Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Pure and Applied Algebra 200 (2005) 191–226

JOURNAL OF
PURE AND
APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Correcting errors and erasures via the syndrome variety

Emmanuela Orsini[a], Massimiliano Sala[b,*]

[a] *Department of Mathematics, University of Pisa, Italy*
[b] *Boole Centre for Research in Informatics, UCC Cork, Ireland*

Received 2 March 2004; received in revised form 15 October 2004
Available online 4 February 2005
Communicated by J. Walker

Abstract

We propose a new syndrome variety, which can be used to decode cyclic codes. We present also a generalization to erasure and error decoding. We can exhibit a polynomial whose roots give the error locations, once it has been specialized to a given syndrome. This polynomial has degree t in the variable corresponding to the error locations and its coefficients are polynomials in the syndromes.
© 2005 Elsevier B.V. All rights reserved.

MSC: 11T71; 12Y05

1. Introduction

Coding theory is one of the main research areas where algebraic tools can be applied to industrial problems. Cyclic codes are a class of error correcting codes which have been widely studied in the last fifty years [2,16,19]. While it is relatively simple to study their internal properties (distance, weight distribution, etc.) to some useful extent, no efficient decoding algorithm is known.

BCH codes form an interesting sub-class of cyclic codes: their internal properties are well known and very efficient decoding procedures exist [9].

[*] Corresponding author.
E-mail addresses: orsini@posso.dm.unipi.it (E. Orsini), msala@bcri.ucc.ie (M. Sala).

0022-4049/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2004.12.027

This is why BCH codes have been one of the “de facto” standards in industrial applications. Unfortunately, long BCH codes are known to have unsatisfactory properties (see [14]). Cyclic codes are not known to suffer from this limitation. What we need for cyclic codes is a good decoding procedure.

In some papers [3,6,7,15], the authors have proposed a decoding procedure for cyclic codes which relies on the computation of the lexicographical Gröbner basis of a suitable ideal. The corresponding variety is known as the CRHT syndrome variety. We are going to show in this paper some related results:

(1) the CRHT syndrome variety has certain drawbacks and so we propose a modified syndrome variety which contains exactly the solutions we are seeking,
(2) we show how our syndrome variety gives rise to an improved decoding algorithm,
(3) we extend our ideas to the simultaneous correction of erasures and errors (although some special cases have been studied by others),
(4) we show that each cyclic code possesses a general error locator polynomial, i.e. a polynomial which contains the error location once it has been specialized to a given syndrome; moreover, we show the existence of similar polynomials for the case of simultaneous correction of errors and erasures.

Probably, the existence of general error locator polynomials for each cyclic code is our main result and we plan future work where these polynomials will be deeply studied. An investigation on the complexity of their computation and on practical decoding via their properties can be found in [4]. It is interesting to note that the existence of general error locator polynomials is not guaranteed for a generic linear code, as shown in [22]. The determination of classes of codes admitting general error locator polynomials is an open and stimulating problem.

In [1], a variant of the CRHT variety has been used to get a heuristic decoding of some binary cyclic codes, also with medium length (up to $n=512$), which turns out to be relatively fast. It may be possible that similar methods can be adapted to our case, with possibly even more effect.

There has been some research on exploiting a variant of the CRHT variety to get internal properties of cyclic codes and their shortened codes (see [21,20]). Some of the techniques employed there (e.g., the use of the polynomial p, Definition 6.1) have been adapted to our case.

This paper is organized as follows:

In Section 2 notation and preliminaries are given. In Section 3 we illustrate the concept of general error locator polynomials. In Section 4 we recall the CRHT syndrome variety and we recall how knowledge of its structure can be used to decode cyclic codes. We study the general structure of some ideals we are going to use in Section 5. We are particularly interested in investigating how the structure of the underlying variety restricts the shape of the Gröbner basis of the ideal. In Section 6, we propose a new syndrome variety and describe the structure of the reduced Gröbner basis of the associated ideal; from this basis it is trivial to obtain the general error locator polynomial of the cyclic code, showing its existence. We extend our syndrome variety to the case when there are also erasures in Section 7. We can prove a similar structure for the reduced Gröbner basis of the corresponding ideal and so we can exhibit for any cyclic code the general error locator polynomials of any type. In Section 8 we show how to use the general error locator polynomial in order to decode a cyclic code, providing also a comparison to Caboara and Mora's algorithm; we show also how to use general locator polynomials of any type in order to decode simultaneously errors and erasures; we provide some examples. We pose some remarks on complexity issues related both to the computation of the general error locator polynomial and to its actual use in Section 9. In Section 10, some possible further work is discussed. In appendix, we prove a technical result which is needed to show the structure of the Gröbner basis of our ideals (and this will open the path to the determination of the general error locator polynomials).

2. Notation and preliminaries

In this section we recall some basic facts about cyclic codes and Gröbner bases that will be used in the remainder of the paper.

2.1. Cyclic codes

Let C be an $[n,k,d]$ cyclic code on a field $\mathbb{F}_q$ with $(q,n)=1$. Let g be the *generator polynomial* of the code C, that is, g is a polynomial of degree $r=n-k$ such that

$$C=\{c(x)\in\mathbb{F}_q[x]\mid c(x)=a(x)g(x)\text{ for some }a(x)\text{ with }deg(a(x))<k\}.$$

We denote by $\mathbb{F}=\mathbb{F}_{q^m}$ the splitting field of x^n-1 over $\mathbb{F}_q$ and by α a *primitive* n*th root of unity*, i.e. $\alpha\in\mathbb{F}$ is such that its powers generate all roots of x^n-1:

$$x^n-1=\prod_{i=0}^{n-1}(x-\alpha^i).$$

As g divides x^n-1, its roots are all distinct and form a subset of the roots of x^n-1. Traditionally we define S_C to be the set

$$S_C=\{i\mid g(\alpha^i)=0\},$$

which is called the *complete defining set* of C. As S_C is partitioned into cyclotomic classes, there are some subsets S of S_C, any of them sufficient to specify the code unambiguously and any such S is called a *defining set*.

It is known that we can view C as the $\mathbb{F}_q$-kernel of the parity-check matrix H (with entries in $\mathbb{F}$):

$$H=\begin{pmatrix}1 & \alpha^{i_1} & \alpha^{2i_1} & \cdots & \alpha^{(n-1)i_1}\\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \cdots & \alpha^{(n-1)i_2}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \alpha^{i_r} & \alpha^{2i_r} & \cdots & \alpha^{(n-1)i_r}\end{pmatrix}$$

We can consider the error vector **e** as a polynomial:

$$e(x) = \sum_{l=1}^{\mu} a_l x^{k_l} \in \mathbb{F}_q[x],$$

where the weight μ satisfies $\mu \leqslant t = [(d-1)/2]$ and the magnitudes and locations of this error pattern are, respectively, $\{a_1, \ldots, a_\mu\}$ and $\{k_1, \ldots, k_\mu\}$, with $a_i \in \mathbb{F}_q$ and $0 \leqslant k_1 < k_2 < \cdots < k_\mu \leqslant n-1$.

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

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

Remark 2.1. Traditionally, the reciprocal of $L(z)$, with roots the inverses $(\alpha^{k_l})^{-1}$, is used as the error locator polynomial. This change of notation is convenient to us.

Let $\mathbf{c} = (c_0, \ldots, c_{n-1})$, $\mathbf{v} = (v_0, \ldots, v_{n-1})$ and $\mathbf{e} = (e_0, \ldots, e_{n-1})$ be, respectively, the transmitted codeword, the received vector and the error vector. If we apply the parity-check matrix H to $\mathbf{v}$, we get

$$H\mathbf{v}^{\mathbf{T}} = H(\mathbf{c}^{\mathbf{T}} + \mathbf{e}^{\mathbf{T}}) = H\mathbf{c}^{\mathbf{T}} + H\mathbf{e}^{\mathbf{T}} = 0 + H\mathbf{e}^{\mathbf{T}} = \mathbf{s}^{\mathbf{T}}$$

where the r-vector $\mathbf{s} = (s_1, \ldots, s_r)$ is called the *syndrome vector* associated to $\mathbf{v}$ (and its entries s_j are called *syndromes*).

The syndromes depend only on the error pattern and two syndromes corresponding to two different errors with weight $\mu \leqslant t$ are necessarily distinct. If no errors occurred in the transmission then $\mathbf{s} = 0$; otherwise if $\mathbf{e} = (\underbrace{0, \ldots, 0}_{k_1-1}, \underset{\substack{\uparrow \\ k_1}}{a_1}, 0, \ldots, 0, \underset{\substack{\uparrow \\ k_l}}{a_l}, 0, \ldots, 0, \underset{\substack{\uparrow \\ k_\mu}}{a_\mu}, \underbrace{0, \ldots, 0}_{n-1-k_\mu})$, we have

$$s_j = H_j \mathbf{v}^{\mathbf{T}} = \sum_{\tilde{l}=0}^{n-1} v_{\tilde{l}} (\alpha^{i_j})^{\tilde{l}} = H_j \mathbf{e}^{\mathbf{T}} = \sum_{l=1}^{\mu} a_l (\alpha^{i_j})^{k_l}, \quad j = 1, \ldots, r.$$

While an error occurs when a symbol in a transmitted word is changed, an *erasure* occurs when the decoder cannot understand a symbol at a certain position (but the position is known). For example, if the binary block $(1, 1, 1, 1)$ suffers from an error in the last component, it becomes the block $(1, 1, 1, 0)$. If the same block, $(1, 1, 1, 1)$, suffers from an erasure in the last component, it becomes $(1, 1, 1, x)$, where 'x' means that the value is unknown.

Let d be the distance of C. We know that the correction capability of the code is $t = [1/2(d-1)]$; in case there are also some erasures, denoting by v the numbers of erasures and by τ the numbers of errors that the code can simultaneously correct, we have

$$2\tau + v < d.$$

We denote the erasure locations by $\{h_1, \ldots, h_v\}$, $0 \leqslant h_1 \leqslant \cdots \leqslant h_v \leqslant n-1$, and retain our notation for errors. Note that $\{h_1, \ldots, h_v\} \cap \{k_1, \ldots, k_\mu\} = \emptyset$.

We define:

1. the vector $\overline{\mathbf{v}} = (\overline{v}_0, \ldots, \overline{v}_{n-1})$ s.t. $\forall i$ we have
$$\overline{v}_i = \begin{cases} v_i & \text{if } i \neq h_j, \ \forall 1 \leqslant j \leqslant v, \\ 0 & \text{otherwise}, \end{cases}$$
2. the vector $\overline{\mathbf{e}} = (\overline{e}_0, \ldots, \overline{e}_{n-1})$ s.t.
$$\overline{e}_i = \begin{cases} e_i & \text{if } i \neq h_j, \forall\ 1 \leqslant j \leqslant v, \\ 0 & \text{otherwise}, \end{cases}$$
3. the vector $\overline{\mathbf{c}} = (\overline{c}_0, \ldots, \overline{c}_{n-1})$ s.t.
$$\overline{c}_i = \begin{cases} c_i & \text{if } i = h_j, \ \forall 1 \leqslant j \leqslant v, \\ 0 & \text{otherwise}. \end{cases}$$

Remark 2.2. While $\overline{\mathbf{v}}$ and $\overline{\mathbf{e}}$ may have non-zero components only in the coordinates different from erasure positions, $\overline{\mathbf{c}}$ may have non-zero components only in the coordinates corresponding to erasure positions.

4. the *truncated syndrome* $\overline{\mathbf{s}} = H\overline{\mathbf{v}}$:
$$\overline{s}_j = \sum_{\tilde{l}=0}^{n-1} \overline{v}_{\tilde{l}} (\alpha^{i_j})^{\tilde{l}} = \sum_{\tilde{l} \in \{0,\ldots,n-1\} \setminus \{h_1,\ldots,h_v\}} v_{\tilde{l}} (\alpha^{i_j})^{\tilde{l}}, \quad j = 1, \ldots, r.$$

Remark 2.3. Note that $\mathbf{c} = \overline{\mathbf{v}} - \overline{\mathbf{e}} + \overline{\mathbf{c}}$, because $\overline{\mathbf{v}} - \overline{\mathbf{e}}$ is the transmitted word restricted to the components $\{0, \ldots, n-1\} \setminus \{h_1, \ldots, h_v\}$ and $\overline{\mathbf{c}}$ is the transmitted word restricted to the other components $\{h_1, \ldots, h_v\}$.

We have $H(\overline{\mathbf{v}} - \overline{\mathbf{e}} + \overline{\mathbf{c}}) = H\mathbf{c} = 0$ and, in case of successful decoding, we can write
$$\overline{s}_j - \sum_{l=1}^{\mu} a_l (\alpha^{i_j})^{k_l} + \sum_{\overline{l}=1}^{v} \overline{c}_{h_{\overline{l}}} (\alpha^{i_j})^{h_{\overline{l}}} = 0, \quad 1 \leqslant j \leqslant r,$$
i.e.
$$\overline{s}_j - \sum_{l=1}^{\mu} a_l (\alpha^{i_j})^{k_l} + \sum_{\overline{l}=1}^{v} c_{h_{\overline{l}}} (\alpha^{i_j})^{h_{\overline{l}}} = 0, \quad 1 \leqslant j \leqslant r. \tag{1}$$

2.2. Polynomials

Let $K[T] = K[T_1, \ldots, T_n]$ be a polynomial ring with coefficients in the field K.

Definition 2.4. For any term-ordering $>$ on $K[T]$ and any polynomial f in $K[T]$, $f = \sum_\alpha a_\alpha T^\alpha$, with $deg(f) = \max_>\{\alpha \in \mathbb{N} \mid a_\alpha \neq 0\}$, we define:

$$Lt(f) = T^{deg(f)}, \text{ the leading term of } f.$$

If we consider the lexicographical ordering such that $T_1 > \cdots > T_n$, each element $f \in K[T_1, \ldots, T_n]$ can be viewed uniquely as a univariate polynomial in the variable T_1 with coefficients in the polynomial ring $K[T_2, \ldots, T_n]$:

$$f = b_h(T_2, \ldots, T_n)T_1^h + b_{h-1}(T_2, \ldots, T_n)T_1^{h-1} + \cdots + b_0(T_2, \ldots, T_n),$$

where we will denote by $Lp(f) = b_h(T_2, \ldots, T_n)$ the ($\mathbf{T_1}$) *leading polynomial* and by $Tp(f) = b_0(T_2, \ldots, T_n)$ the ($\mathbf{T_1}$) *trailing polynomial* of f.

Let I be an ideal in $K[T_1, \ldots, T_n]$. We denote by $\overline{K}$ the algebraic closure of K. Let $S \subset \overline{K}^n$. We denote by

$$\mathscr{V}(I) = \{(\alpha_1, \ldots, \alpha_n) \in \overline{K}^n \mid f(\alpha_1, \ldots, \alpha_n) = 0, \ \forall f \in I\},$$

the set of all the roots of I and by $\mathscr{I}(S)$ the ideal formed by the polynomials in $K[T_1, \ldots, T_n]$ vanishing on S.

Definition 2.5. Let I be an ideal in $K[T_1, \ldots, T_n]$. The l*th elimination ideal* I_l is the ideal of $K[T_{l+1}, \ldots, T_n]$ defined by $I_l = I \cap K[T_{l+1}, \ldots, T_n]$.

Let τ, ν and r be positive natural numbers.

Let $I \subset \mathbb{F}_q[X, W, Z, U, Y]$ be an ideal, with $X = (x_1, \ldots, x_r)$, $W = (w_1, \ldots, w_\nu)$, $Z = (z_\tau, \ldots, z_1)$, $U = (u_\nu, \ldots, u_1)$, $Y = (y_1, \ldots, y_\tau)$. Let G be a subset of I. We will use the following notation:

$$\begin{aligned}
&\mathscr{P}_X = \mathbb{F}_q[X], I_X = I \cap \mathscr{P}_X, \ \ G_X = G \cap \mathscr{P}_X,\\
&\mathscr{P}_{XW} = \mathbb{F}_q[X, W] \backslash \mathbb{F}_q[X], I_{XW} = I \cap \mathscr{P}_{XW}, G_{XW} = G \cap \mathscr{P}_{XW},\\
&\mathscr{P}_{XWZ} = \mathbb{F}_q[X, W, Z] \backslash \mathbb{F}_q[X, W], I_{XWZ} = I \cap \mathscr{P}_{XWZ}, G_{XWZ} = G \cap \mathscr{P}_{XWZ},\\
&\mathscr{P}_{XWZU} = \mathbb{F}_q[X, W, Z, U] \backslash \mathbb{F}_q[X, W, Z], \ \ I_{XWZU} = I \cap \mathscr{P}_{XWZU},\\
&G_{XWZU} = G \cap \mathscr{P}_{XWZU},\\
&\mathscr{P}_{XWZUY} = \mathbb{F}_q[X, W, Z, U, Y] \backslash \mathbb{F}_q[X, W, Z, U], \ \ I_{XWZUY} = I \cap \mathscr{P}_{XWZUY},\\
&G_{XWZUY} = G \cap \mathscr{P}_{XWZUY}.
\end{aligned}$$

Observe that $I = I_X \sqcup I_{XW} \sqcup I_{XWZ} \sqcup I_{XWZU} \sqcup I_{XWZUY}$ and that $G = G_X \sqcup G_{XW} \sqcup G_{XWZ} \sqcup G_{XWZU} \sqcup G_{XWZUY}$ ($\sqcup$ denotes disjoint union).

Remark 2.6. We extend our notation to the case $\nu = 0$, meaning that the variable sets W and U are void, e.g. $\mathscr{P}_{XWZ} = \mathscr{P}_{XZ} = \mathbb{F}_q[X, Z] \backslash \mathbb{F}_q[X]$.

When convenient, we enclose the ideal name within brackets, e.g. $(I)_X = I_X$.

Assume G is a Gröbner basis for an ideal $I \subset K[S, Z, T]$, $S = (s_1, \ldots, s_H)$, $Z = (z_1, \ldots, z_L)$, $T = (t_1, \ldots, t_M)$ w.r.t. a block order with $S < Z < T$ and with the Z-variables lexicographically ordered by $z_1 > z_2 > \cdots > z_L$. Then the elements of $G \cap (K[S, Z] \backslash K[S])$ can be collected in blocks $\{G_i\}_{1 \leqslant i \leqslant L}$:

$$\begin{aligned} G_1 &= \{g_{1,1}(S, z_L, \ldots, z_1), \ldots, g_{1,l_1}(S, z_L, \ldots, z_1)\}, \\ G_2 &= \{g_{2,1}(S, z_L, \ldots, z_2), \ldots, g_{2,l_2}(S, z_L, \ldots, z_2)\}, \\ &\vdots \\ G_L &= \{g_{L,1}(S, z_L), \ldots, g_{L,l_L}(S, z_L)\}, \end{aligned}$$

in such a way that:

- for each i, $G_i \subset K[S, z_L, \ldots, z_{i+1}][z_i] \backslash K[S, z_L, \ldots, z_{i+1}]$,
- the ideal generated by $\bigsqcup_{j>i} G_j$ is the ith elimination ideal I_i.

Clearly each G_i, $1 \leqslant i \leqslant L$, can be decomposed into blocks of polynomials according to their degree with respect to the variable z_i:

$$G_i = \bigcup_{\delta=1}^{\Delta_i} G_{i\delta}.$$

In this way, if $g \in G_{i\delta}$, we have

- $g \in K[S, z_L, \ldots, z_{i+1}][z_i] \backslash K[S, z_L, \ldots, z_{i+1}]$,
- $deg_{z_i}(g) = \delta$, i.e. $g = az_i^\delta + \cdots$ and $a = Lp(g) \in K[S, z_L, \ldots, z_{i+1}]$.

Let $N_{i\delta}$ be the number of elements of $G_{i\delta}$. We name the elements of the set $G_{i\delta} = \{g_{i\delta j}, 1 \leqslant j \leqslant N_{i\delta}\}$ after their order:

$$h < j \Leftrightarrow Lt(g_{i\delta h}) < Lt(g_{i\delta j}).$$

Remark 2.7. We can summarize our description.

Given any two polynomials $g_{lDh} \in G_{lD}$ and $g_{i\delta j} \in G_{i\delta}$, then

$$g_{lDh} < g_{i\delta j} \Leftrightarrow Lt(g_{lDh}) < Lt(g_{i\delta j}) \Leftrightarrow \begin{cases} l > i \;\; or \\ l = i, \;\; D < \delta \;\; or \\ l = i, \;\; D = \delta, h < j. \end{cases} \tag{2}$$

3. General error locator polynomial

Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and $t = [(d-1)/2]$ its correction capability. Let v and τ be two natural numbers such that $2\tau + v < d$, so that C can correct simultaneously v erasures and τ errors. We assume the condition $(n, q) = 1$, which is helpful in defining the notion of *error location* (for a discussion see Section 10).

Let H be one of its parity check matrices. We restrict H to lie in $\mathbb{F}$, the splitting field of $x^n - 1$ over $\mathbb{F}_q$ (for a discussion see Section 10). So the syndromes will lie in $(\mathbb{F})^r$ (with $r \leqslant n - k$) and they will form a vector space of dimension $(n - k)$ over $\mathbb{F}_q$. Let α be a primitive nth root of unity in $\mathbb{F}$.

Definition 3.1. Let $\mathscr{L}_C$ a polynomial in $\mathbb{F}_q[X, z]$, where $X = (x_1, \dots, x_r)$. Then $\mathscr{L}_C$ is a *general error locator polynomial* of C if

(1) $\mathscr{L}_C(X, z) = z^t + a_{t-1}z^{t-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[X]$, $0 \leqslant j \leqslant t-1$, that is, $\mathscr{L}_C$ is a polynomial with degree t with respect to the variable z and its coefficients are in $\mathbb{F}_q[X]$;

(2) given a syndrome $\mathbf{s} = (\bar{s}_1, \dots, \bar{s}_r) \in (\mathbb{F})^{n-k}$, corresponding to an error of weight $\mu \leqslant t$ and error locations $\{k_1, \dots, k_\mu\}$, if we evaluate the X variables in $\mathbf{s}$, then the roots of $\mathscr{L}_C(\mathbf{s}, z)$ are exactly $\{\alpha^{k_1}, \dots, \alpha^{k_\mu}, \underbrace{0, \dots, 0}_{t-\mu}\}$.

Given a generic linear code C, the existence of a polynomial $\mathscr{L}_C$ is not guaranteed and there are examples of linear codes not admitting $\mathscr{L}_C$ (see [22]).

Actually, general error locator polynomials are known only for very simple codes and we recall the case of the binary narrow-sense primitive BCH with $t = 1$ in the following example.

Example 3.2. Let $m \geqslant 2$ be an integer. We can consider the binary cyclic code B, such that $n = 2^m - 1$ and $S_B = \{1, 2\}$. The BCH bound ensures that $3 = \delta \leqslant d$. It is a well-known fact that in this case $d = \delta = 3$ (as $3 = 2^2 - 1$). So B can correct 1 error.

For this code the following equation holds (Section 4)

$$z_1 = x_1$$

where z_1 represents the location of the error (or 0, if no error occurred) and x_1 is the first syndrome. So we have a polynomial in the z variable

$$P(z) = z - x_1$$

with coefficients in the syndromes, leading coefficient 1 and such that its root is:

- either the location of the error, if one error occurred,
- or 0, if no error occurred,

which is exactly what we want from a general error locator polynomial for B, and so $\mathscr{L}_B = P(z)$.

One of our main results is Theorem 6.9, which states

`Every cyclic code admits a general error locator polynomial`

We can extend Definition 3.1 to the case when there are also erasures.

Definition 3.3. Let $\mathscr{L}$ a polynomial in $\mathbb{F}_q[X, W, z]$, $X = (x_1, \dots, x_r)$ and $W = (w_\nu, \dots, w_1)$, where ν is the number of erasures that occurred. Then $\mathscr{L}$ is a *general error locator polynomial of type* ν of C if and only if

(1) $\mathscr{L}(X, W, z) = z^\tau + a_{\tau-1}z^{\tau-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[X, W]$, $0 \leqslant j \leqslant \tau - 1$, that is $\mathscr{L}$ is a polynomial with degree τ in the variable z and coefficients in $\mathbb{F}_q[X, W]$;

(2) for any syndrome $\mathbf{s}=(\bar{s}_1,\ldots,\bar{s}_r)$ and any erasures $\mathbf{w}=(\overline{w}_v,\ldots,\overline{w}_1)$, corresponding to an error of weight $\mu\leqslant t$ and error locations $\{k_1,\ldots,k_\mu\}$, if we evaluate the X variables in $\mathbf{s}$ and the W variables in $\mathbf{w}$, then the roots of $\mathscr{L}(\mathbf{s},\mathbf{w},z)$ are $\{\alpha^{k_1},\ldots,\alpha^{k_\mu},\underbrace{0,\ldots,0}_{\tau-\mu}\}$.

If such $\mathscr{L}$ exists for a given code C, then we name the polynomial $\mathscr{L}_C^v$.

To be consistent with our notation, we refer to $\mathscr{L}_C$ also as to a *general locator polynomial of type* 0, where clearly $\mathscr{L}_C=\mathscr{L}_C^0$.

For a code C, the possession of a general locator polynomial $\mathscr{L}_C^v$ of type v for all $0\leqslant v<d$ is clearly a stronger condition then the possession of a general error locator polynomial $\mathscr{L}_C$, but in Section 7 we prove one of our main results, Theorem 7.7, which states

`Every cyclic code admits a general locator polynomial of type` v, `for` $0\leqslant v<d$.

4. CRHT syndrome variety

In [6] Chen et al. proposed an algorithm for error decoding of cyclic codes starting from the Gröbner basis of a suitable ideal. In this section we describe the structure of the ideal and of the underlying variety, using the improvements due to Caboara and Mora [3]. Although no original results are presented here, we give some insights in Remark 4.2 and Remark 4.3, which will be the starting point of our subsequent construction.

Let C be an $[n,k,d]$ cyclic code with parameters following our previous notation (e.g. d is the code distance).

Definition 4.1. We call *correctable syndromes* the syndrome vectors $\mathbf{s}\in\mathbb{F}^r$ corresponding to errors with weight $\mu\leqslant t$. And we denote by $\Sigma_C\subset\mathbb{F}^r$ the set of all correctable syndromes associated to the code C.

Suppose there are exactly μ errors. We want to express the solutions of the equations:

$$\sum_{l=1}^{\mu} a_l(\alpha^{i_j})^{k_l}-s_j=0,\quad 1\leqslant j\leqslant r,\tag{3}$$

where $\{a_l\}$ and $\{k_l\}$ are unknown, as points in a variety defined by multivariate polynomials. The solutions of (3) are of the form

$$(k_1,\ldots,k_\mu,a_1,\ldots,a_\mu)$$

and are in $\{0,\ldots,n-1\}^\mu\times\mathbb{F}_q^\mu$. Observe that this solution set is not naturally endowed with any algebraic structure. Unfortunately we do not know μ, we know only that $\mu\leqslant t$. For this reason we consider an equation:

$$\sum_{l=1}^{t} a_l(\alpha^{i_j})^{k_l}-s_j=0,\quad 1\leqslant j\leqslant r,\tag{4}$$

such that it is satisfied by the solutions of all equations of kind (3), for all $0 \leqslant \mu \leqslant t$. To ensure this, we choose a symbol k and from now on we set by definition that $\beta^{\mathsf{k}} = 0$, $\forall \beta \in \mathbb{F}$. Using this notation, we can view the solutions of (4) as lying in the space $\{0, \ldots, n-1, \mathsf{k}\}^t \times \mathbb{F}_q^t$. Again, this solutions set is not naturally endowed with any algebraic structure, it is just a set.

If we take a solution of (3), say $(k_1, \ldots, k_\mu, a_1, \ldots, a_\mu)$, we can extend it to a solution of (4) as follows:

$$(k_1, \ldots, k_\mu, a_1, \ldots, a_\mu) \longmapsto (k_1, \ldots, k_\mu, \underbrace{\mathsf{k}, \ldots, \mathsf{k}}_{t-\mu}, a_1, \ldots, a_\mu, \underbrace{*, \ldots, *}_{t-\mu})$$

where $*$ stands for any non-zero element of $\mathbb{F}_q$. This way, to any solutions of (3), we can associate $(q-1)^t$ solutions of (4). These extended solutions will be called *direct extensions*.

Remark 4.2. There are some solutions of (4), which come from solutions of (3), but which are not their direct extensions. For example, if there are $t-2$ errors ($\mu = t-2$) and $(k_1, \ldots, k_\mu, a_1, \ldots, a_\mu)$ is a solution of (3), then, for any $a \in \mathbb{F}_q$ and $b \in \mathbb{F}$, $(k_1, \ldots, k_\mu, b, b, a_1, \ldots, a_\mu, a, -a)$ is a solution of (4), as $a(\alpha^{i_j})^b - a(\alpha^{i_j})^b = 0$.

We introduce the variables $X = (x_1, \ldots, x_r)$, $Z = (z_t, \ldots, z_1)$ and $Y = (y_1, \ldots, y_t)$, with the following meaning:

x_j stands for the syndrome s_j, $1 \leqslant j \leqslant r$,

$$z_l \text{ stands for } \begin{cases} \text{the error location } \alpha^{k_l} & \text{if } 1 \leqslant l \leqslant \mu, \\ 0 & \text{if } \mu < l \leqslant t, \end{cases}$$

$$y_l \text{ stands for } \begin{cases} \text{the error magnitude } a_l & \text{if } 1 \leqslant l \leqslant \mu, \\ \text{any non-zero element of } \mathbb{F} & \text{if } \mu < l \leqslant t. \end{cases}$$

Using this notation, we can now rewrite the equations (3) and (4) in terms of the variables X, Z and Y:

$$\tilde{f}_j : \sum_{l=1}^{\mu} y_l z_l^{i_j} - x_j = 0, \quad 1 \leqslant j \leqslant r, \tag{5}$$

$$f_j : \sum_{l=1}^{t} y_l z_l^{i_j} - x_j = 0, \quad 1 \leqslant j \leqslant r. \tag{6}$$

We can add other equations to specify the range of values that can be assigned to our variables:

$\sigma_j : x_j^{q^m} - x_j = 0,\ 1 \leqslant j \leqslant r,$ since $s_j \in \mathbb{F}$;

$\eta_i : z_i^{n+1} - z_i = 0,\ 1 \leqslant i \leqslant t,$ since $(\alpha^{i_j})^{k_l}$ are either nth roots of unity or zero;

$\lambda_i : y_i^{q-1} - 1 = 0,\ 1 \leqslant i \leqslant t,$ since $a_l \in \mathbb{F}_q \backslash \{0\}$;

Then we obtain the following polynomial equation system:

$$\mathscr{F}_C = \{f_j, \sigma_j, \eta_i, \lambda_i : 1 \leqslant j \leqslant r, 1 \leqslant i \leqslant t\} \subset \mathbb{F}_q[X, Z, Y].$$

The ideal I_C generated by $\mathscr{F}_C$ is the *CRHT-syndrome ideal* associated to the code C and it is easy to see that it is a zero-dimensional ideal. The variety $V(\mathscr{F}_C)$ defined by $\mathscr{F}_C$ is the *CRHT-syndrome variety* and clearly we have $V(\mathscr{F}_C) = V(I_C)$.

Remark 4.3. For every given correctable syndrome $\mathbf{s} \in \Sigma_C$, there are some points in $V(\mathscr{F}_C)$ that determine the error locations and the error values, but in $V(\mathscr{F}_C)$ there are also other points that do not correspond directly to error vectors. In fact, there are points of type

$$(z_1, \ldots, z_\mu, \underbrace{0, \ldots, 0}_{t-\mu}, y_1, \ldots, y_\mu, \mathsf{y}_1, \ldots, \mathsf{y}_{t-\mu}),$$

with y_j an arbitrary element in $\mathbb{F}_q$ for any j, that clearly correspond to direct extensions of $(z_1, \ldots, z_\mu, y_1, \ldots, y_\mu)$ and these points are the points considered in [3,6,15]. But, if $\mu \leqslant t-2$, there are also some points in $V(\mathscr{F}_C)$ not corresponding to direct extensions:

$$(z_1, \ldots, z_\mu, z, z, \underbrace{0, \ldots, 0}_{t-(\mu+2)}, y_1, \ldots, y_\mu, \mathsf{y}_1, \ldots, \mathsf{y}_{t-\mu}),$$

with z any nth root of unity and the other components as above.

Remark 4.4. The role of the polynomials $\sigma_j, \eta_i, \lambda_i$ is noteworthy. They remove all the roots that are in algebraic extensions outside $\mathbb{F}$ and moreover they make the other roots simple. That is, I_C is a radical ideal and

$$V(\mathscr{F}_C) \subset \mathbb{F}^r \times \mathbb{F}^t \times (\mathbb{F}_q)^t.$$

If we calculate the Gröbner basis G_C of the ideal I_C, w.r.t. the lexicographical order induced by

$$x_1 < x_2 < \cdots < x_r < z_t < \cdots < z_1 < y_1 < \cdots < y_t,$$

the Gianni–Kalkbrenner Gröbner Shape Theorem (cf. [12,13]) gives us information on the structure of G_C, as proved in [3]:

Theorem 4.5 (*Caboara and Mora [3]*). *Let G be the reduced Gröbner basis of the CRHT-syndrome ideal I_C w.r.t. the lexicographical order induced by*

$$x_1 < x_2 < \cdots < x_r < z_t < \cdots < z_1 < y_1 < \cdots < y_t.$$

Then G has the following structure:

1. $G = G_X \sqcup G_{XZ} \sqcup G_{XZY}$ *with* $G_{XZ} = \bigcup_{i=1}^{t} G_i, G_i \subset \mathscr{P}_X[z_t, \ldots, z_{i+1}][z_i] \backslash \mathscr{P}_X[z_t, \ldots, z_{i+1}]$ *and*

$$G_i = \bigcup_{\delta=1}^{\Delta_i} G_{i\delta}.$$

2. *for each i, if we evaluate the polynomials of G_i in $(s_1, \dots, s_r, \underbrace{0, \dots, 0}_{t-i})$, let $\mathbf{g_i} \in G_{i\delta}$ be the first polynomial s.t.*

$$Lp(\mathbf{g_i})(s_1, \dots, s_r, 0, \dots, 0) \neq 0$$

i.e.

- $Lp(g)(s_1, \dots, s_r, 0, \dots, 0) = 0, \;\; \forall g \in G_{iD}, \;\; D < \delta$;
- *for each* $\overline{g} \in G_{i\delta}$ *such that* $Lt(\overline{g}) < Lt(\mathbf{g_i})$ (*cf. Remark* (2.7)) *we have*

$$Lp(\overline{g})(s_1, \dots, s_r, 0, \dots, 0) = 0.$$

2. *Then*:

(2.1) $g(s_1, \dots, s_r, z_i, 0, \dots, 0) \equiv 0, \;\; \forall g \in G_{iD}, \;\; Lt(g) < Lt(\mathbf{g_i})$;
(2.2) $\mathbf{g_i}(s_1, \dots, s_r, z_i, 0, \dots, 0) \not\equiv 0$;
(2.3) *for each* $\tilde{g} \in G_{iD}$ *s.t.* $Lt(\mathbf{g_i}) < Lt(\tilde{g})$

$$\mathbf{g_i}(s_1, \dots, s_r, z_i, 0, \dots, 0) \mid \tilde{g}(s_1, \dots, s_r, z_i, 0, \dots, 0);$$

3. *if we suppose that there are at most* $\mu \leqslant t$ *errors, we could have the following cases*:

(3.1) *either*

$$Lp(g)(s_1, \dots, s_r, 0, \dots, 0) = 0 \quad \forall g \in G_{\mu\mu},$$

then:

(a) $g(s_1, \dots, s_r, z_\mu, 0, \dots, 0) \equiv 0, \;\; \forall g \in G_{\mu\mu}$;
(b) *there are at most* $\mu - 1$ *errors*;

(3.2) *or*

$$\exists g \in G_{\mu\mu} \; s.t. \; Lp(g)(s_1, \dots, s_r, 0, \dots, 0) \neq 0,$$

then if:

$$Tp(g)(s_1, \dots, s_r, 0, \dots, 0) \neq 0 :$$

(c) *there are* μ *errors*;
(d) $L(z) = g(s_1, \dots, s_r, 0, \dots, 0, z)$;

$$else$$

(e) *there are at most* $\mu - 1$ *errors*.

Proof. For a proof we refer to [3,12,13,15]. □

From this theorem it is clear how to proceed to get the error locations from a given correctable syndrome $\mathbf{s}$. It is enough to evaluate the polynomials of $G_{\mu\mu}$ in $\mathbf{s}$ for each μ, until we find one which does not vanish. This will be the error locator polynomial. The exact algorithm by Caboara and Mora is reported in Section 6, as Algorithm 8.1.

5. On the structure of some ideals

In this section we state and prove some results which will be useful in later sections. The proof of one of our lemmas is very technical and can be found in the appendix. Our aim is to describe the structure of the reduced Gröbner basis for a special class of zero-dimensional ideals. Independently, the authors of [11] were investigating similar settings.

Lemma 5.1. *Let I be a radical 0-dimensional ideal in $K[S', Z', T]$, with $S' = \{s_1, \dots, s_N\}$, $T = \{t_1, \dots, t_M\}$, $Z' = \{z_t, \dots, z_1\}$ and let G be a reduced Gröbner basis of I w.r.t. a block order s.t. $S' < Z' < T$ and a lexicographical order on the Z': $z_t < \cdots < z_1$.*

If $\mathscr{V}(I) \subset K^{N+t+M}$ and $\mathscr{V}(I_{S'}) = \bigsqcup_{j=1}^{t} \Sigma_j \subset K^N$, with

$$\Sigma_j = \{(\bar{s}_1, \dots, \bar{s}_N) \in \mathscr{V}(I_{S'}) \,|\, \textit{there are exactly } j \textit{ values } \{\bar{z}_t^{(1)}, \dots, \bar{z}_t^{(j)}\}, \\ \textit{s.t. } (\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(i)}) \in \mathscr{V}(I_{S' \cup \{z_t\}}), 1 \leqslant i \leqslant j\},$$

$$\Sigma_j \neq \emptyset, 1 \leqslant j \leqslant t,$$

then we have:

- *$G_t = \bigsqcup_{\delta=1}^{\Delta} G_{t,\delta}$, with $\Delta \geqslant t$,*
- *$G_{t,\delta} \neq \emptyset$, for $1 \leqslant \delta \leqslant t$.*

Proof. Recall that $G_t = G \cap K[S', z_t] \backslash K[S']$.

If $\mathbf{s} = (\bar{s}_1, \dots, \bar{s}_N) \in \Sigma_1$, our hypotheses say that exactly one value $\bar{z}_t^{(1)}$ exists, with $(\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(1)}) \in \mathscr{V}(I_{S' \cup \{z_t\}})$, that is the partial solution $\mathbf{s} \in \mathscr{V}(I_{S'})$ can be extended to a root in $\mathscr{V}(I_{S' \cup \{z_t\}})$ only by appending $\bar{z}_t^{(1)}$. Then at least one polynomial $g_1(s_1, \dots, s_N, z_t) \in G_t$ exists s.t. $deg_{z_t}(g_1) = 1$ and $g_1(\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(1)}) = 0$ and this polynomial will be the generator of the image $\phi_1(I_{S' \cup \{z_t\}})$, where$\phi_1$ is the specialization $f \mapsto f(\mathbf{s}, z_t)$ (see [12]).

Now let j be any number $1 \leqslant j \leqslant t$. If $\mathbf{s} = (\bar{s}_1, \dots, \bar{s}_N) \in \Sigma_j$, our hypotheses say that exactly j values $\bar{z}_t^{(1)}, \dots, \bar{z}_t^{(j)}$ exist, such that the j points $(\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(1)}), \dots, (\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(j)}) \in \mathscr{V}(I_{S' \cup \{z_t\}})$, that is the partial solution $\mathbf{s} \in \Sigma_j$ can be extended only by appending $\bar{z}_t^{(1)}, \dots, \bar{z}_t^{(j)}$. Then at least one polynomial $g_\star(s_1, \dots, s_N, z_t) \in G_t$ exists s.t. $deg_{z_t}(g_\star) = j$, $g_\star(\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(1)}) = 0, \dots, g_\star(\bar{s}_1, \dots, \bar{s}_N, \bar{z}_t^{(j)}) = 0$. Again, the polynomial $g_\star$ will be the generator of the image $\phi_j(I_{S' \cup \{z_t\}})$, where ϕ_j is the specialization $f \mapsto f(\mathbf{s}, z_t)$ (see [12]). □

Lemma 5.1 guarantees that the sets G_j are non-empty for $1 \leqslant j \leqslant t$, but this lemma says nothing about the G_j with $j > t$.

In the appendix, we prove the following lemma:

Lemma 5.2. *Let J be a* 0*-dimensional radical ideal in a polynomial ring* $\mathbb{K}[V_1, \ldots, V_{\mathscr{N}}]$, *where* $\mathbb{K}$ *is any field and* $2 \leqslant \mathscr{N}$. *Let* t *be a natural number* $1 \leqslant \mathsf{t}$. *Let G be the lexicographic Gröbner basis of J (with order $V_1 < \cdots < V_{\mathscr{N}}$) and let $\mathscr{D}$ denote the maximal degree in $V_{\mathscr{N}}$ possessed by the polynomials in G. Let $\mathscr{S}$ be any set of* j *points in $\mathbb{K}^{\mathscr{N}}$ of the type $\mathscr{S} = \{(s_1, \ldots, s_{\mathscr{N}-1}, z_1), \ldots, (s_1, \ldots, s_{\mathscr{N}-1}, z_{\mathsf{j}})\}$, where $(s_1, \ldots, s_{\mathscr{N}-1})$ does not belong to the variety $\mathscr{V}(J \cap \mathbb{K}[V_1, \ldots, V_{\mathscr{N}-1}])$ and* $\mathsf{j} \leqslant \mathsf{t}$. *Denote by J' the ideal formed by all polynomials in J vanishing on $\mathscr{S}$. Let G' be the lexicographic Gröbner basis of J' and let $\mathscr{D}'$ denote the maximal degree in $V_{\mathscr{N}}$ possessed by the polynomials in G'. Then*

- *J' is again radical,*
- *if $\mathscr{D} \leqslant \mathsf{t}$, then $\mathscr{D}' \leqslant \mathsf{t}$.*

Using previous lemma, we now specialize Lemma 5.1 to a case which is more interesting to us.

Lemma 5.3. *Let us consider the same notation and the same hypotheses adopted in Lemma* 5.1. *Let $\bar{\Sigma}_j$ be the subset of $\mathscr{V}(I_{S' \cup \{z_t\}})$ formed by points of type $\{(\bar{s}, \bar{z}_t^{(i)})\}$, with $\bar{s} \in \Sigma_j$ and $1 \leqslant i \leqslant j$. Let $\bar{I}$ be the ideal formed by all polynomials in $K[S', z_t]$ vanishing on $\bar{\Sigma}_1$. Let $\bar{G}$ be the Gröbner basis of $\bar{I}$ and $\bar{D}$ denote the maximal degree in z_t possessed by the polynomials in $\bar{G}$. Suppose $\bar{D} \leqslant t$. Then*

$$\Delta = t$$

Proof. If $t = 1$ we have by definition $\bar{I} = I$, so that $\bar{D} = \Delta$ and hence $t \leqslant \Delta = \bar{D} \leqslant t$.

We have to show the case $t \geqslant 2$.

Let $\bar{s}$ be a point in Σ_2 and let $(\bar{s}, \mathsf{z}^1)$, $(\bar{s}, \mathsf{z}^2)$ be its two extensions to $\mathscr{V}(I_{S' \cup \{z_t\}})$. We now apply Lemma 5.2 using:

- $\mathbb{K}[V_1, \ldots, V_{\mathscr{N}}] = K[S', z_t]$, $J = \bar{I}$,
- $\mathscr{S} = \{(\bar{s}, \mathsf{z}^1), (\bar{s}, \mathsf{z}^2)\}$ (and hence J' will be formed by the polynomials in $\bar{I}$ which vanish on the two points $\{(\bar{s}, \mathsf{z}^1), (\bar{s}, \mathsf{z}^2)\}$),
- $\mathsf{t} = t$, $j = 2$.

The radicality of I implies the radicality of all its elimination ideals and so $I_{S' \cup \{z_t\}} = \mathscr{I}(\bigsqcup_{j=1}^{t} \bar{\Sigma}_j)$, showing $\mathscr{I}(\bar{\Sigma}_1) = \bar{I} \supset I$. The hypotheses of Lemma 5.2 are clearly satisfied as the ideal $\bar{I}$ is obviously radical and $\mathscr{D} = \bar{D} \leqslant t$. But then Lemma 5.2 says that J' is again radical and that in its Gröbner basis the degree in z_t is again bounded by t.

We can repeat this argument adding another pair of points of type $(\bar{s}_1, \ldots, \bar{s}_N, \bar{z}_t^{(1)})$, $(\bar{s}_1, \ldots, \bar{s}_N, \bar{z}_t^{(2)})$, where $(\bar{s}_1, \ldots, \bar{s}_N) \in \Sigma_2$ and hence we can show that the ideal we obtain will be again radical and with our bound on the degree. We can proceed until we have added all points of that type. As a result we have that the same properties are shared by the ideal $I_{[2]}$, that is formed by the polynomials of $I_{S' \cup \{z_t\}}$ vanishing on the set $\bar{\Sigma}_1 \sqcup \bar{\Sigma}_2$.

If $t = 2$ we have finished. Otherwise let us call $I_{[h]}$ the ideal formed by the polynomials of $I_{S' \cup \{z_t\}}$ vanishing on the set $\bigsqcup_{j=1}^{h} \bar{\Sigma}_j$, where $3 \leqslant h \leqslant t$. We want to prove by induction on

h that $I_{[h]}$ possesses the following properties:

- $I_{[h]}$ is radical,
- in its Gröbner basis the degree in z_t is bounded by t,

for all h s.t. $1 \leqslant h \leqslant t$. These properties are satisfied by $I_{[1]} = \bar{I}$ and $I_{[2]}$. We assume then that $I_{[h-1]}$ satisfies our properties and we have to prove that also $I_{[h]}$ does (with $3 \leqslant h \leqslant t$). We again apply Lemma 5.2, choosing h points $(\bar{s}, \bar{z}_t^{(1)}), \ldots, (\bar{s}, \bar{z}_t^{(h)})$ in $\mathscr{V}(I_{S' \cup \{z_t\}})$ s.t. $\bar{s} \in \Sigma_h$, and considering

- $\mathbb{K}[V_1, \ldots, V_{\mathscr{N}}] = K[S', z_t]$, $J = I_{[h-1]}$,
- $\mathscr{S} = \{(\bar{s}, \bar{z}_t^{(1)}), \ldots, (\bar{s}, \bar{z}_t^{(h)})\}$ (and hence J' will be formed by the polynomials in $I_{[h-1]}$ which vanish on the h points in $\mathscr{S}$),
- $\mathsf{t} = t$, $\mathsf{j} = h$.

Once again, the hypotheses of Lemma 5.2 are clearly satisfied and so J' is radical and in its Gröbner basis the degree in z_t is bounded by t. As before we can repeat the argument adding suitable h-tuples of points, one h-tuple at a time, and as soon as we have considered all points in Σ_h we will have that our properties are shared by the ideal formed by the polynomial of $I_{[h-1]}$ vanishing on the set $\bar{\Sigma}_h$, i.e. exactly by the ideal $I_{[h]} = I_{S' \cup \{z_t\}}$. □

Theorem 5.4. *Let I be a radical 0-dimensional ideal in $K[S, A, T]$, $S = \{s_1, \ldots, s_N\}$, $T = \{t_1, \ldots, t_M\}$, $A = \{a_l, \ldots, a_1\}$ and G a reduced Gröbner basis of I w.r.t. a block order s.t. $S < A < T$ and a lexicographical order on the A: $a_l < \cdots < a_1$. Suppose I is such that*

(1) $\mathscr{V}(I_S) = \bigsqcup_{j=1}^{l} \Sigma_j^{(l)}$, *with*

$$\Sigma_j^{(l)} = \{(\bar{s}_1, \ldots, \bar{s}_N) \in \mathscr{V}(I_S) \mid \text{there are exactly } j \text{ values } \{\bar{a}_l^{(1)}, \ldots, \bar{a}_l^{(j)}\},$$
$$s.t. (\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_l^{(i)}) \in \mathscr{V}(I_{S \cup \{a_l\}}), 1 \leqslant i \leqslant j\};$$

(2) $\mathscr{V}(I_{S \cup \{a_l\}}) = \bigsqcup_{j=1}^{l-1} \Sigma_j^{(l-1)}$, *with*

$$\Sigma_j^{(l-1)} = \{(\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_l) \in \mathscr{V}(I_{S \cup \{a_l\}}) \mid \text{there are exactly } j \text{ values}$$
$$\{\bar{a}_{l-1}^{(1)}, \ldots, \bar{a}_{l-1}^{(j)}\}, s.t. (\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_l, \bar{a}_{l-1}^{(i)}) \in \mathscr{V}(I_{S \cup \{a_l, a_{l-1}\}}),$$
$$1 \leqslant i \leqslant j\};$$

(3) $\mathscr{V}(I_{S \cup \{a_l, \ldots, a_h\}}) = \bigsqcup_{j=1}^{h-1} \Sigma_j^{(h-1)}$, $2 \leqslant h \leqslant l-1$ *with*

$$\Sigma_j^{(h-1)} = \{(\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_l, \ldots, \bar{a}_h) \in \mathscr{V}(I_{S \cup \{a_l, \ldots, a_h\}}) \mid \exists \text{ exactly } j \text{ values}$$
$$\{\bar{a}_{h-1}^{(1)}, \ldots, \bar{a}_{h-1}^{(j)}\}, s.t. (\bar{s}_1, \ldots, \bar{s}_N, \bar{a}_l, \ldots, \bar{a}_h, \bar{a}_{h-1}^{(i)})$$
$$\in \mathscr{V}(I_{S \cup \{a_l, \ldots, a_{h-1}\}}), 1 \leqslant i \leqslant j\};$$

(4) *the Gröbner basis of the ideal $\mathscr{I}(\Sigma_1^{(h-1)}) \subset K[S, \{a_l, \ldots, a_h\}]$ does not contain polynomials with degree higher than h w.r.t. the variable a_h.*

Then we have, for $1 \leqslant i \leqslant l$,

$$G_i = \bigsqcup_{\delta=1}^{i} G_{i\delta},$$

with $G_{i\delta} \neq \emptyset$, $1 \leqslant \delta \leqslant i$ *and* $1 \leqslant i \leqslant l$.

Proof.

- In the case $i = t = l$, our statement is just a rephrasing of Lemma 5.3, with $S' = S$, $Z' = A$ and obviously $\Sigma_j = \Sigma_j^{(t)}$.
- In the other cases, we can apply Lemma 5.3, choosing the suitable variable sets. To be more precise, for any $1 \leqslant i \leqslant l-1$, we apply Lemma 5.3 setting $S' = S \cup \{a_t, \ldots, a_i\}$, $Z' = \{a_{i+1}, \ldots, a_1\}$ and $\Sigma_j = \Sigma_j^{(i)}$. We clearly have by definition $\bar{I} = \mathscr{I}(\Sigma_1^{(h-1)}) \subset K[S, \{a_l, \ldots, a_h\}]$. □

Theorem 5.5. *Under the hypotheses of Theorem* 5.4 *and with its notation, we have*:

(1) $\forall 1 \leqslant i \leqslant l$, $G_{ii} = \{g_{ii1}\}$, *i.e. only one polynomial exists in* G_i *with degree* i *w.r.t.* a_i;
(2) $\forall 1 \leqslant i \leqslant l$, $Lp(g_{ii1}) = 1$, $Lt(g_{ii1}) = a_i^i$.

Proof. Since I is a 0-dimensional ideal and G is a Gröbner basis of I, then for all $1 \leqslant i \leqslant l$, there is $m_i \in \mathbb{N}$ such that $a_i^{m_i} = LT(g_i)$ for some $g_i \in G$. We claim that, for each $1 \leqslant i \leqslant l$, $g_i \in G_i$. In fact, if $i = l$ and if we suppose that $g_l \in G_i$, with $i < l$, then $g_l \in K[S, a_l, \ldots, a_{i+1}][a_i] \backslash K[S, a_l, \ldots, a_{i+1}]$ and there would be in g_l variables $a_{l-1}, \ldots, a_i$ greater than a_l because $a_l < a_{l-1} < \cdots < a_i$. But then $Lt(g_l) \neq a_l^{m_l}$ and this contradicts our hypothesis. So we deduce that $g_l \in G_l$. The same argument can be used to prove that $g_i \in G_i$, $\forall 1 \leqslant i < l$. Then at least one polynomial g_i exists in G_i, $1 \leqslant i \leqslant l$, such that $Lt(g_i) = a_i^{m_i}$.

Due to Theorem 5.4, each G_i does not contain polynomials with degree higher than i, but it does contain polynomials with degree in a_i exactly i. So $m_i \leqslant i$, $\forall i \leqslant l$. We want to show that g_i is the polynomial with the greatest leading term in G_i and that it is the only one with degree i in a_i. Suppose on the contrary that for some i there is a polynomial $g_i' \in G_i$ s.t. $deg_{a_i}(g_i') = m_i + \varepsilon$, with $\varepsilon \geqslant 0$. Let the leading term of g_i' be $La_i^{m_i+\varepsilon}$, with L a monomial in $K[S, a_l, \ldots, a_{i-1}]$. But then it is obvious that the leading term $a_i^{m_i}$ of g_i divides the leading term of g_i', since $a_i^{m_i} | a_i^{m_i+\varepsilon}$. So we have two polynomials in a reduced Gröbner basis with the leading term of one dividing the leading term of the other one, which is impossible. □

6. A new syndrome variety

Let C be an $[n, k, d]$ cyclic code.

The CRHT-variety described in Section 4 defines a larger variety than that corresponding to all possible correctable syndromes and, as we have already pointed out in Remark 4.3, there are points in $\mathscr{V}(\mathscr{F}_C)$ that do not determine error vectors. If we denote by $\mathscr{V}_C$

the variety in $(\mathbb{F})^r \times (\mathbb{F})^t \times (\mathbb{F}_q)^t$ corresponding to all error vectors with weight $\mu \leqslant t$, then $\mathscr{V}_C \subset V(\mathscr{F}_C)$. In order to restrict the variety $V(\mathscr{F}_C)$ to $\mathscr{V}_C$, we have to add new polynomials to the polynomial system $\mathscr{F}$.

Definition 6.1. Let $n \in \mathbb{N}$ be an integer and $\mathbb{F}_q[x, y]$ a polynomial ring with $(q, n) = 1$. We denote by $\mathsf{p}(n, x, y) \in \mathbb{F}_q[x, y]$ the following polynomial:

$$\mathsf{p}(n, x, y) = \frac{x^n - y^n}{x - y} = \sum_{i=0}^{n} x^i y^{n-1-i}.$$

Lemma 6.2. *Let $n \in \mathbb{N}$ be an integer with $(q, n) = 1$. Let I the ideal in $\mathbb{F}_q[x, y]$*

$$I = \langle \{x^n - 1, y^n - 1, \mathsf{p}(n, x, y)\}\rangle$$

Let S be the set of points in $\mathbb{F}^2$ s.t.

$$(\overline{x}, \overline{y}) \in S \Leftrightarrow \{\overline{x}^n = 1, \overline{y}^n = 1, \overline{x} \neq \overline{y}\}.$$

Then $\mathscr{V}(I) = S$.

Proof. Let $\overline{x}$, $\overline{y}$ be two points in S, then, as $\overline{x}^n = 1$ and $\overline{y}^n = 1$, $\overline{x}^n - \overline{y}^n = 0$. But $\overline{x}^n - \overline{y}^n = (\overline{x} + \overline{y})\, \mathsf{p}(n, \overline{x}, \overline{y})$ and $\overline{x} \neq \overline{y}$, so $\mathsf{p}(n, \overline{x}, \overline{y}) = 0$. That is, $S \subset \mathscr{V}(I)$.

Let $\overline{x}$, $\overline{y}$ be two points outside S. If $\overline{x}^n - 1 \neq 0$, then $\overline{x}$ does not satisfy one polynomial in I. The same argument works for $\overline{y}^n - 1$. So if $(\overline{x}, \overline{y})$ is not in S and yet it is in I, we must have $\overline{x} = \overline{y}$. But then:

$$\mathsf{p}(n, \overline{x}, \overline{y}) = \mathsf{p}(n, \overline{x}, \overline{x}) = \sum_{i=0}^{n-1} \overline{x}^i \overline{x}^{n-1-i} = n\overline{x}^{n-1}$$

and, as $(q, n) = 1$, $\mathsf{p}(n, \overline{x}, \overline{y}) \neq 0$. □

The previous lemma guarantees that the condition $\mathsf{p}(n, x, y)$ removes the points (x, y) such that $x = y$ and both x and y are non-zero.

The following lemma is then obvious.

Lemma 6.3. *With the same notation and hypotheses of Lemma* 6.2, *let $\bar{x}, \bar{y} \in \mathbb{F}$. If $\bar{x} \cdot \bar{y} \cdot \mathsf{p}(n, \bar{x}, \bar{y}) = 0$ then*:

$$\bar{x} \neq \bar{y} \ \ or \ \ (\bar{x} = 0 \ or \ \bar{y} = 0).$$

By adding the polynomials:

$$\chi_{\tilde{l},l} : z_{\tilde{l}} \cdot z_l \cdot \mathsf{p}(n, z_{\tilde{l}}, z_l) = 0, \quad 1 \leqslant \tilde{l} < l \leqslant t \tag{7}$$

to $\mathscr{F}_C$, we have that for all $\tilde{l}$ and l either $z_{\tilde{l}}$ and z_l are distinct or at least one of them is zero, and we obtain a new syndrome variety $\mathscr{F}'_C$:

$$\mathscr{F}'_{\mathscr{C}} = \{f_j, \sigma_j, \eta_i, \lambda_i, \chi_{\tilde{l},l} \mid 1 \leqslant j \leqslant r, 1 \leqslant i \leqslant t, 1 \leqslant \tilde{l} < l \leqslant t\} \subset \mathbb{F}_q[X, Z, Y].$$

We denote by $\mathbf{I}'_{\mathbf{C}}$ the new syndrome ideal generated by $\mathscr{F}'_C$ and we follow this notation in the remainder of the paper. We must now make sure that the solutions of F'_C are exactly the direct extensions, i.e. that we have not removed too much and that we have removed enough. This is shown by the next lemma.

Lemma 6.4. *For any cyclic code C, the solutions of I'_C are the direct extensions of all errors of weight* $0 \leqslant \mu \leqslant t$.

Proof. The direct extensions of errors of weight $\mu \leqslant t$ are solutions of I'_C, because they were present in $\mathscr{V}(I_C)$ and the adding of conditions of type $z_{\tilde{l}} \cdot z_l \cdot p(n, z_{\tilde{l}}, z_l) = 0$ does not remove these roots, since the locations of errors are obviously distinct.

Now we want to prove the converse. Let

$$\overline{B} = (\overline{x}_1, \ldots, \overline{x}_r, \overline{z}_t, \ldots, \overline{z}_1, \overline{y}_1, \ldots, \overline{y}_t)$$

be a solution of I'_C. We have that $(\overline{z}_t, \ldots, \overline{z}_1)$ is of the form

$$(0, \ldots, 0, \tilde{z}_1, 0, \ldots, 0, \tilde{z}_\mu, 0, \ldots, 0),$$

that is, there are μ non-zero elements in $\mathbb{F}$ with $\tilde{z}_i \neq \tilde{z}_j$, $1 \leqslant i < j \leqslant \mu$, and the others elements are all zeros. We can write $(\overline{y}_1, \ldots, \overline{y}_t)$ in the form

$$(*, \ldots, *, \tilde{y}_1, *, \ldots, *, \tilde{y}_\mu, *, \ldots, *),$$

that is, there are μ non-zero elements in $\mathbb{F}_q$ in the same coordinates as $\tilde{z}_1, \ldots, \tilde{z}_\mu$, and $t - \mu$ other non-zero elements of $\mathbb{F}_q$. As $\{z_j\}_{1 \leqslant j \leqslant \mu}$ are nth roots of unity, we can find k_j, $0 \leqslant k_j \leqslant n-1$, such that $\tilde{z}_j = \alpha^{k_j}$ and as $\tilde{z}_i \neq \tilde{z}_j$, $\forall\ 1 \leqslant i < j \leqslant \mu$, we have $k_i \neq k_j$. Now we construct the vector $e = (0, \ldots, 0, \tilde{y}_1, 0, \ldots, 0, \tilde{y}_\mu, 0, \ldots, 0)$ such that its non-zero elements are in the coordinates $k_1, \ldots, k_\mu$. It is now immediate to see that $\overline{B}$ is a direct extension of the solution of (3) corresponding to e. □

Definition 6.5. We denote by $\Sigma_{C,i} \subset \mathbb{F}^r$ the set of all syndromes corresponding to error vectors with weight exactly i.

Lemma 6.6. *Let J be the ideal $(I'_C)_X = I'_C \cap \mathbb{F}[X]$. Then*

$$\mathscr{V}(J) = \Sigma_C = \bigsqcup_{1 \leqslant \mu \leqslant t} \Sigma_{C,i}.$$

Proof. First we prove that $\Sigma_C = \bigsqcup_{1 \leqslant \mu \leqslant t} \Sigma_{C,i}$. Let $(\overline{x}_1, \ldots, \overline{x}_r)$ be an element in Σ_C. As it is a correctable syndrome, it has to correspond to an error with weight $\mu \leqslant t$. Thus $(\overline{x}_1, \ldots, \overline{x}_r) \in \Sigma_{C,\mu}$. Conversely, let $(\overline{x}_1, \ldots, \overline{x}_r) \in \Sigma_{C,i}$. This is a syndrome corresponding to an error with weight $\mu \leqslant t$, that is, $(\overline{x}_1, \ldots, \overline{x}_r)$ is a correctable syndrome.

We are left to show that $\mathscr{V}(J) = \bigsqcup_{1 \leqslant \mu \leqslant t} \Sigma_{C,i}$.

We prove $\Sigma_{C,\mu} \subset \mathscr{V}(J)$. Let $(\overline{x}_1, \ldots, \overline{x}_r) \in \Sigma_{C,\mu}$, then it is a syndrome corresponding to an error with weight $\mu \leqslant t$, such that the error locations are $(\overline{z}_1, \ldots, \overline{z}_\mu)$ and the error values are $(\overline{y}_1, \dots, \overline{y}_\mu)$. The point

$$\overline{B} = (\overline{x}_1, \dots, \overline{x}_r, \overline{z}_1, \dots, \overline{z}_\mu, \underbrace{0, \dots, 0}_{t-\mu}, \overline{y}_1, \dots, \overline{y}_\mu, \underbrace{1, \dots, 1}_{t-\mu})$$

is a direct extension of an error of weight $\mu \leqslant t$ and so from the previous lemma $\bar{B} \in \mathscr{V}(I'_C)$, but then $\bar{B} \cap K^r = (\overline{x}_1, \dots, \overline{x}_r) \in V(J)$.

We prove now $V(J) \subset \Sigma_C$. Let $(\overline{x}_1, \dots, \overline{x}_r) \in V(J)$, then there are $\{z_i\}_{1 \leqslant j \leqslant t}$ and $\{y_i\}_{1 \leqslant j \leqslant t}$ such that $(\overline{x}_1, \dots, \overline{x}_r, \overline{z}_1, \dots, \overline{z}_t, \overline{y}_1, \dots, \overline{y}_t) \in V(I'_C)$. By the previous lemma, we can write this point as

$$(\overline{x}_1, \dots, \overline{x}_r, 0, \dots, 0, \tilde{z}_1, 0, \dots, 0, \tilde{z}_\mu, 0, \dots, 0, \tilde{y}_1, 0, \dots, 0, \tilde{y}_\mu, 0, \dots, 0),$$

where $(\tilde{z}_1, \dots, \tilde{z}_\mu, \tilde{y}_1, \dots, \tilde{y}_\mu)$ is a solution of (5) with syndrome $(\overline{x}_1, \dots, \overline{x}_r)$ corresponding to an error with weight $\mu \leqslant t$. Thus $(\overline{x}_1, \dots, \overline{x}_r) \in \Sigma_{C,\mu}$. □

Remark 6.7. The same considerations present in Remark 4.4 hold. In particular, I'_C is radical for any cyclic code C.

Lemma 6.6 is needed to show that our syndrome ideal I'_C has exactly the properties described in Section 5, which guarantee the structure of its lexicographic Gröbner basis, as shown in the following theorem.

Theorem 6.8. *Let I'_C be the syndrome ideal generated by $\mathscr{F}'_{\mathscr{C}}$ and let G be the reduced Gröbner basis of I'_C w.r.t. the lexicographical order induced by*

$$x_1 < x_2 < \cdots < x_r < z_t < \cdots < z_1 < y_1 < \cdots < y_t.$$

Then:

1. $G = G_X \cup G_{XZ} \cup G_{XZY}$;
2. $G_{XZ} = \bigcup_{i=1}^t G_i$;
3. $G_i = \bigcup_{\delta=1}^i G_{i\delta}$ *and* $G_{i\delta} \neq \emptyset$, *for* $1 \leqslant i \leqslant t$ *and* $1 \leqslant \delta \leqslant i$;
4. $G_{ii} = \{g_{ii1}\}$, *for* $1 \leqslant i \leqslant t$, *i.e. exactly one polynomial exists with degree i w.r.t. the variable z_i in G_i, and its leading term and leading polynomials are*

$$Lt(g_{ii1}) = z_i^i, \quad Lp(g_{ii}) = 1,$$

5. *for* $1 \leqslant i \leqslant t$ *and* $1 \leqslant \delta \leqslant i - 1$, *for each* $g \in G_{i\delta}$, $Tp(g) = 0$.

Proof. Points (1) and (2) are clear.

To show point (3), we need to apply Theorem 5.4. As Theorem 5.5 shares the same hypotheses, the application of the latter will give automatically point 4.

We want to apply Theorem 5.4 with the following setting:

- $S = X$, $A = Z$ and $T = Y$ (implying in particular that $l = t$),
- $I = I'_C$.
- the order on the $\mathbb{F}[X, Z, Y]$ we have chosen.

The lexicographic order on $\mathbb{F}[X, Y, Z]$ s.t. $x_1 < x_2 < \cdots < x_r < z_t < \cdots < z_1 < y_1 < \cdots < y_t$ is obviously a block order s.t. both $X < Z < Y$ and $z_t < \cdots < z_1$. In this setting, we have to make clear:

- what $\Sigma_j^{(t)}$ represents, for $1 \leqslant j \leqslant t$,
- what $\Sigma_j^{(h-1)}$ represents, for $2 \leqslant h \leqslant t$ and $1 \leqslant j \leqslant h-1$,
- that $\mathscr{V}(I_X) = \bigsqcup_{j=1}^{t} \Sigma_j^{(t)}$,
- that $\mathscr{V}(I_{X\cup\{z_t,\ldots,z_h\}}) = \bigsqcup_{j=1}^{h-1} \Sigma_j^{(h-1)}$.

By definition

$$\Sigma_j^{(t)} = \{(\bar{s}_1, \ldots, \bar{s}_N) \in \mathscr{V}(I_X) \mid \text{ there are exactly } j \text{ values } \{\bar{z}_t^{(1)}, \ldots, \bar{z}_t^{(j)}\}, \\ s.t.\ (\bar{s}_1, \ldots, \bar{s}_N, \bar{z}_t^{(i)}) \in \mathscr{V}(I_{X\cup\{z_t\}}), 1 \leqslant i \leqslant j\}.$$

In other words, a point of $\Sigma_j^{(t)}$ is a syndrome and its extension to $\mathscr{V}(I_{X\cup Z})$ is a point

$$(\bar{s}, \mathsf{z}) = (\bar{s}_1, \ldots, \bar{s}_N, \mathsf{z}_t, \ldots, \mathsf{z}_1) \in \mathbb{F}^r \times \mathbb{F}^t$$

such that among its Z coordinates there are only j distinct components. If $0 \leqslant j \leqslant t-1$, the point $(\bar{s}, \mathsf{z})$ will then be formed by a syndrome $\bar{s}$ corresponding to an error of weight $j-1$ and the elements in $\{\mathsf{z}_t, \ldots, \mathsf{z}_1\}$ which are distinct will form the set $\{\bar{z}_t^{(1)}, \ldots, \bar{z}_t^{(j)}\}$. This set contains precisely the locations of error (which are $j-1$) and the value 0.

The case with $j = t$ is analogous but more complex:

- either $\bar{s}$ corresponds to an error of weight $t-1$, and so $\{\bar{z}_t^{(1)}, \ldots, \bar{z}_t^{(j)}\}$ will be the $t-1$ locations of the error plus $\{0\}$,
- or $\bar{s}$ corresponds to an error of weight t, and so $\{\bar{z}_t^{(1)}, \ldots, \bar{z}_t^{(j)}\}$ will be exactly the t locations of the error.

Summing up, we see (Definition 6.5) that

$$\Sigma_j^{(t)} = \Sigma_{C,j-1}, \ 1 \leqslant j \leqslant t-1, \quad \Sigma_t^{(t)} = \Sigma_{C,t-1} \cup \Sigma_{C,t}$$

and so Lemma 6.6 (and the radicality of our ideals) ensures that

$$\mathscr{V}(I_X) = \bigsqcup_{j=1}^{t} \Sigma_j^{(t)}$$

The proof of

$$\mathscr{V}(I_{X\cup\{z_t,\ldots,z_h\}}) = \bigsqcup_{j=1}^{h-1} \Sigma_j^{(h-1)}$$

can be given with similar arguments.

To show point (4) of Theorem 5.4, we observe that the Gröbner basis of $\mathscr{I}(\Sigma_1^{(h-1)})$ (for $3 \leqslant h \leqslant t$) will be formed by some polynomials only in the X variables plus the single polynomial z_h, because if there is only one possible extension then we must add only 0.

We are left with showing point (5), i.e. that almost all polynomials in G_i (all but the greatest) have no trailing polynomials. This is equivalent to say that any such polynomials, once evaluated on a syndrome $\bar{s}$ (and its portion of $i-1$ Z components), must have 0 as a root (seen as a polynomial in $\mathbb{F}[z_i]$), which is obviously always the case, except when considering the greatest polynomial g_{ii1}. □

We are now ready (see Definition 3.1) for our main result of this section:

Theorem 6.9. *Each cyclic code C possesses a general error locator polynomial $\mathscr{L}_C$.*

Proof. Just take $\mathscr{L}_C = g_{tt1}(x_1, \ldots, x_r, z)$. It is trivial to see that this polynomial satisfies all properties needed by a general error locator polynomial. Actually:

- it lies in $\mathbb{F}_q[X, z]$, because g_{tt1} is an element of a Gröbner basis which can be computed by Buchberger algorithm starting from the polynomials $\mathscr{F}'_C$, with $\mathscr{F}'_C \in \mathbb{F}_q[X, Z, Y]$;
- it never becomes identically zero once evaluated on a correctable syndrome (compare to point 2.2 in Theorem 4.5), as its leading polynomial 1 never vanishes, and so it will contain all locations of errors (and multiple zeros, when appropriate);
- its degree in z is exactly t. □

Remark 6.10. We observe that in [3] to find the error locator polynomial we have to study all G_{XZ}, precisely if we know that there are at most $\mu \leqslant t$ errors, we search for $L(z)$ in $G_{\mu\mu}$. Instead, thanks to Theorem 6.9, we have only to specialize $\mathscr{L}_C$ to a given syndrome. So, we can present and discuss in Section 8 new decoding procedures for cyclic codes.

We now give an example, which illustrates very well the structure of the Gröbner basis as predicted by Theorem 6.8.

Example 6.11. We consider the same example discussed in [3,15]. Let C be the 3 error-correcting BCH [17,6,8] over $\mathbb{Z}_2$. The CRHT syndrome ideal $I = I_C$ is generated by $\mathscr{F}_C$, i.e.

$$z_1 + z_2 + z_3 + x_1, \quad z_1^3 + z_2^3 + z_3^3 + x_2, \quad z_1^5 + z_2^5 + z_3^5 + x_3,$$

$$x_1^{16} - x_1, \quad x_2^{16} - x_2, \quad x_3^{16} - x_3,$$

$$z_1^{16} - z_1, \quad z_2^{16} - z_2, \quad z_3^{16} - z_3$$

If we calculate the Gröbner basis G w.r.t. the lexicographical order induced by: $x_1 < x_2 < x_3 < z_3 < z_2 < z_1$, the elements of G_{XZ} are: $G_3 = G_{3,3} \cup G_{3,16}$, $G_{3,3} = \{g_{3\,3\,1}, g_{3\,3\,2}\}$, $G_{3,16} = \{g_{3\,16\,1}\}$, $G_2 = G_{2,2} \cup G_{2,16}$, $G_{2,2} = \{g_{2\,2\,1}, g_{2\,2\,2}, g_{2\,2\,3}\}$, $G_{2,16} = \{g_{2\,16\,1}\}$,

$G_1 = G_{1,1} = \{g_{1\,1\,1}\}$, where

$$Lp_{z_3}(g_{3\,3\,1}) = \mathbf{z_3^3}(x_2 + x_1^3);$$

$$Lp_{z_3}(g_{3\,3\,2}) = \mathbf{z_3^3}(x_3 + x_1^5);$$

$$g_{3\,16\,1} = \mathbf{z_3^{16}} + z_3;$$

$$Lp_{z_2}(g_{2\,2\,1}) = \mathbf{z_2^2}(x_2 + x_1^3);$$

$$Lp_{z_2}(g_{2\,2\,2}) = \mathbf{z_2^2}(x_3 + x_1^5);$$

$$Lp_{z_2}(g_{2\,2\,3}) = \mathbf{z_2^2}(z_3 + x_1);$$

$$(g_{2\,16\,1}) = \quad \mathbf{z_2^{16}} + z_2;$$

$$Lp_{z_1}(g_{1\,1\,1}) = \mathbf{z_1} + z_2 + z_3 + x_1.$$

We can comment on this structure.

First, observe that the greatest polynomial in G_3 is $z_3^{16} + z_3$ and is the only one in G_3 which does not become identically zero once evaluated on a syndrome. It could be a good candidate as a general error locator polynomial, but unfortunately its degree is 16 instead of 3 and it will never tell us anything useful, except the trivial fact that the error locations must be searched among the 15th roots of unity.

Second, if we look at $G_{3,3}$ we see two polynomials, any of them becoming identically zero on some correctable syndrome and so neither could be a candidate for a general error locator polynomial. To show that for each g in G_3 there is a correctable syndrome $\bar{s}$ such that $g(\bar{s}, z)$ becomes identically zero, we observe that $g(\bar{s}, z) \equiv 0$ is equivalent to $Lp(g)(\bar{s}) = 0$, due to Gianni's Theorem, and then it is enough for us to check if there are correctable syndromes among the roots of $Lp(g)$. The check can be easily done by hand.

Last, there are no polynomials in $G_{3,1}$ or in $G_{3,2}$. So if we have a syndrome corresponding to an error with weight 1, we will not have a polynomial of degree 1 which will give us the error location (once specialized), but we will need a polynomial at least of degree three. This is an apparent contradiction to Gianni's Theorem, but in reality what happens is that to an error of weight 1 many other z values correspond: the ones coming from roots of I which are *not* direct extensions (see Section 4).

If we add conditions (7) to I, we obtain our syndrome ideal $I' = I'_C$:

$$\begin{array}{lll}
z_1 + z_2 + z_3 + x_1, & z_1^3 + z_2^3 + z_3^3 + x_2, & z_1^5 + z_2^5 + z_3^5 + x_3,\\
x_1^{16} - x_1, & x_2^{16} - x_2, & x_3^{16} - x_3,\\
z_1^{16} - z_1, & z_2^{16} - z_2, & z_3^{16} - z_3\\
z_1z_2\mathsf{p}(15, z_1, z_2), & z_1z_3\mathsf{p}(15, z_1, z_3), & z_2z_3\mathsf{p}(15, z_2, z_3)
\end{array}$$

We call G the corresponding Gröbner basis and so the elements of G_{XZ} are:

$$g_{3\,1\,1} = \mathbf{z_3}(x_2^{15}x_1^{15} + x_2^{15} + x_1^{15} + 1);$$

$$\begin{aligned}
g_{3\,2\,1} = \mathbf{z_3^2}(&x_2^{15} + x_2^{14}x_1^3 + x_2^{13}x_1^6 + x_2^{12}x_1^9 + x_2^{11}x_1^{12} + x_2^{10}x_1^{15} + x_2^9x_1^3\\
&+ x_2^8x_1^6 + x_2^7x_1^9 + x_2^6x_1^{12} + x_2^5x_1^{15} + x_2^4x_1^3 + x_2^3x_1^6 + x_2^2x_1^9 + x_2x_1^{12}\\
&+ x_1^{15} + 1) + \mathbf{z_3}(x_2^{15}x_1 + x_2^{14}x_1^4 + x_2^{13}x_1^7 + x_2^{12}x_1^{10} + x_2^{11}x_1^{13} + x_2^{10}x_1\\
&+ x_2^9x_1^4 + x_2^8x_1^7 + x_2^7x_1^{10} + x_2^6x_1^{13} + x_2^5x_1 + x_2^4x_1^4 + x_2^3x_1^7\\
&+ x_2^2x_1^{10} + x_2x_1^{13});
\end{aligned}$$

$$\begin{aligned}
g_{3\,3\,1} = \mathbf{z_3^3} + \mathbf{z_3^2}x_1 + \mathbf{z_3}(&x_3x_2^9 + x_3x_2^8x_1^3 + x_3x_2^4 + x_3x_2x_1^9 + x_2^{15}x_1^2 + x_2^{14}x_1^5\\
&+ x_2^{13}x_1^8 + x_2^{12}x_1^{11} + x_2^{11}x_1^{14} + x_2^{10}x_1^2 + x_2^7x_1^{11} + x_2^6x_1^{14} + x_2^5x_1^2 + x_2^3x_1^8\\
&+ x_2^2x_1^{11} + x_1^2) + (x_3x_2^9x_1 + x_3x_2^8x_1^4 + x_3x_2^4x_1 + x_3x_2x_1^{10} + x_2^{15}x_1^3\\
&+ x_2^{14}x_1^6 + x_2^{13}x_1^9 + x_2^{12}x_1^{12} + x_2^{11}x_1^{15} + x_2^{10}x_1^3 + x_2^7x_1^{12} + x_2^6x_1^{15}\\
&+ x_2^5x_1^3 + x_2^3x_1^9 + x_2^2x_1^{12} + x_2);
\end{aligned}$$

$$g_{2\,1\,1} = \mathbf{z_2}(x_2^{15}x_1^{15} + x_2^{15} + x_1^{15} + 1);$$

$$\begin{aligned}
g_{2\,1\,2} = \mathbf{z_2}(&z_3x_2^{15} + z_3x_2^{14}x_1^3 + z_3x_2^{13}x_1^6 + z_3x_2^{12}x_1^9 + z_3x_2^{11}x_1^{12} + z_3x_2^{10}x_1^{15}\\
&+ z_3x_2^9x_1^3 + z_3x_2^8x_1^6 + z_3x_2^7x_1^9 + z_3x_2^6x_1^{12} + z_3x_2^5x_1^{15} + z_3x_2^4x_1^3 + z_3x_2^3x_1^6\\
&+ z_3x_2^2x_1^9 + z_3x_2x_1^{12} + z_3x_1^{15} + z_3);
\end{aligned}$$

$$\begin{aligned}
g_{2\,2\,1} = \mathbf{z_2^2} + \mathbf{z_2}(z_3 + x_1) + (&z_3^2 + z_3x_1 + x_3x_2^9 + x_3x_2^8x_1^3 + x_3x_2^4 + x_3x_2x_1^9 + x_2^{15}x_1^2\\
&+ x_2^{14}x_1^5 + x_2^{13}x_1^8 + x_2^{12}x_1^{11} + x_2^{11}x_1^{14} + x_2^{10}x_1^2 + x_2^7x_1^{11} + x_2^6x_1^{14}\\
&+ x_2^5x_1^2 + x_2^3x_1^8 + x_2^2x_1^{11} + x_1^2);
\end{aligned}$$

$$g_{1\,1\,1} = \mathbf{z_1} + (z_2 + z_3 + x_1);$$

Thus,

$G_3 = G_{3,3} \cup G_{3,2} \cup G_{3,1},\ \ G_{3,3} = \{g_{3\,3\,1}\},\ G_{3,2} = \{g_{3\,2\,1}\},\ G_{3,1} = \{g_{3\,1\,1}\}$,
$G_2 = G_{2,2} \cup G_{2,1},\ \ G_{2,2} = \{g_{2\,2\,1}\}, G_{2,1} = \{g_{2\,1\,1}, g_{2\,1\,2}\}$,
$G_1 = G_{1,1} = \{g_{1\,1\,1}\}$.

Note that G_3 has exactly the structure described in Theorem 6.8:

1. For each $1 \leqslant i \leqslant 3$, there are in G_i polynomials for each degree δ, $1 \leqslant \delta \leqslant i$, w.r.t. z_i. That is, in G_3 we have polynomials of degree (in z_3) 3, 2 and 1, without gaps (compare to the case previously discussed). In G_2, we have polynomials of degree (in z_2) 2 and 1. In G_1, there are polynomials of degree 1 in (z_1).
2. There are no greater degree polynomials, i.e. in G_3 there are no polynomials of degree in z_3 greater than 3, in G_2 there are no polynomials of degree in z_2 greater than 2 and in G_1 there are no polynomials of degree in z_1 greater than 1.
3. The greatest degree polynomial in G_i is the unique member of $G_{i,i}$, i.e. there is only one polynomial in G_3 of degree 3, there is only one polynomial in G_2 of degree 2, there is only one polynomial in G_1 of degree 1. These three polynomials have, respectively, z_3^3, z_2^2, z_1 as leading terms and 1 as leading polynomial.
4. In particular, the polynomial g_{331} is a *general error locator polynomial* of BCH[17,6,8].

5. The trailing polynomials are all zero, except for the greatest polynomials in each G_i:

$$Tp(g_{3\,1\,1}) = 0,\ \ Tp(g_{3\,2\,1}) = 0,\ \ Tp(g_{3\,3\,1}) \neq 0;$$
$$Tp(g_{2\,1\,1}) = 0,\ \ Tp(g_{2\,2\,1}) \neq 0;$$
$$Tp(g_{1\,1\,1}) \neq 0.$$

Remark 6.12. In some examples that we have computed (like Example 6.11), in addition to the structure that we have foreseen, a curious property holds: in each $G_{t,\delta}$ there is only one polynomial. It would be interesting to know for which cyclic codes this stricter property holds.

7. Extended syndrome variety

Let C be a cyclic code with the same notation used in the preceding section. We will now extend previous results to the case when there are also erasures. To accomplish this, we have to find the solutions of equations (1):

$$\bar{\mathbf{s}}_j + \sum_{l=1}^{\mu} a_l(\alpha^{i_j})^{k_l} + \sum_{\bar{l}=1}^{v} \bar{c}_{\bar{l}}(\alpha^{i_j})^{h_{\bar{l}}} = 0, \quad 1 \leqslant j \leqslant r.$$

where $\{k_l\}$, $\{a_l\}$ and $\{\bar{c}_{\bar{l}}\}$ are unknown and $\{\bar{s}_j\}$, $\{h_{\bar{l}}\}$ are known. We keep consistent with our setting (introduced in Section 4 and Section 6) and we introduce variables $W = (w_v, \ldots, w_1)$ and $U = (u_1, \ldots, u_v)$, where

w_h stands for the erasure locations $(\alpha^{i_j})^{h_{\bar{l}}}$, $1 \leqslant h \leqslant v$;
u_h stands for the erasure values $\bar{c}_{\bar{l}}$, $1 \leqslant h \leqslant v$.

As soon as the word $v(x)$ is received, we know the number v of erasures, their positions $\{w_h\}$, and that

$$\tau \leqslant (d - v)/2.$$

As usual we assume that $\mu \leqslant \tau$ and for this reason we can write

$$\bar{\mathbf{s}}_j + \sum_{l=1}^{\tau} a_l(\alpha^{i_j})^{k_l} + \sum_{\bar{l}=1}^{v} \bar{c}_{\bar{l}}(\alpha^{i_j})^{h_{\bar{l}}} = 0, \quad 1 \leqslant j \leqslant r. \tag{8}$$

Then we rewrite Eqs. (8) in term of X, Z, Y, W and U, where now x_j stands for the truncated syndrome $\bar{s}_j$, $1 \leqslant j \leqslant r$:

f_j: $\sum_{l=1}^{t} y_l z_l^{i_j} + \sum_{\bar{l}=1}^{v} u_{\bar{l}} w_{\bar{l}}^{i_j} - x_j = 0$, $1 \leqslant j \leqslant r$,
σ_j: $x_j^{q^m} - x_j = 0$, $1 \leqslant j \leqslant r$, since $\mathbf{s_j} \in \mathbb{F}$ (note that we are denoting by $\mathbf{s}$ the truncated syndrome);
η_i: $z_i^{n+1} - z_i = 0$, $1 \leqslant i \leqslant \tau$, since $(\alpha^{i_j})^{k_l}$ are nth-roots of unity or zero;
λ_i: $y_i^{q-1} - 1 = 0$, $1 \leqslant i \leqslant \tau$, since $a_l \in \mathbb{F}_q/\{0\}$;

ξ_h: $w_h^n - 1 = 0$, $1 \leqslant h \leqslant v$, since $(\alpha_j^i)^{h_{\bar{l}}}$ are nth-roots of unity;
ζ_h: $u_h^q - u_h = 0$, $1 \leqslant h \leqslant v$, since $\bar{c}_{\bar{l}} \in \mathbb{F}_q$;
χ_{il}: $z_i z_l \mathsf{p}(n, z_i, z_l) = 0$, $1 \leqslant i < l \leqslant \tau$, since $(\alpha^{i_j})^{k_l} \neq (\alpha^{i_j})^{k_{l'}}$;
$\bar{\chi}_{ih}$: $z_i \mathsf{p}(n, z_i, w_h) = 0$, $1 \leqslant i \leqslant \tau$, $1 \leqslant h \leqslant v$, since $(\alpha^{i_j})^{k_l} \neq (\alpha^{i_j})^{h_{\bar{l}}}$;
$\tilde{\chi}_{hk}$: $\mathsf{p}(w_h, w_k) = 0$, $1 \leqslant h < k \leqslant v$, since $(\alpha^{i_j})^{h_{\bar{l}}} \neq (\alpha^{i_j})^{h_{\tilde{l}}}$.

The equations of type χ_{il} ensure that two error locations are distinct if they are non-zero (see Lemma 6.3). The equations of type $\bar{\chi}_{ih}$ ensure that an error cannot occur in a position corresponding to an erasure. The equations of type $\tilde{\chi}_{hk}$ ensure that two erasure locations are distinct.

Remark 7.1. In this section when we say "syndrome" we always mean "truncated syndrome" and so our previous notation for syndromes and syndrome components, such as $\bar{s}$, x_i, etc., will now apply correspondingly to the truncated syndromes and their components.

With this notations we have

$$\mathscr{F}_C^v = \{f_j, \sigma_j, \eta_i, \lambda_i, \xi_h, \zeta_h, \chi_{il}, \bar{\chi}_{ih}, \tilde{\chi}_{hk} \mid 1 \leqslant j \leqslant r, 1 \leqslant i \leqslant \tau, 1 \leqslant h \leqslant v,$$
$$1 \leqslant i < l \leqslant \tau, 1 \leqslant h < k \leqslant v\} \subset \mathbb{F}_q[X, W, Z, U, Y]\}.$$

The ideal I_C^v generated by $\mathscr{F}_C^v$ is the *extended syndrome ideal* and $\mathscr{V}(\mathscr{F}_C^v) = \mathscr{V}(I_C^v)$ is the *extended syndrome variety*.

Remark 7.2. While the syndrome ideal I_C depends only on the code C, the extended syndrome ideal I_C^v depends also on the number of erasures v.

We now need an extension of Definition 4.1:

Definition 7.3. We call *correctable pairs* the pairs of type $(\mathbf{s}, \mathbf{w})$, with syndrome vector $\mathbf{s} \in \mathbb{F}^r$ and error location vector $\mathbf{w} \in \mathbb{F}^v$, corresponding to errors with weight $\mu \leqslant \tau$. We denote by $\Sigma_C^v \subset \mathbb{F}^r \times \mathbb{F}^v$ the set of all correctable pairs associated to the code C, when v erasures have occurred.

We can extend also Definition 6.5:

Definition 7.4. We denote by $\Sigma_{C,i}^v \subset \mathbb{F}^r \times \mathbb{F}^v$ the set of all correctable pairs corresponding to error vectors with weight exactly i.

With arguments similar to those used in the proof of Lemma 6.6 (the key point being that a correctable pair will identify *uniquely* an error vector, thanks to equations of kind χ_{il}, $\bar{\chi}_{ih}$ and $\tilde{\chi}_{hk}$), it is easy to show the following lemma:

Lemma 7.5. *Let J^v be the ideal $(I_C^v)_X = I_C^v \cap \mathbb{F}[X]$. Then*

$$\mathscr{V}(J) = \Sigma_C^v = \bigsqcup_{1 \leqslant \mu \leqslant \tau} \Sigma_{C,i}^v.$$

By Lemma 7.5 and using arguments analogous to those used in Theorem 6.8, it is easy to show the following theorem on the structure of the Gröbner basis of our ideal:

Theorem 7.6. *Let I_C^v be the syndrome ideal generated by $\mathscr{F}_{\mathscr{C}}^v$ and let G be the reduced Gröbner basis of I_C^v w.r.t. the lexicographical order induced by*

$$x_1 < \cdots < x_r < w_1 < \cdots < w_v < z_\tau < \cdots < z_1 < u_1 < \cdots < u_v < y_1 < \cdots < y_\tau .$$

Then:

1. $G = G_X \sqcup G_{XW} \sqcup G_{XWZ} \sqcup G_{XWZU} \sqcup G_{XWZUY}$.
2. $G_{XWZ} = \bigcup_{i=1}^{\tau} G_i$;
3. $G_i = \bigcup_{\delta=1}^{i} G_{i\delta}$ *and* $G_{i\delta} \neq \emptyset$, *for* $1 \leqslant i \leqslant \tau$ *and* $1 \leqslant \delta \leqslant i$;
4. $G_{ii} = \{g_{ii1}\}$, *for* $1 \leqslant i \leqslant \tau$, *i.e. exactly one polynomial exists with degree* i *w.r.t. the variable* z_i *in* G_i, *and its leading term and leading polynomials are*

   $$Lt(g_{ii1}) = z_i^i, \quad Lp(g_{ii}) = 1$$

5. *for* $1 \leqslant i \leqslant \tau$ *and* $1 \leqslant \delta \leqslant i-1$, *for each* $g \in G_{i\delta}$, $Tp(g) = 0$.

From Theorem 7.6, the main result (see Definition 3.3) of this section follows:

Theorem 7.7. *Each cyclic code C possesses a general error locator polynomial* $\mathscr{L}_C^v$ *of any type v, for* $0 \leqslant v < d$.

Proof. Just take $\mathscr{L}_C^v = g_{\tau\tau1}(x_1, \ldots, x_r, w_1, \ldots, w_v, z)$. It is trivial to see that this polynomial satisfies all the properties needed by a general error locator polynomial. Actually:

- it lies in $\mathbb{F}_q[X, W, z]$, because g_{tt1} is an element of a Gröbner basis which can be computed by Buchberger algorithm starting from the polynomials $\mathscr{F}_C^v$, with $\mathscr{F}_C^v \in \mathbb{F}_q[X, W, Z, U, Y]$;
- it never becomes identically zero once evaluated on a correctable pair, as its leading polynomial 1 never vanishes, and so it will contain all locations of errors (and multiple zeros, when appropriate);
- its degree in z is exactly τ. □

8. Algorithms and examples

In this section we first recall the revised CRHT decoding algorithm [3] and then we present a new decoding algorithm for cyclic codes that exploits the properties of a general error locator polynomial (see Theorem 6.9). We are going to show also how to decode simultaneously errors and erasures using general error locator polynomials (see Theorem 7.7).

In [3] Caboara and Mora propose Algorithm 8.1. It accepts as input a syndrome vector and outputs an error locator polynomial.

Algorithm 8.1 (*Revised CRHT-decoding algorithm* [3]).

```
Input s = $(s_1, \ldots, s_r)$;
$\mu := t$; $L := 1$
Repeat
  $j := 0$
  Repeat
    $j := j + 1$
  Until $Lp_{z_\mu}(g_{\mu\mu j})(s_1, \ldots, s_r, 0, \ldots, 0) \neq 0$ or $j > j_{\mu\mu}$
  If $j > j_{\mu\mu}$ then
    $\mu := \mu - 1$
  else
    If $Tp_{z_\mu}(g_{\mu\mu j})(s_1, \ldots, s_r, 0, \ldots, 0) = 0$ do
      $\mu := \mu - 1$
    else
      $L := g_{\mu\mu j}(s_1, \ldots, s_r, 0, \ldots, 0, z)$;
      Output $\mu$, $L(z)$
Until $L \neq 1$ or $\mu = 0$
Output $\mu$, $L(z)$
```

The number of polynomial evaluations that this algorithm has to perform in the worst case is clearly

$$\mathcal{N}(8.1) = \sum_{i=1}^{t} N_{ii} + 1 + t + 1.$$

Thanks to Theorem 6.9, to find the error locator polynomial we can consider directly the general error locator polynomial:

$$\mathcal{L}_C(x_1, \ldots, x_r, z) = z^t + a_{t-1}(x_1, \ldots, x_r)z^{t-1} + \cdots + a_0(x_1, \ldots, x_r).$$

From that we can directly design the following algorithm.

Algorithm 8.2.

```
Input s = $(s_1, \ldots, s_r)$
$\mu = t$
While $a_{t-\mu}(s_1, \ldots, s_r) = 0$ do
  $\mu := \mu - 1$;
Output $\mu$, $L(z)/(z^{t-\mu})$
```

The number of polynomial evaluations that our algorithm has to perform in the worst case is just

$$\mathcal{N}(8.2) = t - 1.$$

Example 8.3. We now apply Algorithm 8.2 to Example 6.11. We have that

$$\mathscr{L}_C = g_{3\,3\,1} = z_3^3 + a(x_1, x_2, x_3)z_3^2 + b(x_1, x_2, x_3)z_3 + c(x_1, x_2, x_3)$$

and

$$\begin{aligned} a &= x_1, \\ b &= x_3x_2^9 + x_3x_2^8x_1^3 + x_3x_2^4 + x_3x_2x_1^9 + x_2^{15}x_1^2 + x_2^{14}x_1^5 + x_2^{13}x_1^8 + x_2^{12}x_1^{11} \\ &\quad + x_2^{11}x_1^{14} + x_2^{10}x_1^2 + x_2^7x_1^{11} + x_2^6x_1^{14} + x_2^5x_1^2 + x_2^3x_1^8 + x_2^2x_1^{11} + x_1^2, \\ c &= x_3x_2^9x_1 + x_3x_2^8x_1^4 + x_3x_2^4x_1 + x_3x_2x_1^{10} + x_2^{15}x_1^3 + x_2^{14}x_1^6 + x_2^{13}x_1^9 + x_2^{12}x_1^{12} \\ &\quad + x_2^{11}x_1^{15} + x_2^{10}x_1^3 + x_2^7x_1^{12} + x_2^6x_1^{15} + x_2^5x_1^3 + x_2^3x_1^9 + x_2^2x_1^{12} + x_2. \end{aligned}$$

So we decode this way:

```
First, given a syndrome $(s_1, s_2, s_3) \neq (0, 0, 0)$, we evaluate the three polynomials
$A = a(s_1, s_2, s_3) = s_1$, $B = b(s_1, s_2, s_3)$, $C = c(s_1, s_2, s_3)$.
**if** $C \neq 0$ **then** $\mu := 3$, $L(z) = z_3^3 + Az_3^2 + Bz_3 + C$,
**else if** $C = 0,\ B \neq 0$
        **then** $\mu := 2$, $L(z) = z_3^2 + Az_3 + B$
**else if** $C = 0,\ B = 0,\ A \neq 0$,
        **then** $\mu := 1$ $L(z) = z_3 + A$ (and so $z_3 = s_1$).
```

The last case $A = B = C = 0$ cannot occur, because this is equivalent to a no error event and this is checked at the beginning, when we make sure that the vector syndrome (s_1, s_2, s_3) is not the zero vector (0, 0, 0).

A modified version of this algorithm can cover the case with erasures. Actually, Theorem 7.7 suggests that, in order to find the error locator polynomial when v erasures have occurred, we exploit the properties of the general error locator polynomial of type v:

$$\begin{aligned} &\mathscr{L}_C^v(x_1, \ldots, x_r, w_1, \ldots, w_v, z) \\ &\quad = z^\tau + a_{\tau-1}(x_1, \ldots, x_r, w_1, \ldots, w_v)z^{\tau-1} + \cdots + a_0(x_1, \ldots, x_r, w_1, \ldots, w_v). \end{aligned}$$

It is then natural to design the following:

Algorithm 8.4.

```
**Input** $\mathbf{s} = (s_1, \ldots, s_r)$, $\mathbf{w} = (w_1, \ldots, w_v)$
$\mu = \tau$
**While** $a_{\tau-\mu}(s_1, \ldots, s_r) = 0$ **do**
 $\mu := \mu - 1$;
**Output** $\mu,\ L(z)/(z^{\tau-\mu})$
```

Algorithm 8.4 will give us the locations of the errors. But to complete our decoding we need also to find the values of the erasures. To find them there are two ways:

- one can set up a system T using Eq. (1) with $1 \leqslant j \leqslant r$: the only unknowns in T are (after performance of Algorithm 8.4) the syndrome values $\{c_{h_{\bar{l}}}\}$; the system T is linear with respect to the variables $\{c_{h_{\bar{l}}}\}$ and so it can be easily solved. This is one of the standard approaches in the simultaneous decoding of errors and erasures.

- An alternative approach is to use again our knowledge of the variety $\mathscr{V}(I_C^v)$: once the syndromes, the erasure locations and the error locations are fixed there is only one value for each of the $\{u_i\}$ (the values of the erasures). So in the reduced Gröbner basis G there must be a polynomial of degree 1 in the lowest u_i (and coefficients in the $\{X, W, Z\}$), i.e. in u_1. Let us call P_1 such polynomial. We can compute a similar Gröbner basis putting u_2 as the lowest variable among the $\{u_i\}$. We would get a polynomial of degree 1 in u_2. And so on. Let us call this polynomials P_i, for $1 \leqslant i \leqslant v$. The polynomials are computed once and for all, before any decoding process starts. So the complete decoding can work this way:

  - we receive a vector with some erasures $\mathbf{w}$ and we compute its associated syndrome $\mathbf{s}$.
  - We give to Algorithm 8.4 as input the pair $(\mathbf{s}, \mathbf{w})$ and we get as output the error locator polynomial $L(z)$.
  - From $L(z)$ we get the error positions $\mathbf{z}$.
  - We compute $u_1 - P_i(\mathbf{s}, \mathbf{w}, \mathbf{z})$ for $1 \leqslant i \leqslant v$ and the results will be the erasure locations.
  - We find the error values with some standard methods [10].

The next example concludes this section. Here we take a very simple cyclic code and we show both its syndrome ideal and one of its extended syndrome ideals.

Example 8.5. We consider the BCH$(n = 7, \delta = 5)$ code C over $\mathbb{F}_2$, i.e. $C = \{0000000, 1111111\}$. If $v = 0$ then our syndrome ideal is

$$\begin{aligned} I = \{&z_1 + z_2 + z_3 + x_1, z_1^3 + z_2^3 + z_3^3 + x_2, \\ &z_1^8 - z_1, z_2^8 - z_2, z_3^8 - z_3, \\ &x_1^2 - x_1, x_2^2 - x_2, \\ &z_1 z_2 \mathsf{p}(7, z_1, z_2), z_2 z_3 \mathsf{p}(7, z_2, z_3), z_1 z_3 \mathsf{p}(7, z_1, z_3)\}, \end{aligned}$$

and the reduced Gröbner basis G is

$$g_1 = x_1^8 + x_1;$$
$$g_2 = x_2^8 + x_2;$$
$$g_{31} = \mathbf{z_3}(x_2^7 x_1^7 + x_2^7 + x_1^7 + 1);$$

$$\begin{aligned} g_{32} = {}&\mathbf{z_3^2}(x_2^7 + x_2^6 x_1^3 + x_2^5 x_1^6 + x_2^4 x_1^2 + x_2^3 x_1^5 + x_2^2 x_1 + x_2 x_1^4 + x_1^7 + 1) \\ &+ \mathbf{z_3}(x_2^7 x_1 + x_2^6 x_1^4 + x_2^5 x_1^7 + x_2^4 x_1^3 + x_2^3 x_1^6 + x_2^2 x_1^2 + x_2 * x_1^5); \end{aligned}$$

$$\begin{aligned} g_{33} = {}&\mathbf{z_3^3} + \mathbf{z_3^2} x_1 + \mathbf{z_3}(x_2^7 x_1^2 + x_2^6 x_1^5 + x_2^5 x_1 + x_2^4 x_1^4 + x_2^3 x_1^7 + x_2^3) \\ &+ x_2^7 x_1^3 + x_2^6 x_1^6 + x_2^5 x_1^2 + x_2^4 x_1^5 + x_2 + x_1^3; \end{aligned}$$

$$g_{2\,1\,1} = z_2 x_2^7 x_1^7 + z_2 x_2^7 + z_2 x_1^7 + z_2;$$

$$\begin{aligned} g_{2\,1\,2} = {} & z_2z_3x_2^7 + z_2z_3x_2^6x_1^3 + z_2z_3x_2^5x_1^6 + z_2z_3x_2^4x_1^2 + z_2z_3x_2^3x_1^5 + z_2z_3x_2^2x_1 \\ & + z_2z_3x_2x_1^4 + z_2z_3x_1^7 + z_2z_3; \end{aligned}$$

$$\begin{aligned} g_{2\,2\,1} = {} & z_2^2 + z_2z_3 + z_2x_1 + z_3^2 + z_3x_1 + x_2^7x_1^2 + x_2^6x_1^5 + x_2^5x_1 + x_2^4x_1^4 \\ & + x_2^3x_1^7 + x_2^3; \end{aligned}$$

$$g_{1\,1\,1} = z_1 + z_2 + z_3 + x_1.$$

G has the structure described in Theorem 6.8: in fact G_3 has exactly one polynomial for each degree $\delta \leqslant 3$. The trailing polynomials of g_{31} and g_{32} are zero, and the leading polynomial of g_{33} is 1.

If $v = 1$ then $2\tau + 1 < 7$, i.e. $\tau \leqslant 2$. The extended syndrome ideal is

$$\begin{aligned} I = \{ & z_1 + z_2 + u_1w_1 + x_1,\ z_1^3 + z_2^3 + u_1w_1^3 + x_2, \\ & z_1^8 + z_1,\ z_2^8 + z_2,\ w_1^7 + 1,\ u_1^2 - u_1, \\ & z_1z_2\mathsf{p}(7, z_1, z_2),\ z_1\mathsf{p}(7, z_1, w_1),\ z_2\mathsf{p}(7, z_2, w_1), \}; \end{aligned}$$

and the reduced Gröbner basis G is

$$\begin{aligned} g_1 &= x_1^8 + x_1; \\ g_2 &= x_2^8 + x_2; \\ g_3 &= w_1^3x_2x_1^7 + w_1^3x_2 + w_1x_2^4x_1^7 + w_1x_2^4 + x_2^2x_1^7 + x_2^2; \end{aligned}$$

$$\begin{aligned} g_4 = {} & w_1^3x_2^4 + w_1^3x_2^2x_1^6 + w_1^3x_2x_1^2 + w_1^3x_1^5 + w_1^2x_2^4x_1 + w_1^2x_2^2x_1^7 + w_1^2x_2x_1^3 + w_1^2x_1^6 \\ & + w_1x_2^7 + w_1x_2^6x_1^3 + w_1x_2^3x_1^5 + w_1x_2x_1^4 + x_2^7x_1 + x_2^6x_1^4 + x_2^5 + x_2^4x_1^3 \\ & + x_2x_1^5 + x_1; \end{aligned}$$

$$\begin{aligned} g_5 &= w_1^7 + 1; \\ g_6 &= \mathbf{z_2}(x_2^7x_1^7 + x_2^7 + x_1^7 + 1); \\ g_7 &= \mathbf{z_2}(w_1^3x_1^7 + w_1^3 + w_1x_2^3x_1^7 + w_1x_2^3 + x_2x_1^7 + x_2); \end{aligned}$$

$$\begin{aligned} g_8 = \mathbf{z_2}(& w_1^6x_2^3 + w_1z^6x_2^2x_1^3 + w_1^6x_1^2 + w_1^5x_2^3x_1 + w_1^5x_2^2x_1^4 + w_1^5x_1^3 + w_1^4x_2^3x_1^2 \\ & + w_1^4x_2^2x_1^5 + w_1^4x_1^4 + w_1^3x_2^3x_1^3 + w_1^3x_2^2x_1^6 + w_1^3x_1^5 + w_1^2x_2^3x_1^4 + w_1^2x_2^2 \\ & + w_1^2x_1^6 + w_1x_2^3x_1^5 + w_1x_2^2x_1 + w_1x_1^7 + x_2^5x_1^7 + x_2^5 + x_2^3x_1^6 + x_2^2x_1^2 + x_1); \end{aligned}$$

$$\begin{aligned} g_9 = \mathbf{z_2^2} + \mathbf{z_2}(& w_1^6x_1^2 + w_1^5x_2 + w_1^4x_1^4 + w_1^3x_2^2x_1^6 + w_1^3x_2x_1^2 + w_1^3x_1^5 + w_1^2x_2^4x_1 \\ & + w_1^2x_2^2x_1^7 + w_1^2x_2^2 + w_1^2x_2x_1^3 + w_1^2x_1^6 + w_1x_2^5x_1^6 + w_1x_2x_1^4 + w_1x_1^7 \\ & + x_2^7x_1 + x_2^6x_1^4 + x_2^5 + x_2^4x_1^3 + x_2x_1^5 + x_1) + (w_1^6x_2 + w_1^6x_1^3 + w_1^5x_2x_1 \\ & + w_1^5x_1^4 + w_1^4x_2^2x_1^6 + w_1^4x_2x_1^2 + w_1^3x_2x_1^3 + w_1^3x_1^6 + w_1^2x_2^5x_1^6 + w_1^2x_2^2x_1 \\ & + w_1^2x_2x_1^4 + w_1^2x_1^7 + w_1x_2^4x_1^3 + w_1x_2^3x_1^6 + w_1x_2x_1^5 + w_1x_1 \\ & + x_2^7x_1^2 + x_2^6x_1^5 + x_2^5x_1 + x_2^4x_1^4); \end{aligned}$$

$$\begin{aligned}
g_{10} = {} & \mathbf{z_1} + z_2 + w_1^6x_1^2 + w_1^5x_2 + w_1^4x_1^4 + w_1^3x_2^2x_1^6 + w_1^3x_2x_1^2 + w_1^3x_1^5 + w_1^2x_2^4x_1 \\
& + w_1^2x_2^2x_1^7 + w_1^2x_2^2 + w_1^2x_2x_1^3 + w_1^2x_1^6 + w_1x_2^5x_1^6 + w_1x_2x_1^4 + w_1x_1^7 \\
& + x_2^7x_1 + x_2^6x_1^4 + x_2^5 + x_2^4x_1^3 + x_2x_1^5 + x_1
\end{aligned}$$

$$\begin{aligned}
g_{11} = {} & \mathbf{u}_1 + w_1^6x_1 + w_1^5x_1^2 + w_1^4x_2 + w_1^3x_1^4 + w_1^2x_2^4 + w_1x_2^2 + x_2^7 \\
& + x_2^6x_1^3 + x_2^5x_1^6 + x_2^3x_1^5 + x_1^7.
\end{aligned}$$

Note that we have only one polynomial of degree 2 in G_2, but we have some polynomials of degree 1 in G_1. According to Theorem 7.7, g_9 is a general locator polynomial of type 1 for C, i.e.

$$\mathscr{L}_C^1(z) = z_2^2 + az_2 + b,$$

with

$$\begin{aligned}
a = {} & w_1^6x_1^2 + w_1^5x_2 + w_1^4x_1^4 + w_1^3x_2^2x_1^6 + w_1^3x_2x_1^2 + w_1^3x_1^5 + w_1^2x_2^4x_1 + w_1^2x_2^2x_1^7 \\
& + w_1^2x_2^2 + w_1^2x_2x_1^3 + w_1^2x_1^6 + w_1x_2^5x_1^6 + w_1x_2x_1^4 + w_1x_1^7 + x_2^7x_1 + x_2^6x_1^4 \\
& + x_2^5 + x_2^4x_1^3 + x_2x_1^5 + x_1,
\end{aligned}$$

$$\begin{aligned}
b = {} & w_1^6x_2 + w_1^6x_1^3 + w_1^5x_2x_1 + w_1^5x_1^4 + w_1^4x_2^2x_1^6 + w_1^4x_2x_1^2 + w_1^3x_2x_1^3 + w_1^3x_1^6 \\
& + w_1^2x_2^5x_1^6 + w_1^2x_2^2x_1 + w_1^2x_2x_1^4 + w_1^2x_1^7 + w_1x_2^4x_1^3 + w_1x_2^3x_1^6 + w_1x_2x_1^5 \\
& + w_1x_1 + x_2^7x_1^2 + x_2^6x_1^5 + x_2^5x_1 + x_2^4x_1^4.
\end{aligned}$$

If we apply Algorithm 8.4 we obtain

- given a correctable pair $(\mathbf{s}, \mathbf{w})$, we evaluate $A = a(\mathbf{s}, \mathbf{w})$ and $B = b(\mathbf{s}, \mathbf{w})$,

```
    **if** $B \neq 0$ **then** $\mu :=2$, $L(z) = z_2^2 + Az_2 + B$,
    **else if** $B = 0,\ A \neq 0$,
            **then** $\mu :=1$, $L(z) = z_2 + A$
```

Remark 8.6. If $\mu = 1$ then we obtain directly $z_2 = A$.

Remark 8.7. To calculate the erasure value u_1, we could use the polynomial $P_1 = g_{11}$, as explained in the discussion after Algorithm 8.4.

9. Computational remarks

In this paper we are interested in studying the structure of our syndrome ideal and in showing the existence of general error locator polynomials for cyclic codes. We are not concerned about complexity issues, which are deeply analyzed in [4]. Albeit our focus is not on the computational side, we feel committed to sketch some ideas, at least for the erasure free case.

There are two kinds of problems:

- the Gröbner basis of our ideal I_C requires a lot of time to be computed, even for small codes,

- even if we get the general error locator polynomial, it can be a polynomial composed of many monomials and so its use can give rise to a non-efficient decoding.

The first remark we would like to pose is that we do not need *a priori* to compute the Gröbner basis to get a general error locator polynomial $\mathscr{L}_C$ for C. As we have shown the existence of $\mathscr{L}_C$ (Theorem 6.9), we are allowed to seek it in any way we find convenient. For example, it is possible that $\mathscr{L}_C$ can be computed with some interpolation technique.

The second remark is that even if we have to compute the Gröbner basis, it could be that for some classes of codes it turns out to be an easy task, exploiting some extra algebraic conditions (a similar approach can be found in [17] for the determination of the distance of cyclic codes using the syndrome variety).

Suppose now that we have got, somehow, the general error locator polynomial for C. It could be that $\mathscr{L}_C$ is a huge polynomial, making it apparently infeasible for decoding. We would like to make two comments on this apparently bad situation:

- the polynomial $\mathscr{L}_C$ cannot be really huge, because it is an element of the *reduced* Gröbner basis of our ideal; that means in particular that its coefficients (which are polynomials in the $\{x_i\}$) are reduced with respect to the ideal $(I_C)_X$ whose variety is composed by all correctable syndromes (and a Gröbner basis for that ideal is easily got taking all elements in G_X); this fact imposes some restrictions on the shape of $\mathscr{L}_C$;
- in [1], it is shown how the CRHT variety can be used in practice to get efficient decoding of cyclic codes also for medium length cyclic codes (up to $n = 512$ in the binary case); it is clear that similar methods can be adapted to our case, with possibly even more effect.

10. Further work

First, we would like to discuss the hypothesis $(n, q) = 1$, which we have enforced. This hypothesis is traditionally used in the context of cyclic code theory and is relaxed rarely (but see [23,5]). This guarantees in particular that the generator polynomial will be a simple polynomial. In effect, this condition is very helpful in defining the notion of “error location”. An error location is some power of an element α of $\mathbb{F}$, with α of order n. The condition $(n, q) = 1$ clearly implies the existence of such α. If we relax this hypothesis, we will need to redefine an *error location* in a way which does not lose its important properties. Further research in this direction is planned.

Second, we would like to note a detail of our definition of general error locator polynomial: the coefficients of $\mathscr{L}_C$ have to lie in $\mathbb{F}_q$ and not in $\mathbb{F}$. This is a strict condition. On the other hand, for *any* linear code, it is not difficult to prove the existence of a polynomial with a similar definition but with coefficients in the larger field. But this case is only important for codes like the Reed–Solomon codes, where the two fields coincide.

Last, we believe it is important to investigate other algebraic codes to see whether they admit a general error locator polynomial or not. The second author, with others, is investigating the cases of classical Goppa codes and of quasi-cyclic codes.

Acknowledgements

The authors are indebted to many people for suggestions and comments. We would like to mention Patrizia Gianni, Carlo Traverso (University of Pisa), Barry Trager (IBM), Teo Mora (University of Genoa), Patrick Fitzpatrick, Emmanuel Popovici (UCC Cork), Tom Hoeholdt (Technical University of Denmark) and Joachim Rosenthal (Notre Dame, US). The authors are particularly indebted to the anonymous referee.

The second author wishes to thank some of his students for their contribution, in particular Jennifer Manginelli. The first author would like to thank the second author (her supervisor).

A special thank to Marc Giusti, for the use of the computational cluster MEDICIS.

Appendix

This section is devoted to prove Lemma 5.2.

Lemma 5.2. *Let J be a* 0*-dimensional radical ideal in a polynomial ring* $\mathbb{K}[V_1, \dots, V_{\mathcal{N}}]$, *where* $\mathbb{K}$ *is any field and* $2 \leqslant \mathcal{N}$. *Let* $\mathtt{t}$ *be a natural number* $1 \leqslant \mathtt{t}$. *Let G be the lexicographic Gröbner basis of J*, $V_1 < \cdots < V_{\mathcal{N}}$, *and let* $\mathcal{D}$ *denote the maximal degree in* $V_{\mathcal{N}}$ *possessed by the polynomials in G. Let* $\mathcal{S}$ *be any set of* $\mathtt{j}$ *points in* $\mathbb{K}^{\mathcal{N}}$ *of the type* $\mathcal{S} = \{(s_1, \dots, s_{\mathcal{N}-1}, z_1), \dots, (s_1, \dots, s_{\mathcal{N}-1}, z_{\mathtt{j}})\}$, *where* $(s_1, \dots, s_{\mathcal{N}-1})$ *does not belong to the variety* $\mathcal{V}(J \cap \mathbb{K}[V_1, \dots, V_{\mathcal{N}-1}])$ *and* $\mathtt{j} \leqslant \mathtt{t}$. *Denote by J' the ideal formed by all polynomials in J vanishing on* $\mathcal{S}$. *Let G' be the lexicographic Gröbner basis of J' and let* $\mathcal{D}'$ *denote the maximal degree in* $V_{\mathcal{N}}$ *possessed by the polynomials in G'. Then*

- *J' is again radical,*
- *if* $\mathcal{D} \leqslant \mathtt{t}$, *then* $\mathcal{D}' \leqslant \mathtt{t}$.

We want to use Theorem 3.1 from [18]. Using their notation, we rephrase their result in the case

- $M = A = A^q = \mathbb{K}[V_1, \dots, V_{\mathcal{N}}]$,
- H is just the identity on $\mathbb{K}[V_1, \dots, V_{\mathcal{N}}]$,
- M_l and M_{l+1} are ideals in $\mathbb{K}[V_1, \dots, V_{\mathcal{N}}]$. For simplicity, we use M and N instead.

Theorem 10.1 (*O'Keeffe and Fitzpatrick [18]*). *Let* $M \supset N$ *be two ideals in* $\mathbb{K}[V_1, \dots, V_{\mathcal{N}}]$ *such that*:

- *there is a* $\mathbb{K}$*-linear map* $\theta_l : M \mapsto \mathbb{K}$ *s.t.* $ker(\theta_l) = N$,
- *there are* $\mathcal{N}$ *elements* $\{\beta_k\}$ *in* $\mathbb{K}$ *s.t.* $(V_k - \beta_k)M \subset N$.

Let $W = \{W[1], \dots, W[r]\}$ *be a strictly ordered Gröbner basis of M relative to a term order* $<$, *then a Gröbner basis W' of N can be constructed as follows*:

1. *compute* $\alpha_h = \theta_l(W[h])$, *for* $1 \leqslant h \leqslant r$,
2. *if* $\alpha_h = 0$ *for all* h, *then* $W' = W$,
3. *otherwise let* $h_\star$ *be the least h* s.t. $\alpha_h \neq 0$.

We then have $W' = W_1 \cup W_2 \cup W_3$, *with*

- $W_1 = \{W[h] \mid h < h_\star\}$,
- $W_2 = \{(V_k - \beta_k)W[h_\star] \mid 1 \leqslant k \leqslant \mathcal{N}\}$,
- $W_3 = \{W[h] - (\alpha_h/\alpha_{h_\star})W[h_\star] \mid h > h_\star\}$.

Theorem 10.1 says that the new Gröbner basis, if it is different from the old, is formed by some elements of the old, the shifts of a special element of the old, and the other elements of the old translated by a suitable multiple of the special element.

Remark 10.2. Let D be the maximal degree with respect to a variable V_i possessed by the polynomials in W. Let D' be the maximal degree with respect to the same variable V_i possessed by the polynomials in W'. Moving from W to W' can raise this degree (and so $D' = D + 1$) only if the special element $W[h_\star]$ is a polynomial with degree D in V_i, in fact:

- in W_1 nothing changes,
- in W_2 the polynomial $(V_i - \beta_i)W[h_\star]$ has degree in V_i obviously increased by 1 w.r.t. $W[h_\star]$,
- in W_3, for any $W[h]$ the degree in V_i cannot increase to a value higher than $\max(\deg_{V_i} W[h_\star], \deg_{V_i} W[h])$, which is clearly not greater than D.

We now proceed to the proof.

Proof of Lemma 5.2. The ideal J' is again radical, as J was radical and we are adding new points to its variety, with no multiplicity.

The Gröbner basis G can be decomposed into two parts $G = G_{\mathcal{N}-1} \sqcup G_{\mathcal{N}}$, so that $G_{\mathcal{N}-1} = G \cap \mathbb{K}[V_1, \ldots, V_{\mathcal{N}-1}]$ and $G_{\mathcal{N}} = G \backslash G_{\mathcal{N}-1}$. The polynomial set $G_{\mathcal{N}-1}$ is obviously the (lexicographic) Gröbner basis of the elimination ideal $J_{\mathcal{N}-1} = J \cap \mathbb{K}[V_1, \ldots, V_{\mathcal{N}-1}]$.

We want to apply Theorem 10.1 to the following nested ideals:

- $M_1 = J$,
- $M_2 = \{f \in M_1 \mid f(s_1, \ldots, s_{\mathcal{N}-1}, z_1) = 0\}$, $M_2 \subset M_1$,
- $\ldots,$
- $J' = M_{\mathrm{j}+1} = \{f \in M_{\mathrm{j}} \mid f(s_1, \ldots, s_{\mathcal{N}-1}, z_{\mathrm{j}}) = 0\}$, $M_{\mathrm{j}+1} \subset M_{\mathrm{j}}$.

We first consider M_1 and M_2. The map $\theta_1 : M_1 \mapsto \mathbb{K}$ is clearly the evaluation $\theta_1(f) = f(s_1, \ldots, s_{\mathcal{N}-1}, z_1)$ and the conditions $(V_k - \beta_k)M_1 \subset M_2$ are satisfied if we take $\beta_k = s_k$, for $1 \leqslant k \leqslant \mathcal{N} - 1$, and $\beta_{\mathcal{N}} = z_1$. So we can apply Theorem 10.1 directly, with $W = G$ and W' the Gröbner basis of M_2.

We claim that $W[h_\star]$ lies in $G_{\mathcal{N}-1}$. Otherwise, as all elements of $G_{\mathcal{N}-1}$ precede the other elements of G, we have $\theta_1(g) = 0$ for each $g \in G_{\mathcal{N}-1}$. This is equivalent to saying that $(s_1, \ldots, s_{\mathcal{N}-1})$ is a root of each element in $G_{\mathcal{N}-1}$ and then it is an element of the corresponding variety $\mathcal{V}(J_{\mathcal{N}-1})$, which contradicts the hypothesis.

As $g_1 = W[h_\star]$ lies in $G_{\mathcal{N}-1}$, the new Gröbner basis $G_2 = W'$ does not increase its maximum degree in the $V_{\mathcal{N}}$, unless it was zero, because of the adding of the polynomial $(V_{\mathcal{N}} - z_1)g_1$ (see Remark 10.2). So, the degree bound on W' will be $\max(1, D) \leqslant \mathtt{t}$. Let us call D_1 the new degree bound.

If $\mathtt{j} = 1$, we have finished. Otherwise, we consider M_2 and M_3. The map $\theta_2 : M_2 \mapsto \mathbb{K}$ is the evaluation $\theta_1(f) = f(s_1, \ldots, s_{\mathcal{N}-1}, z_2)$ and the conditions $(V_k - \beta_k)M_1 \subset M_2$ are satisfied if we take $\beta_k = s_k$, for $1 \leqslant k \leqslant \mathcal{N} - 1$, and $\beta_{\mathcal{N}} = z_2$. We can apply Theorem 10.1 directly, with $W = G_2$ and W' the Gröbner basis of M_3.

This time it is not guaranteed that $W[h_\star]$ lies in the portion of W having degree 0 (because we have removed g_1). If it happens, we can argue as before and we get the same result, i.e. the degree bound on W' will be $\max(1, D_1) \leqslant \mathtt{t}$.

Otherwise, we claim that there is at least an element in W of degree 1 in $V_{\mathcal{N}}$ which vanishes on $(s_1, \ldots, s_{\mathcal{N}-1}, z_2)$. Actually, the recently added polynomial $(V_{\mathcal{N}} - z_1)g_1$ will do. If $(V_{\mathcal{N}} - z_1)g_1(s_1, \ldots, s_{\mathcal{N}-1}, z_2) = 0$, then $g_1(s_1, \ldots, s_{\mathcal{N}-1})$ must be zero, as $z_1 \neq z_2$. But then we are again in the case where all g in G vanish on $(s_1, \ldots, s_{\mathcal{N}-1})$, which has been proved to be impossible.

Let $g_2 = W[h_\star]$. Then the new Gröbner basis $G_3 = W'$ does not increase its maximum degree in the $V_{\mathcal{N}}$, unless it was 1, because of the addition of the polynomial $(V_{\mathcal{N}} - z_2)g_2$ (see Remark 10.2). So, the degree bound on W' will be $\max(2, D_1) \leqslant \mathtt{t}$. Let us call D_2 the new degree bound.

Let us call D_l the degree bound on the Gröbner basis of M_{l+1}. It is clear that we can argument similarly in the other cases, showing that we never add polynomials in the bases with degree in $V_{\mathcal{N}}$ greater than l. In this way, we obtain that D_l is

$$\max(l, D_{l-1}) \leqslant \mathtt{t}\,.$$

As $D_{\mathtt{j}} = D'$ and $\mathtt{j} \leqslant \mathtt{t}$, we have finished.

Remark 10.3. This result could be deduced by the uniform geometric decomposition of the ideal, as independently shown in [11]. But our proofs are preferred because of their constructive nature.

References

[1] D. Augot, M. Bardet, J.-C. Faugere, Efficient decoding of cyclic codes above the correction capacity of the code using Gröbner bases, ISIT: IEEE International Symposium on Information Theory, 2003.

[2] R. Brualdi, W.C. Huffman, V. Pless, Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 649–754.

[3] M. Caboara, T. Mora, The Chen–Reed–Helleseth–Truong decoding algorithm and the Gianni–Kalkbrenner Gröbner shape theorem, Appl. Algeb. Eng. Commun. Comput. 13 (2002) 209–232.

[4] M. Caboara, T. Mora, E. Orsini, M. Sala, Fast decoding of cyclic codes via the syndrome variety, to appear.

[5] G. Castagnoli, J.L. Massey, P. Schoeller, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 337–342.

[6] X. Chen, I.S. Reed, T. Helleseth, K. Truong, Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance, IEEE Trans. Inform. Theory 40 (1994) 1654–1661.

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

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

[9] P. Fitzpatrick, On the key equation, IEEE Trans. Inform. Theory 41 (1995) 1290–1302.

[10] G.D. Forney Jr., On decoding BCH Codes, IEEE Trans. Inform. Theory 10 (1965) 549–557.

[11] E. Fortuna, P. Gianni, B. Trager, Structure of zero-dimensional ideals, to appear.

[12] P. Gianni, Properties of Gröbner bases under specialization, Lecture Notes in Computer Science, vol. 378, Springer, Berlin, Heidelberg, New York, 1989, pp. 293–297.

[13] M. Kalkbrenner, Solving system of algebraic equation using Gröbner bases, Lecture Notes in Computer Science, vol. 378, Springer, Berlin, Heidelberg, New York, 1989, pp. 282–292.

[14] S. Lin, E.J. Weldon Jr., Long BCH codes are bad, Inform. Control 11 (4) (1967) 445–451.

[15] P. Loustaunau, E.V. York, On the decoding of cyclic codes using Gröbner bases, Appl. Algeb. Eng. Commun. Comput. 8 (6) (1997) 469–483.

[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[17] T. Mora, M. Sala, On the Gröbner bases for some symmetric systems and their application to coding theory, J. Scientific Comput. 35 (2003) 177–194.

[18] H. O'Keeffe, P. Fitzpatrick, Gröbner basis solution of constrained interpolation problems, Lin. Alg. Appl., 2002, 533–551.

[19] W.W. Peterson, E.J. Weldon Jr., Error Correcting Codes, MIT Press, Cambridge, MA, 1972.

[20] M. Sala, Gröbner bases and distance of cyclic codes, Appl. Algeb. Eng. Commun. Comput. 13 (2) (2002) 137–162.

[21] M. Sala, A Gröbner basis technique to compute distance and weight distribution of cyclic codes and their shortened codes, BCRI Preprint Series, No. 10, 2003.

[22] M. Sala, General error locator polynomials for linear codes, to appear.

[23] J.H. Van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 343–345.