. We will use the lexicographical ordering $<$ induced by $x_1 < \cdots < x_n$. In order to describe the structure of the Gröbner basis of an ideal, we need to consider $\mathcal{P}$ also as univariate polynomials in the variable x_n with coefficients in the polynomial ring $\mathbb{F}[x_1, \ldots, x_{n-1}]$. For any element $f \in \mathcal{P}$ we have:

$$f = \sum_{k=0}^{h} b_k(x_1, \ldots, x_{n-1})x_n^k = Tp(f) + \cdots + Lp(f)x_n^h,$$

where we will denote by $Lp(f) = b_h(x_1, \ldots, x_{n-1})$ the *leading polynomial* and by $Tp(f) = b_0(x_1, \ldots, x_{n-1})$ the *trailing polynomial* of f.

Definition 5.1. *Let $I \subset \mathcal{P}$ be an ideal and d an integer such that $d \leq n$. The d–th elimination ideal I_d is the ideal of $\mathbb{F}[x_1, \ldots, x_d]$ defined by $I_d = I \cap \mathbb{F}[x_1, \ldots, x_d]$.*

We consider an ideal $I \subset \mathcal{P}$ and we name $\mathcal{V}(I_d) \subset \overline{\mathbb{F}}^d$ the set of the roots of I_d. Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $I \subset \mathcal{P}$ w.r.t. $<$, ordered so that $\mathbf{T}(g_1) < \cdots < \mathbf{T}(g_s)$. For any $\iota \leq n$, let G_ι be $G \cap \mathbb{F}[x_1, \ldots, x_\iota]$ and

$$\forall \ell \in \mathbb{N},\ G_{\iota\ell} := \{g \in G_\iota \setminus G_{\iota-1} \mid \deg_{x_\iota}(g) = \ell\},$$

so that each G_ι can be decomposed into blocks of polynomials according to their degree with respect to the variable x_ι: $G_\iota = \sqcup_\ell G_{\iota\ell}$. In this way, if $g \in G_{\iota\ell}$, we have

- $g \in \mathbb{F}[x_1, \ldots, x_{\iota-1}][x_\iota] \setminus \mathbb{F}[x_1, \ldots, x_{\iota-1}]$;
- $\deg_{x_\iota}(g) = \ell$, i.e. $g = Lp(g)x_\iota^\ell + \ldots + Tp(g)$.

Theorem 5.2 ([12, 13])**.** *Let $\alpha := (a_1, \ldots, a_d) \in \mathcal{V}(I_d)$ and Φ_α s.t. $\Phi_\alpha : \mathcal{P} \to \mathbb{F}[x_{d+1}, \ldots, x_n]$,*

$$f(X) \to f(\alpha, x_{d+1}, \ldots, x_n).$$

Let ϵ be the minimal value such that $\Phi_\alpha(Lp(g_\epsilon)) \neq 0$ and j, δ the values such that $g_\epsilon \in G_{j\delta}$. Then

1. *$j = d + 1$;*

2. *for each $g \in G_{\iota\ell}$:*
   - *if $\iota \leq d$ then $\Phi_\alpha(g) = 0$;*
   - *if $\iota = d+1 = j, \ell < \delta$ then $\Phi_\alpha(g) = 0$;*
3. $\Phi_\alpha(g_\epsilon) = \gcd\left(\Phi_\alpha(g) : g \in G_{d+1}\right) \in \overline{\mathbb{F}}[x_{d+1}]$*;*
4. *for each $a \in \overline{\mathbb{F}}$;*

$$(a_1, \ldots, a_d, a) \in \mathcal{V}(I_{d+1}) \iff \Phi_\alpha(g_\sigma)(a) = 0. \qquad \square$$

This theorem allows us to improve the CRHT–algorithm. We use variables $(x_1, \ldots, x_{n-k}), (z_1, \ldots, z_t)$ and $(y_1, \ldots, y_t)$ as in $\mathcal{F}_{CRHT_q}$, and we set $\mathcal{Q} := \mathbb{F}_q[x_1, \ldots, x_{n-k}]$ and $\mathcal{P} := \mathbb{F}_q[x_1, \ldots, x_{n-k}, z_t, \ldots, z_1, y_1, \ldots, y_t]$. Then we consider the following equations:

$$f_i := \sum_{l=1}^{t} y_l z_l^j - x_i, \; h_j := z_j^{n+1} - z_j, \; \lambda_j := y_j^q - 1, \; \chi_i := x_i^{q^m} - x_i.$$

We obtain the polynomial equations system:

$$\mathcal{F}_{CM} = \{f_i, h_j, \lambda_j, \chi_i : 1 \leq j \leq t, 1 \leq i \leq n-k\} \subset \mathcal{P}.$$

Remark 5.3. *Respect to $\mathcal{F}_{CRHT_q}$ this system adds the relations $x_i^{q^m} - x_i$ satisfied by the syndromes. The role of the polynomials h_j, λ_j, χ_j, is noteworthy, in fact they remove all the roots that are in algebraic extensions outside $\mathbb{F}$ and they make the other roots simple. This means that the syndrome ideal I, which is a zero dimensional ideal, is also radical.*

Let G be the reduced Gröbner basis of the I w.r.t. the lex ordering $<$ induced by $x_1 < \cdots < x_{n-k} < z_t < \cdots < z_1 < y_1, \cdots < y_t$. Let us then denote, for each $\iota \leq n$ and each $\ell \in \mathbb{N}$

$$G_\iota := G \cap \mathcal{Q}[z_t, \cdots, z_\iota] \text{ and } G_{\iota\ell} := \{g \in G_\iota \setminus G_{\iota+1} : \deg_{x_\iota}(g) = \ell\}.$$

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

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

Theorem 5.4. *With the above notation, we have:*

- *if $\ell < \iota$ then $G_{\iota\ell} = \emptyset$;*
- *if $\ell > \iota$ then $\ell = n+1, G_{\iota\ell} = \{z_\iota^{n+1} - z_\iota\}$*

For each $g \in G_{\iota\iota}$,

$$Lp(g)(s_1, \ldots, s_{n-k}, 0, \ldots, 0) \neq 0 \iff g(s_1, \ldots, s_{n-k}, 0, \ldots, 0, z_\mu) \neq 0.$$

If the error has weight μ, then, for each $g \in G_{\iota\iota}$,

1. *if $\iota < \mu$ then $g(s_1, \dots, s_{n-k}, 0, \dots, 0, z_\iota) = 0$;*
2. *if $\iota = \mu$ and $Lp(g)(s_1, \dots, s_{n-k}, 0, \dots, 0) \neq 0$ then*
$$0 \neq g(s_1, \dots, s_{n-k}, 0, \dots, 0, z_\mu) = z_\mu^\mu L_e(z_\mu);$$
3. *if $\iota = \mu + 1$ and $Lp(g)(s_1, \dots, s_{n-k}, 0, \dots, 0) \neq 0$ then*
$$g(s_1, \dots, s_{n-k}, 0, \dots, 0, z_\iota) = z_\iota \cdot (z_\iota^\mu L_e(z_\iota));$$
4. *if $\iota > \mu + 1$ and $Lp(g)(s_1, \dots, s_{n-k}, 0, \dots, 0) \neq 0$ then*
$$z_\iota \cdot (z_\iota^\mu L_e(z_\iota)) \mid g(s_1, \dots, s_{n-k}, 0, \dots, 0, z_\iota).$$

Example 5.5. *We consider the cyclic code $[15, 5, 7]$ over $\mathbb{F}_2$ and defining set $\{1, 3, 5\}$. The syndrome ideal I is generated by: $\{z_1+z_2+z_3+x_1,\ z_1^3+z_2^3+z_3^3+x_3,\ z_1^5+z_2^5+z_3^5+x_5, x_1^{16}+x_1,\ x_2^{16}+x_2,\ x_3^{16}+x_3,\ z_1^{16}+z_1,\ z_2^{16}+z_2,\ z_3^{16}+z_3\}$. The relevant part of the reduced Gröbner basis of I is $\{g_{3\ 3\ 1}, g_{3\ 3\ 2}, g_{3\ 3\ 3}, g_{3\ 16\ 1}, g_{2\ 2\ 1}, g_{2\ 2\ 2}, g_{2\ 2\ 3}, g_{2\ 2\ 4}, g_{2\ 16\ 1}, g_{1\ 1\ 1}\}$, where*[1]

$$\begin{aligned}
g_{3\ 3\ 1} &= z_3^3(\mathbf{x_2x_3^3} + \mathbf{x_2}) + z_3^2x_1x_2x_3^3 + z_3^2x_1x_2 + z_3x_1^{11}x_2^3 + z_3x_1^8x_2^4x_3^3 \\
&+ z_3x_1^6x_2^3x_3 + z_3x_1^5x_2^{10} + z_3x_1^5x_2^5x_3^3 + z_3x_1^5x_3^3 + z_3x_1^4x_2^2x_3^2 + z_3x_1^3x_2^4x_3 \\
&+ z_3x_1^2x_2^{11}x_3^3 + z_3x_1^2x_2^{11} + z_3x_1^2x_2^6x_3^3 + z_3x_1^2x_2^6 + z_3x_1x_2^8x_3^2 + z_3x_1x_2^3x_3^2 \\
&+ z_3x_2^{10}x_3 + z_3x_2^5x_3 + z_3x_3 + \mathtt{x_1^{12}x_2^3} + \mathtt{x_1^8x_2x_3^2} + \mathtt{x_1^7x_2^8x_3} + \mathtt{x_1^7x_2^3x_3} + \mathtt{x_1^6x_2^{10}} \\
&+ \mathtt{x_1^6x_3^3} + \mathtt{x_1^5x_2^{12}x_3^2} + \mathtt{x_1^4x_2^9x_3} + \mathtt{x_1^3x_2^{11}} + \mathtt{x_1^3x_2^6x_3^3} + \mathtt{x_1^3x_2^6} + \mathtt{x_1^3x_2x_3^3} + \mathtt{x_1^3x_2} \\
&+ \mathtt{x_1^2x_2^{13}x_3^2} + \mathtt{x_1x_2^{15}x_3} + \mathtt{x_1x_2^{10}x_3} + \mathtt{x_1x_3} + \mathtt{x_2^{12}x_3^3} + \mathtt{x_2^7x_3^3} + \mathtt{x_2^2},
\end{aligned}$$

$$\begin{aligned}
g_{3\ 3\ 2} &= z_3^3(\mathbf{x_2^5} + \mathbf{x_3^3}) + z_3^2x_1x_2^5 + z_3^2x_1x_3^3 + z_3x_1^{11}x_2^2 + z_3x_1^8x_2^{13}x_3^3 + z_3x_1^8x_2^8 \\
&+ z_3x_1^8x_2^3 + z_3x_1^7x_2^5x_3^2 + z_3x_1^6x_2^7x_3 + z_3x_1^5x_2^{14}x_3^3 + z_3x_1^5x_2^9x_3^3 + z_3x_1^5x_2^9 \\
&+ z_3x_1^4x_2x_3^2 + z_3x_1^3x_2^{13}x_3 + z_3x_1^2x_2^{10}x_3^3 + z_3x_1^2x_2^5x_3^3 + z_3x_1^2x_2^5 + z_3x_1^2 \\
&+ z_3x_1x_2^{12}x_3^2 + z_3x_1x_2^7x_3^2 + z_3x_2^9x_3 + \mathtt{x_1^{12}x_2^2} + \mathtt{x_1^8x_2^5x_3^2} + \mathtt{x_1^7x_2^{12}x_3} + \mathtt{x_1^7x_2^2x_3} \\
&+ \mathtt{x_1^6x_2^9x_3^3} + \mathtt{x_1^6x_2^4} + \mathtt{x_1^5x_2x_3^2} + \mathtt{x_1^4x_2^{13}x_3} + \mathtt{x_1^3x_2^{15}} + \mathtt{x_1^3x_2^{10}x_3^3} + \mathtt{x_1^3x_2^{10}} \\
&+ \mathtt{x_1^3x_3^3} + \mathtt{x_1^3} + \mathtt{x_1^2x_2^2x_3^2} + \mathtt{x_1x_2^9x_3} + \mathtt{x_2^{11}},
\end{aligned}$$

$$\begin{aligned}
g_{3\ 3\ 3} &= z_3^3(\mathbf{x_1} + \mathbf{x_2^2x_3^2}) + z_3^2x_1^2 + z_3^2x_1x_2^2x_3^2 + z_3x_1^{12}x_2^2 + z_3x_1^8x_2^5x_3^2 + z_3x_1^8x_3^2 \\
&+ z_3x_1^7x_2^{12}x_3 + z_3x_1^7x_2^7x_3 + z_3x_1^7x_2^2x_3 + z_3x_1^6x_2^{14}x_3^3 + z_3x_1^6x_2^9x_3^3 + z_3x_1^6x_2^9 \\
&+ z_3x_1^5x_2^{11}x_3^2 + z_3x_1^5x_2x_3^2 + z_3x_1^4x_2^{13}x_3 + z_3x_1^4x_2^8x_3 + z_3x_1^4x_2^3x_3 + \\
&+ z_3x_1^3x_2^{10}x_3^3 + z_3x_1^3x_2^{10} + z_3x_1^3x_2^5x_3^3 + z_3x_1^3x_2^5 + z_3x_1^2x_2^{12}x_3^2 + z_3x_1x_2^4x_3 \\
&+ z_3x_2^{11}x_3^3 + z_3x_2^6x_3^3 + \mathtt{x_1^{10}x_2^3} + \mathtt{x_1^8x_2^{12}x_3} + \mathtt{x_1^8x_2^7x_3} + \mathtt{x_1^7x_2^4x_3^3} + \mathtt{x_1^6x_2^{11}x_3^2} \\
&+ \mathtt{x_1^6x_2^6x_3^2} + \mathtt{x_1^5x_2^8x_3} + \mathtt{x_1^5x_2^3x_3} + \mathtt{x_1^4x_2^{15}} + \mathtt{x_1^4x_2^{10}} + \mathtt{x_1^4x_2^5x_3^3} \\
&+ \mathtt{x_1^3x_2^7x_3^2} + \mathtt{x_1^2x_2^4x_3} + \mathtt{x_1x_2^{11}} + \mathtt{x_1x_2^6x_3^3} + \mathtt{x_1x_2^6} + \mathtt{x_2^{13}x_3^2} + \mathtt{x_2^8x_3^2} \\
g_{3\ 16\ 1} &= z_3^{16} + z_3,
\end{aligned}$$

[1] The **bold** polynomials are the leading polynomials, the `typewriter` ones are the trailing polynomials.

$$
\begin{aligned}
g_{2\ 2\ 1} &= z_2^2(\mathbf{x_2x_3^3+x_2})+z_2z_3(\mathbf{x_2x_3^3+x_2})+z_2x_1(\mathbf{x_2x_3^3+x_2})+z_3^2x_2x_3^3+z_3^2x_2\\
&+ z_3x_1x_2x_3^3+z_3x_1x_2+\mathtt{x}_1^{11}\mathtt{x}_2^3+\mathtt{x}_1^8\mathtt{x}_2^4\mathtt{x}_3^3+\mathtt{x}_1^7\mathtt{x}_2\mathtt{x}_3^2+\mathtt{x}_1^6\mathtt{x}_2^3\mathtt{x}_3+\mathtt{x}_1^5\mathtt{x}_2^{10}\\
&+ \mathtt{x}_1^5\mathtt{x}_2^5\mathtt{x}_3^3+\mathtt{x}_1^5\mathtt{x}_3^3+\mathtt{x}_1^4\mathtt{x}_2^2\mathtt{x}_3^2+\mathtt{x}_1^3\mathtt{x}_2^4\mathtt{x}_3+\mathtt{x}_1^2\mathtt{x}_2^{11}\mathtt{x}_3^3+\mathtt{x}_1^2\mathtt{x}_2^{11}\\
&+ \mathtt{x}_1^2\mathtt{x}_2^6\mathtt{x}_3^3+\mathtt{x}_1^2\mathtt{x}_2^6+\mathtt{x}_1\mathtt{x}_2^8\mathtt{x}_3^2+\mathtt{x}_1\mathtt{x}_2^3\mathtt{x}_3^2+\mathtt{x}_2^{10}\mathtt{x}_3+\mathtt{x}_2^5\mathtt{x}_3+\mathtt{x}_3,
\end{aligned}
$$

$$
\begin{aligned}
g_{2\ 2\ 2} &= z_2^2(\mathbf{x_2^5+x_3^3})+z_2z_3(\mathbf{x_2^5+x_3^3})+z_2x_1(\mathbf{x_2^5+x_3^3})+z_3^2x_2^5+z_3^2x_3^3+z_3x_1x_2^5\\
&+ z_3x_1x_3^3+\mathtt{x}_1^{11}\mathtt{x}_2^2+\mathtt{x}_1^8\mathtt{x}_2^{13}\mathtt{x}_3^3+\mathtt{x}_1^8\mathtt{x}_2^8+\mathtt{x}_1^8\mathtt{x}_2^3+\mathtt{x}_1^7\mathtt{x}_2^5\mathtt{x}_3^2+\mathtt{x}_1^5\mathtt{x}_2^9\mathtt{x}_3^3+\mathtt{x}_1^5\mathtt{x}_2^9+\mathtt{x}_1^4\mathtt{x}_2\mathtt{x}_3^2\\
&+ \mathtt{x}_1^3\mathtt{x}_2^{13}\mathtt{x}_3+\mathtt{x}_1^2\mathtt{x}_2^{10}\mathtt{x}_3^3+\mathtt{x}_1^2\mathtt{x}_2^5\mathtt{x}_3^3+\mathtt{x}_1^2\mathtt{x}_2^5+\mathtt{x}_1^2+\mathtt{x}_1\mathtt{x}_2^{12}\mathtt{x}_3^2+\mathtt{x}_1\mathtt{x}_2^7\mathtt{x}_3^2+\mathtt{x}_2^9\mathtt{x}_3,
\end{aligned}
$$

$$
\begin{aligned}
g_{2\ 2\ 3} &= z_2^2(\mathbf{x_1+x_2^2x_3^2})+z_2z_3(\mathbf{x_1+x_2^2x_3^2})+z_2x_1(\mathbf{x_1+x_2^2x_3^2})+z_3^2x_1+z_3^2x_2^2x_3^2\\
&+ z_3x_1^2+z_3x_1x_2^2x_3^2+\mathtt{x}_1^{12}\mathtt{x}_2^2+\mathtt{x}_1^8\mathtt{x}_2^5\mathtt{x}_3^2+\mathtt{x}_1^8\mathtt{x}_3^2+\mathtt{x}_1^7\mathtt{x}_2^{12}\mathtt{x}_3+\mathtt{x}_1^7\mathtt{x}_2^7\mathtt{x}_3+\mathtt{x}_1^7\mathtt{x}_2^2\mathtt{x}_3\\
&+ \mathtt{x}_1^6\mathtt{x}_2^{14}\mathtt{x}_3^3+\mathtt{x}_1^6\mathtt{x}_2^9\mathtt{x}_3^3+\mathtt{x}_1^6\mathtt{x}_2^9+\mathtt{x}_1^5\mathtt{x}_2^{11}\mathtt{x}_3^2+\mathtt{x}_1^5\mathtt{x}_2\mathtt{x}_3^2+\mathtt{x}_1^4\mathtt{x}_2^{13}\mathtt{x}_3+\mathtt{x}_1^4\mathtt{x}_2^8\mathtt{x}_3+\mathtt{x}_1^4\mathtt{x}_2^3\mathtt{x}_3\\
&+ \mathtt{x}_1^3\mathtt{x}_2^{10}\mathtt{x}_3^3+\mathtt{x}_1^3\mathtt{x}_2^{10}+\mathtt{x}_1^3\mathtt{x}_2^5\mathtt{x}_3^3+\mathtt{x}_1^3\mathtt{x}_2^5+\mathtt{x}_1^2\mathtt{x}_2^{12}\mathtt{x}_3^2+\mathtt{x}_1\mathtt{x}_2^4\mathtt{x}_3+\mathtt{x}_2^{11}\mathtt{x}_3^3+\mathtt{x}_2^6\mathtt{x}_3^3,
\end{aligned}
$$

$$
\begin{aligned}
g_{2\ 2\ 4} &= z_2^2(\mathbf{z_3+x_2^2x_3^2})+z_2z_3(\mathbf{z_3+x_2^2x_3^2})+z_2x_1(\mathbf{z_3+x_2^2x_3^2})+z_3^2x_2^2x_3^2+z_3x_1x_2^2x_3^2\\
&+ \mathtt{x}_1^{12}\mathtt{x}_2^2+\mathtt{x}_1^8\mathtt{x}_2^5\mathtt{x}_3^2+\mathtt{x}_1^8\mathtt{x}_3^2+\mathtt{x}_1^7\mathtt{x}_2^{12}\mathtt{x}_3+\mathtt{x}_1^7\mathtt{x}_2^7\mathtt{x}_3+\mathtt{x}_1^7\mathtt{x}_2^2\mathtt{x}_3+\mathtt{x}_1^6\mathtt{x}_2^{14}\mathtt{x}_3^3+\mathtt{x}_1^6\mathtt{x}_2^9\mathtt{x}_3^3\\
&+ \mathtt{x}_1^6\mathtt{x}_2^9+\mathtt{x}_1^5\mathtt{x}_2^{11}\mathtt{x}_3^2+\mathtt{x}_1^5\mathtt{x}_2\mathtt{x}_3^2+\mathtt{x}_1^4\mathtt{x}_2^{13}\mathtt{x}_3+\mathtt{x}_1^4\mathtt{x}_2^8\mathtt{x}_3+\mathtt{x}_1^4\mathtt{x}_2^3\mathtt{x}_3+\mathtt{x}_1^3\mathtt{x}_2^{10}\mathtt{x}_3^3\\
&+ \mathtt{x}_1^3\mathtt{x}_2^{10}+\mathtt{x}_1^3\mathtt{x}_2^5\mathtt{x}_3^3+\mathtt{x}_1^3\mathtt{x}_2^5+\mathtt{x}_1^3+\mathtt{x}_1^2\mathtt{x}_2^{12}\mathtt{x}_3^2+\mathtt{x}_1\mathtt{x}_2^4\mathtt{x}_3+\mathtt{x}_2^{11}\mathtt{x}_3^3+\mathtt{x}_2^6\mathtt{x}_3^3+\mathtt{x}_2,\\
g_{2\ 16\ 1} &= z_2^{16}+z_2, \quad g_{1\ 1\ 1}=z_1+z_2+z_3+x_1.
\end{aligned}
$$

that we can rewrite compactly as

$$
\begin{aligned}
g_{3\ 3\ 1} &= z_3^3(\mathbf{x_2x_3^3+x_2})+\cdots+A\\
g_{3\ 3\ 2} &= z_3^3(\mathbf{x_2^5+x_3^3})+\cdots+B\\
g_{3\ 3\ 3} &= z_3^3(\mathbf{x_1+x_2^2x_3^2})+\cdots+C\\
g_{3\ 16\ 1} &= z_3^{16}+z_3,\\
g_{2\ 2\ 1} &= z_2^2(\mathbf{x_2x_3^3+x_2})+\cdots+D\\
g_{2\ 2\ 2} &= z_2^2(\mathbf{x_2^5+x_3^3})+\cdots+E\\
g_{2\ 2\ 3} &= z_2^2(\mathbf{x_1+x_2^2x_3^2})+\cdots+F\\
g_{2\ 2\ 4} &= z_2^2(\mathbf{z_3+x_2^2x_3^2})+\cdots+G\\
g_{2\ 16\ 1} &= z_2^{16}+z_2, \quad g_{1\ 1\ 1}=z_1+z_2+z_3+x_1,
\end{aligned}
$$

If we restrict our attention to the leading polynomials we note that $Lp(g_{3\ 3\ 1}) = Lp(g_{2\ 2\ 1})$, $Lp(g_{3\ 3\ 2}) = Lp(g_{2\ 2\ 2})$ and $Lp(g_{3\ 3\ 3}) = Lp(g_{2\ 2\ 3})$. Moreover we can observe a telescopic behavior, namely:

$$
\begin{aligned}
g_{3\ 3\ 1}(x_1,x_2,x_3,z_3) &= z_3g_{2\ 2\ 1}(x_1,x_2,x_3,0,z_3)+Tp(g_{3\ 3\ 1})(x_1,x_2,x_3),\\
g_{3\ 3\ 2}(x_1,x_2,x_3,z_3) &= z_3g_{2\ 2\ 2}(x_1,x_2,x_3,0,z_3)+Tp(g_{3\ 3\ 2})(x_1,x_2,x_3),\\
g_{3\ 3\ 3}(x_1,x_2,x_3,z_3) &= z_3g_{2\ 2\ 3}(x_1,x_2,x_3,0,z_3)+Tp(g_{3\ 3\ 3})(x_1,x_2,x_3),\\
g_{2\ 2\ *}(x_1,x_2,x_3,0,z_2) &= z_2Lp(g_{2\ 2\ *})(z_2+x_1)+Tp(g_{2\ 2\ *})(x_1,x_2,x_3).
\end{aligned}
$$

We conclude this section with the algorithm proposed in [6]. It accepts as input a syndrome vector and outputs an error locator polynomial.

```
$\mu := t$, $g := 1$,
    Repeat
        $j := 0$
        Repeat $j := j + 1$
        Until $Lp(g_{\mu\mu j})(s,0) \neq 0$ or $j > j_{\mu\mu}$
        If $j > j_{\mu\mu}$ then $\mu := \mu - 1$
        else
        If $Tp(g_{\mu\mu j})(s,0) = 0$ do $\mu := \mu - 1$
        else
            $g(z) := g_{\mu\mu j}(s,0,z)$;
    Until $g \neq 1$ or $\mu = 0$
Output $\mu$, $x^{\mu} g(x^{-1})$
```

Table 2: Caboara decoding algorithm

The decoder performs the following branchings:

$$\begin{array}{llllllll}
s_2 s_3^3 + s_2 \neq 0 & A \neq 0 & & & & & \rightarrow & g_{3\ 3\ 1} \\
 & A = 0 & D \neq 0 & & & & \rightarrow & g_{2\ 2\ 1} \\
 & & D = 0 & & & & \rightarrow & g_{1\ 1\ 1} \\
s_2 s_3^3 + s_2 = 0 & s_2^5 + s_3^3 \neq 0 & B \neq 0 & & & & \rightarrow & g_{3\ 3\ 2} \\
 & & B = 0 & E \neq 0 & & & \rightarrow & g_{2\ 2\ 2} \\
 & & & E = 0 & & & \rightarrow & g_{1\ 1\ 1} \\
 & s_2^5 + s_3^3 = 0 & s_1 + s_2^2 s_3^2 \neq 0 & C \neq 0 & & & \rightarrow & g_{3\ 3\ 3} \\
 & & & C = 0 & F \neq 0 & & \rightarrow & g_{2\ 2\ 3} \\
 & & & & F = 0 & & \rightarrow & g_{1\ 1\ 1} \\
 & & s_1 + s_2^2 s_3^2 = 0 & s_2^2 s_3^2 \neq 0 & G \neq 0 & & \rightarrow & g_{2\ 2\ 4} \\
 & & & & G = 0 & s_1 \neq 0 & \rightarrow & g_{1\ 1\ 1} \\
 & & & & & s_1 = 0 & \rightarrow & 1 \\
 & & & s_2^2 s_3^2 = 0 & s_1 \neq 0 & & \rightarrow & g_{1\ 1\ 1} \\
 & & & & s_1 = 0 & & \rightarrow & 1
\end{array}$$

Remark 5.6. [*6*] *reports also a proposal (suggested by M. Sala) of computing and processing, for each $\mu, 1 \leq \mu \leq t$, the Gröbner basis of the ideal, encoding only the case in which there are exactly μ errors and performing a postprocessing using Gröbner technology in order to improve the syndrome test. The result (still for $\{1,3,5\}$) is a very promising decision tree:*

$$\begin{array}{llllrcl}
s_2 = 0 & s_3 = 0 & & \Longrightarrow & L & = & 1 \\
s_2 = 0 & s_3 \neq 0 & & \Longrightarrow & L & = & 1 + z s_1 + z^2 s_1^2 \\
s_2^5 + 1 = 0 & s_3 = 0 & s_1 = 0 & \Longrightarrow & L & = & 1 + z^3 s_2 \\
s_2^5 + 1 = 0 & s_3 = 0 & s_1 \neq 0 & \Longrightarrow & L & = & 1 + z s_1 \\
 & & & & & + & z^2 \left(s_1^{11} s_2^2 s_1^5 s_2^4 \right) + z^3 s_1^9 s_2^3 \\
s_2^5 + 1 = 0 & s_3 \neq 0 & \sigma = 0 & \Longrightarrow & L & = & 1 + z s_1 \\
s_2^5 + 1 = 0 & s_3 \neq 0 & \sigma \neq 0 & \Longrightarrow & L & = & 1 + z s_1 \\
 & & & & & + & z^2 \left(s_1^2 + s_2^4 s_3^4 \right) \left(s_1^5 s_3^2 + \sigma^{-1} \right) \\
 & & & & & + & z^3 s_1^2 s_2^2 s_3 \left(s_1^5 + s_2^{10} s_3^{10} \right) \sigma^{-1} \\
s_2^6 + s_2 \neq 0 & s_3 = 0 & & \Longrightarrow & L & = & 1 + z s_1 + z^2 s_1^2 s_2^5
\end{array}$$

$$\begin{array}{llllcll}
s_2^6+s_2\neq 0 & s_3^3\neq 0 & s_1=0 & \Longrightarrow & L & = & 1+z^2s_2^{-1}s_3+z^3s_2 \\
s_2^6+s_2\neq 0 & s_3^3\neq 0 & \rho=0 & \Longrightarrow & L & = & 1+zs_1+z^2s_2^9s_3 \\
s_2^6+s_2\neq 0 & s_3^3\neq 0 & s_1\rho\neq 0 & \Longrightarrow & L & = & 1+zs_1 \\
 & & & & & + & z^2\left(s_1^5s_2^8s_3+s_1^3s_2^2s_3^2\right)\rho^{-1} \\
 & & & & & + & z^2\left(s_1^2s_2^9s_3+s_2^{13}s_3^2\right)\rho^{-1} \\
 & & & & & + & z^3s_1^4s_2^3s_3 \\
 & & & & & + & z^3s_1^3s_2^5+s_1s_2^{-1}s_3+s_2^{-4}
\end{array}$$

$$\begin{array}{lrcl}
\text{where} & \rho & := & s_1^2+s_1s_2^2s_3^2+s_2^{-1}s_3 \\
 & \sigma & := & s_1+s_2^2s_3^2.
\end{array}$$

□

6 The general error locator polynomial

If we consider the syndrome variety $V(\mathcal{F}_{\mathcal{CM}})$, then we have that, for every given correctable syndrome $\mathsf{s}\in(\mathbb{F}_{q^m})^{n-k}$, there are some points in $V(\mathcal{F}_{\mathcal{CM}})$ that uniquely determine the error locations and the error values. Unfortunately in $V(\mathcal{F}_{\mathcal{CM}})$ there are also other points that do not correspond directly to error vectors. Such points are of type:

$$(\xi_1,\dots,\xi_\mu,\zeta,\zeta,\underbrace{0,\dots,0}_{t-(\mu+2)},\overline{y}_1,\dots,\overline{y}_\mu,Y,-Y,\mathsf{y}_1,\dots,\mathsf{y}_{t-(\mu+2)}),$$

with ζ any n-th root of unity, Y,y_j arbitrary elements in $\mathbb{F}_q$ and $\overline{y}_j$ in $\mathbb{F}_q$ the error values corresponding to the error locators ξ_j. In [15] a new syndrome variety is proposed, which permits to eliminate these spurious solutions and to define the general error locator polynomial. We consider $[n,k,d]$ cyclic codes over $\mathbb{F}_q$, with $(q,n)=1$. We need the following definition.

Definition 6.1. *Let $n\in\mathbb{N}$ be an integer. We denote by $p_{l\tilde{l}}\in K[z_1,\dots,z_t]$ the polynomial:*

$$p_{l\tilde{l}}:=\frac{\left(z_l^n-z_{\tilde{l}}^n\right)}{z_l-z_{\tilde{l}}},1\leq l<\tilde{l}\leq t.$$

We consider a new syndrome ideal $I=\mathbb{I}(V(\mathcal{F}_{OS}))$, the OS ideal, as:

$$\mathcal{F}_{OS}=\{f_i,h_j,\chi_i,\lambda_j,\mathsf{p}_{l\tilde{l}},\ 1\leq l<\tilde{l}\leq t,1\leq i\leq n-k,j\in S\}\quad\subset\mathcal{P},$$

where

$$f_i:=\sum_{l=1}^{t}y_lz_l^j-x_i,\ \ \mathsf{p}_{l\tilde{l}}:=z_{\tilde{l}}z_lp_{l\tilde{l}},$$

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

Let G be the reduced Gröbner basis of I w.r.t. the lex ordering with $x_1<\cdots<x_{n-k}<z_t<\cdots<z_1<y_1<\cdots<y_t$. We have

Theorem 6.2 ([15])**.** *Let I and G be as above. Then:*

- $G \cap \mathcal{Q}[z_1, \dots, z_t] = \cup_{i=1}^{t} G_i$*;*
- $G_i = \cup_{\delta=1}^{i} G_{i\delta}$ *and* $G_{i\delta} \neq \emptyset$*,* $1 \leq i \leq t$ *and* $1 \leq \delta \leq i$*;*
- $G_{ii} = \{g_{ii1}\}$*,* $1 \leq i \leq t$*, i.e. exactly one polynomial exists with degree i w.r.t. the variable z_i in G_i;*
- $Lt(g_{ii1}) = z_i^i, \quad Lp(g_{ii1}) = 1$*;*
- *if* $1 \leq i \leq t$ *and* $1 \leq \delta \leq i-1$*, then* $\forall g \in G_{i\delta}$*,* $Tp(g) = 0$.

Let g_{tt1} be the unique polynomial with degree t w.r.t. variable z_t in G_t:

$$g_{tt1} = z_t^t + \sum_{l=1}^{t} a_{t-l} z_t^{t-l}$$

The following properties are equivalent:

- there are exactly μ errors;
- $a_{t-l}(s) = 0$ for $l > \mu$ and $a_{t-\mu}(s) \neq 0$;
- $g_{tt1}(s, z_t) = z^{t-\mu}\,(L_e(z))$;

and imply that $\sigma(z) = z^{\mu} g_{tt1}(s, z^{-1})$. This means that g_{tt1} is a monic polynomial in $\mathcal{Q}[z]$ 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 $t - \mu$,

and is called a **general error locator polynomial** of C.

Theorem 6.3 ([15])**.** *Every cyclic code possesses a general error locator polynomial.*

Once we have computed a general error locator polynomial for the code C, the decoding algorithm is straightforward:

```
Input  s = $(s_1, \dots, s_{n-k})$
  $\mu = t$
While  $a_{t-\mu}(s_1, \dots, s_{n-k}) = 0$  do
  $\mu := \mu - 1$;
Output $\mu$, $L_e(z)$
```

Table 3: Orsini–Sala decoding algorithm

Example 6.4. *We consider the cyclic code of Example 5.5 with the $\mathcal{OS}$ syndrome ideal. The result is already relatively small*

$$\begin{array}{rcl} g_{331} & = & \mathbf{z_3^3} + z_3^2 x_1 + z_3(x_3 x_2^9 + x_3 x_2^8 x_1^3 + x_3 x_2^4 + x_3 x_2 x_1^9) + z_3(x_2^{15} x_1^2 + x_2^{14} x_1^5 + x_2^{13} x_1^8 \\ & + & x_2^{12} x_1^{11} + x_2^{11} x_1^{14}) + z_3(x_2^{10} x_1^2 + x_2^7 x_1^{11} + x_2^6 x_1^{14} + x_2^5 x_1^2 + x_2^3 x_1^8 + x_2^2 x_1^{11} + x_1^2) \\ & + & x_3 x_2^9 x_1 + x_3 x_2^8 x_1^4 + x_3 x_2^4 x_1 + x_3 x_2 x_1^{10} + x_2^{15} x_1^3 + x_2^{14} x_1^6 + x_2^{13} x_1^9 + x_2^{12} x_1^{12} \\ & + & x_2^{11} x_1^{15} + x_2^{10} x_1^3 + x_2^7 x_1^{12} + x_2^6 x_1^{15} + x_2^5 x_1^3 + x_2^3 x_1^9 + x_2^2 x_1^{12} + x_2 \end{array}$$

but clever guessing inspired by eye-inspection gives a more compact presentation

$$g_{331} = A^3 + AE + B$$

where $A := x_1 + z_3, \quad B := x_2 + x_1^3, \quad C := x_3 + x_1^5,$

$$D := x_2^8 + x_2^7 x_1^3 + x_2^3 + x_1^9, \quad E := x_1^2(B^{15} - 1) - C x_2 D.$$

The efficiency of this algorithm obviously depends on the sparsity of the general error locator polynomial. Even if at present there is no known theoretical proof of the sparsity of general error locator polynomials, there are some experimental evidence, at least in the binary case. In [17] and [16] it is shown that this algorithm may be applied efficiently to all binary cyclic code with $t \leq 2$ and length n less then 63, as we now detail. Recalling that the following trivial theorem holds for each binary cyclic codes with $t \leq 2$,

Theorem 6.5. *Let C be a code with $t = 1$ and $\mathbf{s}$ a correctable syndrome, then the general error locator polynomial is $\mathcal{L}_C(X, z) = z + a$, where $a \in \mathbb{F}_2[X]$. Moreover, there is one error if and only if $a(\mathbf{s}) \neq 0$ and in that case the error location is $a(\mathbf{s})$. Let C be a code with $t = 2$, $\mathbf{s}$ a correctable syndrome and $\bar{z}_1$ and $\bar{z}_2$ the error locations. Then $\mathcal{L}_C(X, z) = z^2 + az + b$, where $a, b \in \mathbb{F}_2[X]$, and $b(\mathbf{s}) = \bar{z}_1 \bar{z}_2$, $a(\mathbf{s}) = \bar{z}_1 + \bar{z}_2$. Moreover, there are two errors if and only if $b(\mathbf{s}) \neq 0$, and there is an error if and only if $b(\mathbf{s}) = 0$ and $a(\mathbf{s}) \neq 0$ (in this case the error location is $a(\mathbf{s})$).*

Let us now state the main theorems of [17]:

Theorem 6.6. *Let C be a binary $[n, k, d]$ code with $n \leq 61$ and $d = 3, 4$ $[t = 1]$. We denote by S a defining set of C and $\mathcal{L}_C \in \mathbb{F}_q[x_1, \ldots, x_{n-k}][z]$ a general error locator polynomial. Then there are only four cases:*

1) *C has a defining set of type $S = \{m\}$, with $(n, m) = 1$. Then there exixts an integer k modulo n such that $\mathcal{L}_C = z + x_1^k$.*

2) *C has a defining set of type $S = \{m, h\}$, with $(m, h) = 1$. Then there exist two integers m' and h' modulo n such that*

$$\mathcal{L}_C = z + x_1^{m'} x_2^{h'} .$$

3) C is a sub-code of a code C' of type 1) or 2) and $\mathcal{L}_C = \mathcal{L}_{C'}$.

4) C is equivalent to a code C' of type 1), 2) or 3) and $\mathcal{L}_C$ can be trivially obtained from $\mathcal{L}_{C'}$.

The following theorem shows an interesting property for a wide class of 2-error correcting codes.

Theorem 6.7. *Let C be a code with length $3 \leq n \leq 125 (n \neq 105)$ and distance $d = 5, 6$. Then C is equivalent to a code D s.t. $1 \in S_D$.*

From this it is easy to prove that if C is a binary $[n, k, d]$ code with $7 \leq n < 63$ (n odd) and $d = 5, 6$, then

$$\mathcal{L}_C = z^2 + x_1 z + b(x_1, \dots, x_{n-k}),$$

where $b(x_1, \dots, x_{n-k}) \subset \mathbb{F}_2[x_1, \dots, x_{n-k}]$.

Theorem 6.8. *Let C be a binary $[n, k, d]$-code with $7 \leq n < 63$ (n odd) and $d = 5, 6$, $[t = 2]$. Then there are seven cases:*

1. *n is such that the code with defining set $\{0, 1\}$ has distance $d \geq 5$;*
2. *C is a BCH code, i.e. $S_C = \{1, 3\}$ and*
$$b = x_1^{n-1}(x_1^3 + x_2);$$
3. *C admits a defining set $S_C = \{1, n-1, l\}$, with $l = 0, n/3$, and*
$$b = \begin{cases} x_1 x_2^{-1}(1 + x_3) & l = 0 \\ \frac{x_3^3+1}{x_1^{n/3} x_2^{2/3n} x_3+1} & l = n/3 \end{cases}$$
4. *C admits a defining set $S_C = \{1, n/l\}$, for some $l \geq 3$;*
5. *C is one of the following*
   - $n = 31$, $S_C = \{1, 15\}$;
   - $n = 31$, $S_C = \{1, 5\}$;
   - $n = 45$, $S_C = \{1, 21\}$;
   - $n = 51$, $S_C = \{1, 9\}$;
   - $n = 51$, $S_C = \{0, 1, 5\}$
6. *C is a sub-code of one of the codes of the above cases;*
7. *C is equivalent to one of the codes of the above cases.*

In all cases b is very short and in most cases a formula can be given.

7 A Newton-based decoder

A different approach based on Newton identities (3) has been recently proposed [3] (see also [2]): unlike [15], whose aim is to produce a single *general* locator, they follow the suggestion given by [6] (Remark 5.6) of splitting the computation according to the potential weights. Denote

$$\mathcal{F}_\mu^{(\hat\sigma)} := \left\{ \hat\sigma_j - (-1)^j \sum_{1 \le l_1 \le \cdots \le l_j \le \mu} z_{l_1} \cdots z_{l_j}, 1 \le j \le \mu \right\} \subset \mathbb{F}[\hat\sigma_1, \ldots, \hat\sigma_\mu, z_1, \ldots, z_\mu],$$

$$\mathcal{F}_\mu^{(X)} := \left\{ x_i - \textstyle\sum_{j=1}^{\mu} z_j^i, 1 \le i \le \mu + n \right\} \cup \{x_{i+n} - x_i, 1 \le i \le \mu\} \subset \mathbb{F}[X, z_1, \ldots, z_\mu],$$

$$\mathsf{I}_\mu \subset \mathbb{F}[\hat\sigma, X, Z] = \mathbb{F}[\hat\sigma_1, \ldots, \hat\sigma_\mu, x_1, \ldots, x_{\mu+n}, z_1, \ldots, z_\mu] := \mathcal{Q}$$

the ideal generated by $\mathcal{F}_\mu^{(\hat\sigma)} \cup \mathcal{F}_\mu^{(X)}$, $\Delta_\mu := \prod_{i=1}^{\mu} z_i \prod_{1 \le i < j \le \mu} (z_i - z_j)$ and[2] $\mathsf{I}_\mu^\infty = \{f \in \mathcal{Q} :$ exists $n \in \mathbb{N} : f\Delta_\mu^n \in \mathsf{I}_\mu\} \cap \mathbb{F}[\hat\sigma_1, \ldots, \hat\sigma_\mu, x_1, \ldots, x_{\mu+n}]$.

Fact 7.1. *[3] Denoting by G_μ the Gröbner basis of I_μ^∞ w.r.t. the lex ordering induced by $\hat\sigma_i < x_l, l \notin S_C$ and $\hat\sigma_i > x_l, l \in S_C$, $T_\mu := G_\mu \cap \mathbb{F}[x_l : l \in S_C]$, the following hold*

1. *I_μ^∞ is a radical 0-dimensional ideal;*
2. *its roots (σ_i, s_l) are exactly the values $\sigma_i = (-1)^j \sum_{1 \le l_1 \le \cdots \le l_j \le \mu} e_{l_1}$ and $s_l = \sum_{j=1}^{\mu} e_j^l$ where $e_1, \ldots, e_\mu$ run among the error locations of the words of weight exactly μ;*
3. *for each $i, 1 \le i \le \mu$ there are $p_{i\mu}, q_{i\mu} \in \mathbb{F}_q[x_l : l \in S_C]$ such that $p_{i\mu}\sigma_i - q_{i\mu} \in G_\mu$*
4. *for an error e and the corresponding syndromes $(s_l : l \in S_C)$ we have*
   - *the weight of e is μ if and only if $t(s_l) = 0$ for each $t \in T_\mu$*
   - *the corresponding error locator polynomial is $1 + \sum_{i=1}^{\mu} \frac{q_{i\mu}(s_l)}{p_{i\mu}(s_l)} z^i$* □

Thus the associated decoding algorithm consists in

1. (precomputation) For each weight μ compute the Gröbner basis G_μ of I_μ^∞ w.r.t the lex ordering induced by $\hat\sigma_i < x_l, l \notin S_C$ and $\hat\sigma_i > x_l, l \in S_C$,

[2] I_μ^∞ can be computed as $\mathsf{I}_\mu^\infty = \bar{\mathsf{I}}_\mu \cap \mathbb{F}[\hat\sigma_1, \ldots, \hat\sigma_\mu, x_1, \ldots, x_{\mu+n}]$ where $\bar{\mathsf{I}}_\mu \subset \mathcal{Q}[T]$ is the ideal generated by $\mathcal{F}_\mu^{(\hat\sigma)} \cup \mathcal{F}_\mu^{(X)} \cup \{1 - \Delta_\mu T\}$

2. (precomputation) For each μ and each i extract the polynomials $p_{i\mu}, q_{i\mu} \in \mathbb{F}[x_l : l \in S_C]$ such that $p_{i\mu}\sigma_i - q_{i\mu} \in G_\mu$

3. (precomputation) For each μ, identify the set $T_\mu := G_\mu \cap \mathbb{F}[x_l : l \in S_C]$

4. (on line) for any received word

   (a) compute the corresponding syndromes $(s_l : l \in S_C)$

   (b) evaluating $t(s_l), t \in T_\mu$, deduce μ

   (c) return $L_e(z) := 1 + \sum_{i=1}^{\mu} \frac{q_{i\mu}(s_l)}{p_{i\mu}(s_l)} z^i$

Remark 7.2. *Unfortunately, [3] avoid discussing the size of the data, thus preventing from to making a fair comparison with the results of [15]. Mainly on the basis of the results of [1] the gut feeling of the first author is that while [3] loses against [15] as regards space (μ diffierent error locator polynomials have necessarily to be stored) probably one should prefer [3] as regards time.*

The reader can in any case reach his own opinion comparing [15] data (Example 6.4) *with the best available approximation of [3] data, namely Remark* 5.6. □

8 Acknowledgements

Part of these results have been presented at Linz D1 2006, which was a workshop within the Special Semester on Groebner Bases, February–July 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

The second author would like to thank T. Mora and her supervisor M. Sala.

References

[1] Alonso M.E., Becker E., Roy M.-F., Wörmann T. *Zeroes, Multiplcicities and Idempotents for Zerodimensional Systems*, Progress in Mathematics **143** (1996), 1–16, Birkhäuser

[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] D. Augot, M. Betti, E. Orsini, Introducing to cylic code.

[5] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill (1968)

[6] M. Caboara, The Chen-Reed-Helleseth-Truong Decoding Algorithm and the Gianni-Kalkbrenner Gröbner Shape Theorem ,*J AAECC*, **13** (2002)

[7] 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. on Inf. Th.*, **40** (1994) , 1654–1661.

[8] X. Chen, I. S. Reed, T. Helleseth, K. Truong, General Principles for the Algebraic Decoding of Cyclic Codes, *IEEE Trans. on Inf. Th.*, **40** (1994) , 1661–1663.

[9] X. Chen, I. S. Reed, T. Helleseth, K. Truong, Algebraic decoding of cyclic codes: A polynomial Ideal Point of View, *Contemporary Mathematics*, **168** (1994), 15–22

[10] A.B. III Cooper, Direct solution of BCH decoding equations, In E. Arikan (Ed.) *Communication, Control and Singal Processing*, 281–286, Elsevier (1990)

[11] A.B. III Cooper, Finding BCH error locator polynomials in one step *Electronic Letters*, **27** (1991) 2090–2091

[12] P. Gianni, Properties of Gröbner bases under specialization, step *Lect. N. Comp. Sci.*, **378** 293–297, (1991)

[13] M. Kalkbrenner, Solving systems of algebraic equations using Gröbner bases, step *Lect. N. Comp. Sci.*, **378** 282–292, (1991)

[14] P. Loustaunau, E.V. York, On the decoding of cyclic codes using Gröbner bases,*J AAECC*, **8** (1997) 469–483.

[15] E. Orsini, M. Sala, Correcting errors and erasures via the syndrome variety, *J. Pure Appl. Algebra*, **200** (2005), 191–226.

[16] E. Orsini, M. Sala, General error locator polynomials for binary cyclic codes with $t \leq 2$ and $n < 63$, *IEEE Trans. Inform. Theory*, 53, 1095–1107, 2007.

[17] T. Mora E. Orsini, M. Sala, General error locator polynomials for binary cyclic codes with $t \leq 2$ and $n < 63$, *BCRI preprint*, 2005, available at `http://www.bcri.ucc.ie`.