AAECC manuscript No.
(will be inserted by the editor)

HELP: a sparse error locator polynomial for BCH codes

Michela Ceria · Teo Mora · Massimiliano Sala

Received: date / Accepted: date

Abstract In 1990 Cooper suggested to use Groebner bases' computations to decode cyclic codes and his idea gave rise to many research papers. In particular, as proved by Sala-Orsini, once defined the polynomial ring whose variables are the syndromes, the locations and the error values and considered the syndrome ideal, only *one* polynomial of a lexicographical Groebner basis for such ideal is necessary to decode (the general error locator polynomial, a.k.a. GELP). The decoding procedure only consists in evaluating this polynomial in the syndromes and computing its roots: the roots are indeed the error locations. A possible bottleneck in this procedure may be the evaluation part, since *a priori* the GELP may be dense.
In this paper, focusing on binary cyclic codes with length $n = 2^m - 1$, correcting up to two errors, we give a *Groebner-free, sparse* analog of the GELP, the *half error locator polynomial* (HELP). In particular, we show that it is *not necessary* to compute the whole Groebner basis for getting such kind of locator polynomial and we construct the HELP, studying the quotient algebra of the polynomial ring modulo the syndrome ideal by a combinatorial point of view. The HELP turns out to be computable with quadratic complexity and it has *linear growth* in the length n of the code: $O\left(\frac{n+1}{2}\right)$.

Keywords Cyclic codes · Syndrome variety · Locator polynomial

Mathematics Subject Classification (2010) 94B35 · 94B15 · 05E40 · 13P10

This research has been partially funded by INdAM - Istituto Nazionale di Alta Matematica

M. Ceria
Department of Computer Science, University of Milan
Tel.: +39 0250316361
E-mail: michela.ceria@gmail.com

T. Mora
Department of Mathematics, University of Genoa
E-mail: 5919@unige.it

M. Sala
Department of Mathematics, University of Trento
E-mail: maxsalacodes@gmail.com

1 Introduction

The classical decoding of BCH codes $C \subset \mathbb{F}_q^n$, correcting up to t errors, is based on solving the so-called *key equation* [4]: $\sigma(x)S(x) \equiv \omega(x) \pmod{x^{2t}}$, where, denoted by $a \in \mathbb{F}_q[a] =: \mathbb{F}_{q^m}$ a primitive n^{th}-root of unity, we have $S(x) = \sum_{i=1}^{2t} s_i x^{i-1}$, where $s_i := \sum_{j=1}^{\mu} e_{\ell_j} a^{i\ell_j}$, is the syndrome polynomial associated to the error $\sum_{j=1}^{\mu} e_{\ell_j} a^{\ell_j}, \mu \leq t$, and $\sigma(x) = \prod_{j=1}^{\mu}(1 - xa^{\ell_j})$ is the classical error locator polynomial.
In 1990 Cooper [19,20] suggested to use Groebner bases' computations for binary cyclic codes' decoding: let C be a binary BCH code, correcting up to t errors, and $\bar{s} = (s_1, \ldots, s_{2t})$ be the syndrome vector associated to a received word. Cooper's idea consisted in interpreting the error locations $z_1, \ldots z_t$ of C as the roots of the syndrome equation system:

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

Therefore, the plain error locator polynomial was seen as the monic generator $g(z_1)$ of the principal ideal

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

which was computed via the elimination property of lexicographical Groebner bases. In a series of papers [16–18] Chen et al. improved and generalized Cooper's approach to decoding, according to two different research paths. The first, related to the Groebner basis computation of the ideal generated by the Newton identities inspired [2,3]. In the second, they considered [17] the *syndrome variety* (Definition 3)

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

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

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

a series of polynomials $g_\mu(x_1, \ldots, x_{n-k}, Z), \mu \leq t$, such that, for any error with weight μ and associated syndromes $s_1, \ldots, s_{n-k} \in \mathbb{F}_{q^m}$, $g_\mu(s_1, \ldots, s_{n-k}, Z)$ in $\mathbb{F}_{q^m}[Z]$ is the plain error locator polynomial. This approach was improved in a series of paper [5, 27] culminating with [32] which, specializing Gianni-Kalkbrener Theorem [22,24], stated Theorem 6 below. For a survey of this *Cooper Philosophy* see [30] and on Sala-Orsini locator [6].

Recently the same problem has been reconsidered within the frame of *Grobner-free Solving* [28,35,34], explicitly expressed and sponsored in the book [33, Vol.3,40.12,41.15]; such approach aims to avoid the computation of a Groebner basis of a (0-dimensional) ideal $J \subset \mathcal{P}$ in favour of combinatorial algorithms, describing instead the structure of the algebra $\mathcal{P}/J$. In particular, given a finite set of distinct points $\mathbf{X} = \{P_1, ..., P_N\}$ and, for each point P_i the related primary q_i described via suitable functionals $\{\ell_{i1}, \ldots, \ell_{ir_i}\}$, the aim is to describe the combinatorial structure of both the ideal $\mathsf{I} = \cap_i \mathsf{q}_i$ and the *algebra* $\mathbb{F}[\mathbf{N}(\mathsf{I})] = \mathcal{P} \setminus \mathsf{I}$ avoiding Buchberger Algorithm and Groebner bases of I and

even Buchberger reduction modulo I, in favour of combinatorial algorithms, as variations of Cerlienco-Mureddu Algorithm [8,9,13–15,21] and Lundqvist interpolation formula [28], dealing with $\mathbb{F}[\mathbf{N}(\mathsf{I})]$ and $\{\ell_{ij}, 1 \le i \le N, 1 \le j \le r_i\}$.
In this paper, we focus on the case of a binary cyclic code C with primary defining set $\{1, l\}$, correcting up to two errors. In particular, starting from its syndrome variety, we first study the structure of the quotient algebra (Section 4) and then, we use this information in order to define the *half error locator polynomial* (Section 5, Definition 12), a sparse and efficient polynomial that, evaluated in the syndromes of the received word, gives as roots the corresponding error locations. A constructive proof of existence is given in Section 6.1, while a discussion on future works is given in Section 7.

2 Notation

Throughout this paper we mainly follow the notation of [33].
We denote by $\mathcal{P} := \mathbf{k}[x_1, ..., x_n]$ the ring of polynomials in n variables with coefficients in the field $\mathbf{k}$. The *semigroup of terms*, generated by the set $\{x_1, ..., x_n\}$ is:

$$\mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \mid \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}.$$

If $t = x_1^{\gamma_1} \cdots x_n^{\gamma_n}$, then $\deg(t) = \sum_{i=1}^n \gamma_i$ is the *degree* of t and, for each $h \in \{1, ..., n\}$ $\deg_h(t) := \gamma_h$ is the *h-degree* of t.
A *semigroup ordering* $<$ on $\mathcal{T}$ is a total ordering such that

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

Once we have fixed a semigroup ordering $<$ on $\mathcal{T}$, a polynomial $f \in \mathcal{P}$ can be represented as a linear combination of terms arranged w.r.t. $<$, where the coefficients are in the base field $\mathbf{k}$:

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

The term $\mathsf{T}(f) := t_1$ is the *leading term* of f, while $Lc(f) := c(f, t_1)$ is the *leading coefficient* of f and $tail(f) := f - c(f, \mathsf{T}(f))\mathsf{T}(f)$ is the *tail* of f.
A *term ordering* is a semigroup ordering such that 1 is lower than every variable or, equivalently, it is a *well ordering*.
The *lexicographical ordering* induced by $x_1 < ... < x_n$, i.e:

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

which is a term ordering, is the one we use in all the paper. We drop the subscript and denote it by $<$ instead of $<_{Lex}$, since no other ordering is employed and there is no possibility of confusion.
A subset $J \subseteq \mathcal{T}$ is a *semigroup ideal* if $t \in J \Rightarrow st \in J,\ \forall s \in \mathcal{T}$; a subset $\mathsf{N} \subseteq \mathcal{T}$ is an *order ideal* if $t \in \mathsf{N} \Rightarrow s \in \mathsf{N}\, \forall s | t$. We have that $\mathsf{N} \subseteq \mathcal{T}$ is an order ideal if and only if $\mathcal{T} \setminus \mathsf{N} = J$ is a semigroup ideal.

Given a semigroup ideal $J \subset \mathcal{T}$ we define $\mathsf{N}(J) := \mathcal{T} \setminus J$. The minimal set of generators $\mathsf{G}(J)$ of J is called the *monomial basis* of J. For all subsets $G \subset \mathcal{P}$, $\mathsf{T}\{G\} := \{\mathsf{T}(g),\ g \in G\}$ and $\mathsf{T}(G)$ is the semigroup ideal of leading terms defined as $\mathsf{T}(G) := \{t\mathsf{T}(g),\ t \in \mathcal{T}, g \in G\}$.
Fixed a term order $<$, for any ideal $I \triangleleft \mathcal{P}$ the monomial basis of the semigroup ideal $\mathsf{T}(I) = \mathsf{T}\{I\}$ is called *monomial basis* of I and denoted again by $\mathsf{G}(I)$ and the order ideal $\mathsf{N}(I) := \mathcal{T} \setminus \mathsf{T}(I)$ is called *Groebner escalier* of I.

Let $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ be a finite set of distinct points

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

The *ideal of points* of $\mathbf{X}$ is

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

Given a finite set of polynomials F, we call $I(F)$ the ideal generated by F.

For any (0-dimensional, radical) ideal $J \subset \mathcal{P}$ let $V(J)$ be the set of finite rational points of J over the algebraic closure of $\mathbf{k}$. We have the obvious duality between I and $V = V(I)$.

2.1 Cerlienco-Mureddu correspondence

In this section, we give a brief description of Cerlienco-Mureddu algorithm, introduced in [13–15]. This is the very first combinatorial algorithm that, given a finite set of distinct points $\mathbf{X} = \{P_1, ..., P_N\}$ finds the lexicographical Groebner escalier $\mathsf{N}(I(\mathbf{X}))$ for the ideal of points of $\mathbf{X}$.
In particular, in [13], the authors consider an *ordered* finite set of distinct points in $\mathbf{k}^n$, namely $\underline{\mathbf{X}} = [P_1, ..., P_N]$, and prove that there is a one-to-one correspondence between $\underline{\mathbf{X}}$ and the terms of the lexicographical Groebner escalier $\mathsf{N}(I(\mathbf{X}))$ of $I(\mathbf{X})$:

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

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

Their way to find Φ consists in using only combinatorics on the coordinates of the elements in $\mathbf{X}$. In particular, the only operations needed are comparisons among the coordinates of the points. The algorithm iterates on the points of $\mathbf{X}$ and it is recursive on the variables: it pays - due to recursion - the price of having a bad complexity: a straightforward implementation of the algorithm has complexity proportional to n^2N^2. The iterative algorithm developed in [9], gives the same result eliminating recursion and keeping iterativity on the points, via the introduction of a data structure (the Bar Code) that stores the information on the computed terms needed to perform the algorithm on the subsequent points, so the complexity turns out to be $O(N^2 \log(N)n)$.

2.2 Cyclic codes

In this section, we give a brief recap on cyclic codes, recalling all the standard notation which is needed to understand this paper.
Let C be an $[n,k,d]_q$ code that is, a q-ary cyclic code, where n represents its length, k the dimension and d the distance. The polynomial $g(x) \in \mathbb{F}_q[x]$ is its *generator polynomial*; we point out that $\deg(g) = n-k$ and $g \mid x^n - 1$. Let $\mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$.
If a denotes a primitive n-th root of unity, we call *complete defining set* of C the set

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

This set is completely partitioned in cyclotomic classes, so we can take one element for each such class and obtain a set $S \subset S_C$, which identifies uniquely the code C. This set S is a *primary defining set* of C. If we decide to consider some elements from each cyclotomic class, without caring to take them all, we talk more generally about a *defining set* of C.
If H is a parity-check matrix of C, $\mathbf{c}$ is a codeword (i.e. $c \in C$), $\mathbf{e} \in (\mathbb{F}_q)^n$ an error vector and $\mathbf{v} = \mathbf{c} + \mathbf{e}$ a received vector, the vector $\mathbf{s} \in (\mathbb{F}_{q^m})^{n-k}$ such that its transpose $\mathbf{s^T}$ is $\mathbf{s^T} = H\mathbf{v^T}$ is called *syndrome vector*. We call *correctable syndrome* a syndrome vector corresponding to an error of weight $\mu \leq t$, where t is the *error correction capability* of the code, namely the maximal number of errors that the code can correct. If the errors occur in positions $k_1, ..., k_\mu$, the *error locations* are defined to be $a^{k_1}, ..., a^{k_\mu}$. We call *error locator polynomial* a polynomial whose roots are the error locations.
Some special cyclic codes are the so called *BCH codes*; we define them since they will be treated in what follows as first simple examples, due to their particular structure (see [29] for more details).

Theorem 1 (BCH bound) *Consider an $[n,k,d]_q$ cyclic code C, with $GCD(n,q) = 1$ and defining set $S_C = \{i_1, ..., i_{n-k}\}$. Suppose there are $\delta - 1$ consecutive number in S_C, say $\{m_0 + i,\ 0 \leq i \leq \delta - 2\} \subset S_C$. Then $d \geq \delta$.*

Definition 2 *If C is the $[n,k,d]_q$ cyclic code, with defining set $S = \{m_0 + i,\ 0 \leq i \leq \delta - 2,\ m_0 \geq 0,\ m_0 + \delta - 2 \leq n-1\}$, then C is a* BCH code *of* designed distance δ.
A BCH code is narrow sense *if $m_0 = 1$ and* primitive *if $n = q^m - 1$.*

There are different methods to decode a BCH code. As an example, we can use the *extended Euclid algorithm*, the algorithm due to *Berlekamp-Massey* [4] or the so called *Cooper's philosophy*, which will be explained in next section.

3 Motivation: the decoding problem

In his papers [19,20], Cooper suggested to employ Groebner basis theory in order to decode cyclic codes. More precisely, he considers a primitive binary BCH code of length $n = 2^m - 1$. Let $a \in \mathbb{F}_{2^m}$ a primitive n-th root of unity and C our primitive BCH code over $\mathbb{F}_2$, with defining set $S_{C'} = \{2i+1,\ i = 0, ..., t-1\}$. The related complete defining set is the union $S_C = \bigcup_{i=0}^{t-1} C_{2i+1}$ of cyclotomic classes generated by $2i+1$,

$i = 0, ..., t-1$. Once received $\mathbf{v} \in (\mathbb{F}_2)^n$, the decoder computes the syndrome vector $\mathbf{s} = (s_0, ..., s_{2t-1}) \in (\mathbb{F}_{2^m})^{2t}$, in order to find the error locations a^j. We define new variables $z_1, ..., z_t$, standing for the t error locations, that are either a^{l_i}, $l_i \in \{1, ..., n\}$ or zero (when the $\mu < t$). Then, the error locations are a solution $(\xi_1, ..., \xi_t) \in (\mathbb{F}_{2^m})^t$ of a system of t polynomials over $\mathbb{F}_{2^m}[z_1, ..., z_t]$, i.e.

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

The problem for this nonlinear system is that sometimes is ineffective to compute its solutions, so Cooper proposes to use Groebner bases in this framework. In [17], Chen et al. generalize Cooper's idea to use Groebner bases techniques to binary cyclic codes.
In [16] Chen et al. generalize Cooper's philosophy to q-adic codes proposing a solution for decoding an error whose weight is assumed known.
Moreover, they give an alternative approach via Newton's identities in the binary case, but, since it goes beyond our interest, we do not treat it. For details, one can see [29]. For the improvements by Augot-Bardet-Faugère, one can see [2,3].
In the context defined so far, for any word to be decoded, we need to compute a Groebner basis and the syndromes are considered as parameters, computed expressively from the received word and substituted into the system. Moreover, different Groebner basis computations must be performed for different potential error weights, until the true weight of the actual error is obtained.
In [18], Chen et al. proposed a new method which consists of *considering the syndromes as variables x_i* and computing the Groebner basis as a preprocessing. The growth of the number of variables is a problem of this method. On the other hand, the Groebner basis is computed *only once*.
Following [29], we denote by $\mathbf{x}, \mathbf{y}, \mathbf{z}$ the multivariables representing, respectively, the syndromes, the locations and the error values, i.e. the variables for the polynomial ring
$\mathbb{F}_q[x_1, ..., x_{n-k}, z_t, ..., z_1, y_1, ..., y_t] = \mathbb{F}_q[\mathbf{x}, \mathbf{y}, \mathbf{z}]$.
Then, we consider

$$\mathcal{F}_{Chen2} := \left\{ \sum_{j=1}^{t} y_j z_j^i - x_i, \ i \in S \right\} \cup \{z_j^{n+1} - z_j, \ 1 \le j \le t\} \cup \{y_j^{2^m-1} - 1, \ 1 \le j \le t\} \subset \mathbb{F}_q[\mathbf{x}, \mathbf{y}, \mathbf{z}],$$

$I = I(\mathcal{F}_{Chen2}) \triangleleft \mathbb{F}_{q^m}[\mathbf{x}, \mathbf{y}, \mathbf{z}]$, $V(I) \subset (\mathbb{F}_{q^m})^{2\mu}$ and $\mathcal{G}$ the lexicographical reduced Groebner basis with $x_1 < ... < x_{n-k} < z_t < ... < z_1 < y_1 < ... < y_t$.

Definition 3 *The zerodimensional ideal I is the* syndrome ideal *and its variety $V(I)$ the* syndrome variety.

Loustaunau and York, in [27], improved the approach introduced by Chen. They suggested to use the FGLM algorithm to make the Groebner computation.
Caboara and Mora, in [5], gave a corrected and optimized version of Chen's algorithm, basing on the studies on the structure of Groebner bases for zerodimensional

ideals by Gianni [22] and Kalkbrenner [24], who stated Gianni- Kalkbrenner theorem.

We sketch now the improvements due to M.Sala and E.Orsini.
Consider the syndrome variety $V(I)$ defined by Caboara-Mora in [5] and a correctable syndrome $\mathbf{s} \in (\mathbb{F}_{q^m})^{n-k}$; there are some points in the variety that uniquely determine the potential error locations and error values, but, unfortunately, there are also points, called *spurious solutions* from now on, not corresponding directly to some error vector.

Definition 4 *[16, 32] A point $(s_1, \dots, s_{n-k}, y_1, \dots, y_t, z_1, \dots, z_t) \in V(I)$ is said* spurious *if there are at least two values z_i, z_j, $1 \le i \ne j \le \mu$, such that $z_i = z_j \ne 0$.*

M.Sala and E.Orsini propose a new syndrome variety eliminating these points. They consider an $[n, k, d]_q$ cyclic code with $GCD(q, n) = 1$ and give the following

Definition 5 *Let $n \in \mathbb{N}$ be an integer. We denote $p_{ll'} \in \mathbb{F}_q[z_1, ..., z_t]$ as*

$$p_{ll'} := \frac{z_l^n - z_{l'}^n}{z_l - z_{l'}},\ 1 \le l < l' \le t.$$

The syndrome ideal is $I = (\mathcal{F}_{OS})$ with

$$\mathcal{F}_{OS} = \{f_i, h - j, \chi_i, \lambda_j, z_{l'} z_l p_{ll'}, 1 \le l < l' \le t,\ 1 \le i \le n - j,\ j \in S\} \subset \mathbb{F}_q[\mathbf{x}, \mathbf{y}, \mathbf{z}]$$

with

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

If $Q := \mathbb{F}_q[x_1, ..., x_{n-k}]$, $\mathcal{G}$ is the usual reduced Groebner basis and for each $\iota = 1, ..., t$, for each l, $\mathcal{G}_\iota := \mathcal{G} \cap Q[z_t, ..., z_\iota]$, $\mathcal{G}_{\iota l} = \{g \in \mathcal{G}_\iota \setminus \mathcal{G}_{\iota+1},\ deg_\iota(g) = l\}$ and the polynomials are ordered such that their leading terms are ordered w.r.t. lex, then

Theorem 6 *It holds*

1. $\mathcal{G} \cap Q[z_1, ..., z_t] = \bigcup_{i=1}^{t} \mathcal{G}_i$;
2. $\mathcal{G}_i = \bigcup_{\delta=1}^{i} \mathcal{G}_{i\delta}$, $\mathcal{G}_{i\delta} \ne \emptyset$, $1 \le i \le t$, $1 \le \delta \le i$;
3. $\mathcal{G}_{ii} = \{g_{ii1}\}$, $1 \le i \le t$;
4. $\mathsf{T}(g_{ii1}) = z_i^i$, $Lp(g_{ii1}) = 1$;
5. *if* $1 \le i \le t$, $1 \le \delta \le i - 1$, *then* $\forall g \in \mathcal{G}_{i\delta}\ z_i \mid g$.

Let g_{tt1} the unique polynomial in $\mathcal{G}_t$ with $deg_{z_t}(g_{tt1}) = t$:

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

T.F.A.E., for each syndrome vector $s = (s_1, \dots, s_{n-k}) \in (\mathbb{F}_{q^m})^{n-k}$ corresponding to an error with weight bounded by t:

1. there are exactly μ errors $\zeta_1, \dots \zeta_\mu$;
2. $b_{t-l}(s) = 0$ for $l > \mu$ and $b_{t-\mu}(s) \neq 0$;
3. $g_{tt1}(s_1, \dots, s_{n-k}, z_t) = z^{t-\mu} \prod_{j=1}^{\mu}(z - \zeta_i)$.

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

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

It is called *general error locator polynomial* of C.

Theorem 7 ([36]) *Every cyclic code possesses a general error locator polynomial.*

Once we get a general error locator polynomial for C, the decoding algorithm only consists in evaluating it at the syndromes, so its efficiency depends on the sparsity of the involved general error locator polynomial.

There is no known theoretical general proof of the sparsity of general error locator polynomials, there are some experimental evidence, at least in the binary case. Some improvements to the algorithm have been given in [31]. In [37] is stated that

> *Actually*[1] *the number of monomials of $\mathcal{L}$ apparently grows linearly, since $|\mathcal{L}| \leq n$. We give some theoretical explanations for the sparsity of our polynomials, in all cases except two.*
> *A complete proof for all cases (any and any) seems far beyond our means, at present, but we plan to investigate more and more particular cases, hoping sooner or later to get the profound reason behind the sparsity, whose experimental evidence is apparent (at least in the binary case).*

Our paper makes some analysis on the topic, showing that furher improvements can be made, aiming to an efficient decoding procedure.

4 Degroebnerization: the Groebner escalier of the syndrome variety

The works on the general error locator polynomial (GELP) by Sala-Orsini, employ Groebner bases computation to get *one* polynomial they need for the decoding problem, namely the GELP. In other words, all the other polynomials in the Groebner basis computed by Orsini-Sala are useless for decoding.
A more recent research framework is the *Grobner-free Solving*, stated first in [35, 28] and explicitly expressed and sponsored in the book [33, Vol.3,40.12,41.15]. This approach aims to avoid the computation of a Groebner basis of a (0-dimensional) ideal $J \subset \mathcal{P}$ in favour of combinatorial algorithms describing instead the structure of the quotient algebra $\mathcal{P}/J$.
Our analysis places itself in this framework. Once deduced the structure of the quotient algebra via Cerlienco-Mureddu correspondence on the syndrome variety, it is possible to compute via interpolation the only polynomial needed for decoding, without passing through the whole Groebner basis computation. The consequence, for the case $t = 2$, is a preprocessing which is quadratic (and a decoding which is linear) on

[1] In the paper [37], $\mathcal{L}$ is the general error locator polynomials

the length of the code.
In this section, we study the structure of the lexicographical Groebner escalier for the syndrome ideal in the case of a code of length $n = 2^m - 1$ and primary defining set $S = \{1, l\}$ over $\mathbb{F}_{2^m}$. We consider the polynomial ring $\mathbb{F}_{2^m}[x_1, x_2, z_1, z_2]$, equipped with the lexicographical ordering induced by $x_1 < x_2 < z_1 < z_2$. In particular, we remark that the variable ordering is reversed with respect to that by Sala-Orsini [31, 32] and that the variables corresponding to the error values will not be used in this paper, because talking about error values in a binary code is redundant.
Before proving the particular shape of the structure of the lexicographical Groebner escalier for the syndrome ideal in our case, we state the following general

Lemma 8 *Let $\mathbf{X} = \{P_1, ..., P_N\}$ be a finite set of simple points in $\mathbf{k}^n$ and let d be the number of distinct elements in $\mathbf{k}$ that appear as first coordinate of some point in $\mathbf{X}$. Let $I(\mathbf{X}) \triangleleft \mathbf{k}[x_1, ..., x_n]$ be the ideal of points of $\mathbf{X}$ and $\mathsf{N}(\mathbf{X})$ its lexicographical Groebner escalier, supposing $x_1 < x_2 < ... < x_n$. Then it holds $1, x_1, x_1^2, ..., x_1^{d-1} \in \mathsf{N}(\mathbf{X})$.*

Proof The statement, which is a trivial consequence of Cerlienco-Mureddu correspondence [13], can be proved by induction on the number of points as well.

If $\tau \in \mathcal{T}$ is a term and $\mathsf{H} \subset \mathcal{T}$, we define

$$\tau\mathsf{H} := \{\tau\sigma,\ \sigma \in \mathsf{H}\}.$$

Theorem 9 *With the above notation, set $\mathsf{H} = \{1, x_1, ..., x_1^{q-2}\}$, where $q = n + 1 = 2^m$. The lexicographical Groebner escalier ($x_1 < x_2 < z_1 < z_2$) of the ideal $I = I(\mathbf{X})$ described as the ideal associated to $\mathbf{X} = \{(c + d, c^l + d^l, c, d),\ c, d \in \mathbb{F}_{2^m},\ c, \neq d\}$ has the form*

$$\mathsf{N}(I) = \mathsf{N}' \cup z_1\mathsf{N}',$$

where

$$\mathsf{N}' = \mathsf{H} \cup x_2\mathsf{H} \cup ... \cup x_2^{\frac{q}{2}-1}\mathsf{H}.$$

Proof Consider the set $\mathbf{X}$. If we fix $c, d \in \mathbb{F}_{2^m}$ and we consider the associated points

$$P_1 := (c + d, c^l + d^l, c, d),\ P_2 := (c + d, c^l + d^l, d, c),$$

clearly P_1, P_2 share the same first two coordinates so, by Cerlienco-Mureddu Correspondence we can partition $\mathbf{X}$ as $\mathbf{X} = \mathbf{X}_1 \sqcup \mathbf{X}_2$, such that if, for some $c, d \in \mathbb{F}_{2^m}$ $(c + d, c^l + d^l, c, d) \in \mathbf{X}_1$, necessarily $(c + d, c^l + d^l, d, c) \in \mathbf{X}_2$ and if $\mathsf{N}_1 = \mathsf{N}(I(\mathbf{X}_1))$ then $\mathsf{N} = \mathsf{N}(I(\mathbf{X}_1)) \cup z_1\mathsf{N}(I(\mathbf{X}_1))$. We restrict then to $\mathbf{X_1}$.
The assertion is proved by Cerlienco-Mureddu Correspondence if we can show that, among the points having the same first coordinate $c + d$, it is impossible that two points share also the second coordinate $c^l + d^l$, but since the first two coordinates are correctable syndromes, this is true since there is only one error vector corresponding to each correctable syndrome [23,29].

Now, by hypothesis, $c \neq d \in \mathbb{F}_{2^m}$ hence, clearly, $c + d \neq 0$; on the other hand, $\forall f \in \mathbb{F}_q^*$, $\forall c \in \mathbb{F}_q^*$, $c \neq f$, let $d = f - c$. We have $d \neq c$, $d \neq 0$ and $f = c + d$. Clearly it also holds $f = f + 0$. The above relations imply that the points in $\mathbf{X}_1$ have $(q - 1)$ different first coordinates $f = c + d$, so, by Cerlienco-Mureddu correspondence (see

Lemma 8), it must be $1, x_1, ..., x_1^{q-2} \in \mathsf{N}$.
Moreover, the pairs (c, d) such that $c + d = f \in \mathbb{F}_{2^m}^*$ are exactly $\frac{2^m-2}{2}$ if we impose $c, d \neq 0$. Since also $f + 0 = f$, we add the pair $(f, 0)$, obtaining that *there are* 2^{m-1} *distinct points for each first coordinate*.

If we identify each term $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{T}$ with its exponents' list $(\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ and we regards $(\alpha_1, ..., \alpha_n)$ as a point in the n-dimensional affine space, we can say that the escalier of ideal I, as proved in Theorem 9 has the shape of *two superimposed rectangles*.

Remark 10 *If we want to study the case in which* exactly two errors *occur, we should remove from the variety the points of the form*

$$(c, c^l, c, 0),\ (c, c^l, 0, c),$$

so the escalier becomes

$$\mathsf{N}(I) = \mathsf{N}' \cup z_1\mathsf{N}',$$

where $\mathsf{N}' = \mathsf{H} \cup x_2\mathsf{H} \cup ... \cup x_2^{\frac{q}{2}-2}\mathsf{H}$.
For an extensive study of the escalier associated to the syndrome varieties, both for $n = 2^m - 1$ *and for the case* $n \mid 2^m - 1$*, see [11]. The paper, indeed, examines all the possible cases and computes all the related escaliers.*

Example 1 Let us consider the case of $m = 3$, so the binary BCH code with $n = 7$ and $S = \{1, 3\}$. In this case the syndrome variety is $\mathbf{X} = \{(c + d, c^3 + d^3, c, d),\ c, d \in \mathbb{F}_8,\ c, \neq d\}$ and it has exactly $\binom{8}{2} = 56$ elements. The Groebner escalier $\mathsf{N}(I(\mathbf{X}))$ is given by $\mathsf{N}(I) = \mathsf{N}' \cup z_1\mathsf{N}'$, where $\mathsf{N}' = \mathsf{H} \cup x_2\mathsf{H} \cup ... \cup x_2^3\mathsf{H}$ and $\mathsf{H} = \{1, x_1, ..., x_1^6\}$, as shown in Figure 1.

5 HELP: Half Error Locator Polynomial

The particular shape of the escalier, shown in the previous Section 4, deeply influences the decoding procedure. To show it, we first recall Marinari-Mora's Theorem, that will constitute a tool for the construction of our locator polynomial.

Theorem 11 ([1,7], [33] II, Theorem 33.6.4) *Consider a zerodimensional radical ideal* $I \triangleleft \mathcal{P} := \mathbf{k}[x_1, ..., x_n]$*, fixing on* $\mathcal{P}$ *the lexicographical order* $<$*, induced by* $x_1 < ... < x_n$*. Denote by* $\mathsf{N}(I)$ *the associated (lexicographical) Groebner escalier and by* $\mathsf{G}(I) = \{\tau_1, ..., \tau_r\} \subset \mathcal{T}$*,* $\tau_i := x_1^{d_{i,1}} \cdots x_n^{d_{i,n}}$ *the monomial basis for the (lexicographical) semigroup ideal of leading terms* $\mathsf{T}(I)$*. Then, there exist polynomials*

$$\gamma_{m\delta i} = x_m - g_{m\delta i}(x_1, ..., x_{m-1}),$$

for each $i \in \{1, ..., r\}$*,* $m \in \{1, ..., n\}$ *and* $\delta \in \{1, ..., d_{i,m}\}$ *such that the products*

$$f_i = \prod_m \prod_\delta \gamma_{m\delta i},\ \ i = 1, ..., r$$

form a minimal Groebner basis of I*, with respect to* $<$*.*

Theorem 11 also provides a partition on the points in $\mathbf{X}$ for each polynomial f_i in the minimal Groebner basis, in perfect accordance with Cerlienco-Mureddu correspondence. Indeed, for each $f_i = \prod_m \prod_\delta \gamma_{m\delta i},\ i = 1, ..., r$, as many disjoint subsets of $\mathbf{X}$ as the factors $\gamma_{m\delta i}$ are provided:

$$\mathbf{X} = \bigsqcup_{m,\delta} \mathbf{X}_{m\delta i},\ i = 1, ..., r.$$

Each set $\mathbf{X}_{m\delta i}$ contains the elements in $\mathbf{X}$ such that the corresponding factor $\gamma_{m\delta i}$ vanishes on them. The factors $\gamma_{m\delta i}$, actually, are computed via interpolation on the points of $\mathbf{X}_{m\delta i}$, deduced for each factor using Cerlienco-Mureddu correspondence.

Since each point of the syndrome variety has the form $(c + d, c^l + d^l, c, d)$, the polynomial $z_1 + z_2 + x_1$ must appear in the lexicographical Groebner basis of $I(\mathbf{X})$. Therefore, we can say that $z_2 = z_1 + x_1$. This implies that, since $x_1 = c + d$ is known (it is the first syndrome), once one can recover the first error location $z_1 = c$, the second one - $z_2 = d$ - is easily and rapidly found. Therefore, we can concentrate in finding only $z_1 = c$.

The ideal $I(\mathbf{X})$ is by construction a zerodimensional radical ideal. Indeed it is the vanishing ideal of a finite set of points without any multiplicity. Therefore, its Groebner basis must contain one polynomial whose leading term is a *pure power* of a variable,

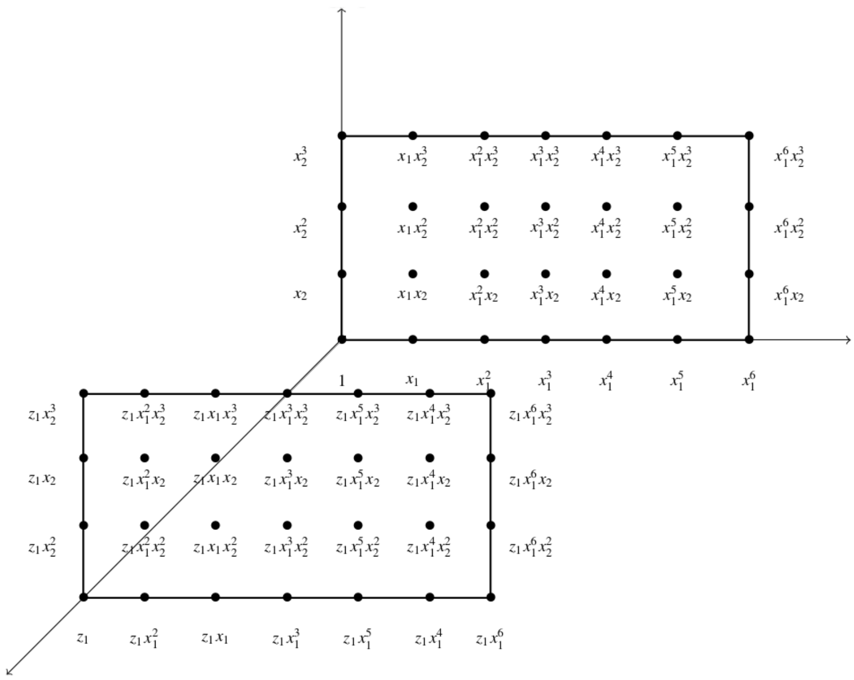

Fig. 1 Groebner escalier for the case in Example 1.

for each variable in the polynomial ring. Since the Groebner basis that we are considering is minimal, there must have only one polynomial of this shape for each variable. More precisely, the basis must contain a polynomial with leading term $x_1^{m_1}$, $x_2^{m_2}$, $z_1^{m_3}$, $z_2^{m_4}$, $m_1, m_2, m_3, m_4 \in \mathbb{N}$.
Due to the escalier's shape, proved in Theorem 9, the polynomial with leading term given by $z_1^{m_3}$, $m_3 \in \mathbb{N}$, must have $m_3 = 2$. Indeed, if $m_3 > 2$ then the term z_1^2 would be in the escalier, contradicting Theorem 9. Similarly (see also [11]), $m_1 = n$, $m_2 = \frac{n+1}{2}$ and $m_4 = 1$.
By Theorem 11, then, the polynomial f in the minimal Groebner basis, with $\mathsf{T}(f) = z_1^2$ can be decomposed in

$$f = F_c F_d = (z_1 + f_c(x_1, x_2))(z_1 + f_d(x_1, x_2)),$$

getting also the partition $\mathbf{X} = \mathbf{Z}_c \sqcup \mathbf{Z}_d$, $|\mathbf{Z}_c| = |\mathbf{Z}_d| = \frac{1}{2}|\mathbf{X}|$ such that

- F_c vanishes on $\mathbf{Z}_c$; F_d vanishes on $\mathbf{Z}_d$;
- $(x_1, x_2, z_1, z_2) \in \mathbf{Z}_c \Leftrightarrow (x_1, x_2, z_2, z_1) \in \mathbf{Z}_d$ (this last condition is a trivial consequence of Cerlienco-Mureddu correspondence).

This implies that, if we are able to recover the polynomial F_c (or, symmetrically, F_d) and we substitute the syndromes of the points in $\mathbf{Z}_c$ (or, symmetrically, Z_d) that are actually all the possible syndromes (remember that the elements in Z_c, Z_d differ only on the third and the fourth coordinates, namely on the error locations), then we recover c (or, symmetrically, d) and the remaining location to find is trivially recovered using the equation $z_1 + z_2 + x_1$.
These ideas lead to the definition of Half Error Locator Polynomial (HELP):

Definition 12 *With the above notation we call Half Error Locator Polynomial a polynomial*

$$\eta(x_1, x_2, z_1) := z_1 + h(x_1, x_2)$$

obtained as a factor of the linear factorization stated in Theorem 11 for the polynomial f in the minimal Groebner basis of $I(\mathbf{X})$ such that $\mathsf{T}(f) = z_1^2$.

Once the HELP is computed, the decoding problem can be translated in an easy substitution of the syndromes in this polynomial. Clearly, decoding becomes inefficient and expensive if the HELP is a dense polynomial. In the next section, we will show how to compute a sparse HELP for the case $n = 2^m - 1$, $S = \{1, l\}$.

6 Computing the HELP

As we have seen in Section 5, the set $\mathbf{X}$ can be partitioned as $\mathbf{X} = \mathbf{Z}_c \sqcup \mathbf{Z}_d$, $|\mathbf{Z}_c| = |\mathbf{Z}_d| = \frac{1}{2}|\mathbf{X}|$ such that

a. F_c vanishes on $\mathbf{Z}_c$; F_d vanishes on $\mathbf{Z}_d$;
b. $(x_1, x_2, z_1, z_2) \in \mathbf{Z}_c \Leftrightarrow (x_1, x_2, z_2, z_1) \in \mathbf{Z}_d$.

Looking at condition b., we see that we have to pick a point for each pair

$$\{(c + d, c^l + d^l, c, d), (c + d, c^l + d^l, d, c)\}.$$

The way we pick the point can influence the characteristics of the HELP we will find.

Example 2 Considering the binary BCH code with $n = 7$, $S = \{1, 3\}$, we can get with two different choices on the points the polynomials:

- $z_1 + a^3x_1^6x_2^2 + ax_1^5x_2^2 + a^6x_1^4x_2^2 + a^4x_1^3x_2^2 + x_1^2x_2^2 + x_1x_2^2 + a^5x_2^2 + a^6x_1^6x_2 + a^2x_1^4x_2 + x_1^3x_2 + a^5x_1^2x_2 + a^3x_1x_2 + ax_2 + a^6x_1^6 + a^4x_1^5 + a^2x_1^4 + x_1^3 + a^5x_1^2 + a$, corresponding to the partitioning set $\mathsf{Z} := \{(a, a, a^4, a^2), (a, a^2, a^5, a^6), (a, a^6, 1, a^3), (a^2, a^2, a, a^4), (a^2, a^4, a^5, a^3), (a^2, a^5, a^6, 1), (a^3, a^5, a^2, a^5), (a^3, 1, a^6, a^4), (a^3, a, 1, a), (a^4, a^4, a, a^2), (a^4, a, a^3, a^6), (a^4, a^3, 1, a^5), (a^5, a^6, a, a^6), (\mathbf{a^5}, \mathbf{1}, \mathbf{a^3}, \mathbf{a^2}), (a^5, a^4, a^4, 1), (a^6, a^2, a^2, 1), (a^6, a^3, a^3, a^4), (a^6, 1, a^5, a)(1, a^5, a^3, a), (1, a^6, a^4, a^5), , (1, a^3, a^6, a^2), (a, a, a^4, a^2), (a, a^2, a^5, a^6), (a, a^6, 1, a^3)\}$
- $z_1+a^6x_1^2x_2^2+a^4x_1^5x_2+a^3x_1$, corresponding to the partitioning set $\mathsf{Z} := \{(a, a, a^4, a^2), (a, a^2, a^5, a^6), (a, a^6, 1, a^3), (a^2, a^2, a, a^4), (a^2, a^4, a^5, a^3), (a^2, a^5, a^6, 1), (a^3, a^5, a^2, a^5), (a^3, 1, a^6, a^4), (a^3, a, 1, a), (a^4, a^4, a, a^2), (a^4, a, a^3, a^6), (a^4, a^3, 1, a^5), (a^5, a^6, a, a^6), (\mathbf{a^5}, \mathbf{1}, \mathbf{a^2}, \mathbf{a^3}), (a^5, a^4, a^4, 1), (a^6, a^2, a^2, 1), (a^6, a^3, a^3, a^4), (a^6, 1, a^5, a), (1, a^5, a^3, a), (1, a^6, a^4, a^5), (1, a^3, a^6, a^2), (a, a, a^4, a^2), (a, a^2, a^5, a^6), (a, a^6, 1, a^3)\}$

Note that in the two sets only the choice of the boldface point has been changed and the resulting HELP is completely different. Moreover, these two polynomials correct up to two errors but for the case of one error c, they return the value 0, so to compute c we need the second equation $z_2 = z_1 + x_1$, namely we have $x_1 = c$, $z_1 = 0$ and we have to compute c as second location: $z_2 = 0 + c$. We will see soon that we can compute sparse HELPs giving directly the error c in this case.

If we examine the sparsest polynomial in Example 2, we can notice that it obeys a very evident pattern. Imagine the terms to be placed in a chessboard indicized by the pure powers of x_1 and x_2 and consider the terms in these two variables appearing in the HELP $z_1 + a^6x_1^2x_2^2 + a^4x_1^5x_2 + a^3x_1$:

$$
\begin{array}{c|cccc}
x_1^6 & 0 & 0 & 0 & 0 \\
x_1^5 & 0 & a^4 & 0 & 0 \\
x_1^4 & 0 & 0 & 0 & 0 \\
x_1^3 & 0 & 0 & 0 & 0 \\
x_1^2 & 0 & 0 & a^6 & 0 \\
x_1 & a^3 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
\hline
 & 1 & x_2 & x_2^2 & x_2^3
\end{array}
$$

We can see that the terms are disposed in the chessboard as with a series of *knight moves* starting from x_1: each term is computed from the previous multiplying by the move $x_1^{-3}x_2$ (and keeping in mind that the exponents of x_1 are integers $\mod 7$, whereas x_2's exponents are integers $\mod 4$).
This drove us to thing that the general form for the HELP in the case $n = 2^m - 1$ $S = \{1, l\}$ could be conjectured to be

$$\eta(x_1, x_2, z_1) = z_1 + \sum_{i=1}^{\frac{n+1}{2}} a_i x_1^{(n+1-li) \mod n} x_2^{(i-1) \mod \frac{n+1}{2}},$$

where the coefficients $a_i \in \mathbb{F}_{2^m}$ are still to be determined.
We conjecture, moreover, that the HELP can be found performing Lagrange interpolation in the points with first coordinate $c + d = 1$ with $\frac{d}{c} = a^{2i+1}$ plus the point $(1, 1, 1, 0)$ in the terms t^i, $0 \leq i \leq 2^{m-1}$, where $t = x_1^{-l \mod n} x_2$ that is t is the knight gambit. It has the form $\eta(x_1, x_2, z_1) = z_1 + x_1 g(t)$, where $g(t)$ is the Lagrange interpolator.
Some HELPs have been found in this way. As an example, for the code with $n = 7$ and $S = \{1, 3\}$ over $\mathbb{F}_8$, the HELP is $z_1 + x_1(x_1^5 x_2^3 + a^2 x_1 x_2^2 + a^4 x_1^4 x_2 + a)$ and it has been found interpolating the points in the set $\{(1, a^5, a^3, a), (1, a^6, a^4, a^5), (1, a^3, a^6, a^2),$ $(1, 1, 1, 0)\}$ over the terms $1, x_1^4 x_2, x_1 x_2^2, x_1^5 x_2^3$. We display here the knight gambit:

$$\begin{array}{c|cccc}
x_1^6 & 0 & 0 & 0 & 1 \\
x_1^5 & 0 & a^4 & 0 & 0 \\
x_1^4 & 0 & 0 & 0 & 0 \\
x_1^3 & 0 & 0 & 0 & 0 \\
x_1^2 & 0 & 0 & a^2 & 0 \\
x_1 & a & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
\\
 & 1 & x_2 & x_2^2 & x_2^3
\end{array}$$

It is easy to verify that the HELP corrects up to two errors and that if only one error occurs it is directly returned as output by the HELP.

In the following subsection, we summarize the data we know on the problem and we conclude giving a constructive proof of existence for the HELP. In particular we prove our conjectures on its shape.

6.1 HELP exists and it can be found.

Our aim is to decode a binary cyclic code C over $\mathbb{F}_{2^m}$, length $n = 2^m - 1$ and *primary* defining set $S_C = \{1, l\}$.
We have the $n(n-1)$ *non spurious points* (namely points composed by non spurious syndromes and the corresponding errors)

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

or, equivalently, $\binom{n}{2}$ pairs

$$\Big\{\big(c + d, c^l + d^l, c, d\big), \big(c + d, c^l + d^l, d, c\big)\Big\}, c, d \in \mathbb{F}_{2^m}^*, c \neq d. \quad (1)$$

Moreover, we have to consider the n pairs of the form

$$\Big\{\big(c, c^l, c, 0\big), \big(c, c^l, 0, c\big)\Big\}, c \in \mathbb{F}_{2^m}^*, \quad (2)$$

which correspond to the occurrence of one single error. In total, we have $\binom{n+1}{2}$ pairs, corresponding to the occurrence of one or two errors.

Denoting by a any primitive element of $\mathbb{F}_{2^m}$ and setting $a^{-\infty} = 0$, we can represent these pairs as[2]

$$\left\{\left(c(1+a^{2i+1}), c^l(1+a^{2li+l}), c, a^{2i+1}c\right), \left(c(1+a^{2i+1}), c^l(1+a^{2li+l}), a^{2i+1}c, c\right), c \in \mathbb{F}^*_{2^m}\right\}, \quad (3)$$

$i \in \{0, ..., 2^{m-1} - 1\} \cup \{-\infty\}$.

setting $d/c := a^{2i+1}$ (in the case $d = 0, c \neq 0$, $a^{2i+1} = a^{-\infty}$).
HELP, by construction, is the polynomial $\eta(x_1, x_2, z_1) = z_1 + h(x_1, x_2)$ such that if h is evaluated at each of the $\binom{n+1}{2}$ points

$$\left(c(1+a^{2i+1}), c^l(1+a^{2li+l})\right), c \in \mathbb{F}^*_{2^m}, i \in \{0, ..., 2^{m-1} - 1\} \cup \{-\infty\} \quad (4)$$

returns the value c.

Theorem 13 *The Lagrange interpolator $g(t), deg(g) = 2^{m-1} + 1$, which returns $(1 + a^{2i+1})^{-1}$ when evaluated at each values*

$$t = (1+a^{2i+1})^{-l}(1+a^{2li+l}), i \in \{0, ..., 2^{m-1} - 1\} \cup \{-\infty\}, \quad (5)$$

gives a HELP, in the sense that, defined $h(x_1, x_2) = x_1 g(x_1^{-l} x_2)$, it holds

$$\eta(x_1, x_2, z_1) = z_1 + h(x_1, x_2) = z_1 + x_1 g(x_1^{-l} x_2).$$

Proof To prove that η is a HELP, we have to prove that, given a point

$$P = \left(c(1+a^{2i+1}), c^l(1+a^{2li+l})\right), c \in \mathbb{F}^*_{2^m}, i \in \{0, ..., 2^{m-1} - 1\} \cup \{-\infty\}$$

it holds $h(P) = c$.
Note that $x_1 = c(1 + a^{2i+1})$ implies $c = x_1(1 + a^{2i+1})^{-1}$ and

$$x_2 = c^l(1+a^{2li+l}) = x_1^l(1+a^{2i+1})^{-l}(1+a^{2li+l}). \quad (6)$$

Now, consider a point of the form $P = \left(c(1+a^{2i+1}), c^l(1+a^{2li+l}), c, a^{2i+1}c\right), c \in \mathbb{F}^*_{2^m}, i \in \{0, ..., 2^{m-1} - 1\} \cup \{-\infty\}$ and evaluate $h(P)$:

$$\begin{aligned} h(P) = h(x_1, x_2) &= x_1 g(x_1^{-l} x_2) = x_1 g(x_1^{-l} x_1^l (1+a^{2i+1})^{-l}(1+a^{2li+l})) \\ &= c(1+a^{2i+1})(1+a^{2i+1})^{-1} = c. \end{aligned}$$

This proves that η is a HELP.

Remark 14 *We point out that our HELP is consistent also with the case in which no errors occur, even if we do not consider the point $(0, 0, 0, 0)$ in our variety. Indeed, the HELP has shape $\eta(x_1, x_2, z_1) = z_1 + x_1 g(x_1, x_2)$. When no error occurs, we have $x_1 = 0$, leading to $\eta = z_1$, giving the only root $z_1 = 0$. Since then $z_2 = z_1 + x_1$, it holds $z_2 = 0 + 0 = 0$ and so we retrieve the two zero locations.*

[2] Indeed the last point has exponent $2i + 1 = 2(2^{m-1} - 1) + 1 = 2^m - 1 = n$. Note also that $|\{0, ..., 2^{m-1} - 1\} \cup \{-\infty\}| = 2^{m-1} + 1$.

7 Perspectives and works in progress

The examined case, with $n = 2^m - 1$ and $S = \{1, l\}$, is a particular case of the more general $n \mid 2^m - 1$ and $S = \{1, l\}$. In this more general case, the syndrome variety becomes

$$\mathbf{X} = \{(c + d, c^l + d^l, c, d),\ c, d \in \mathcal{R}_n,\ c, \neq d\},$$

where $\mathcal{R}_n$ is the set of n-th roots of unity over $\mathbb{F}_{2^m}$.
The escalier in the general case becomes a bit more complicated. Considering again the graphical representation described in Section 4, we can say that it is placed again on two totally symmetric superimposed planes, but the internal structure of every single plane is different. Indeed, each plane is formed by "stripes" of length n and height 1, corresponding to the cosets of the group R_n.
These stripes are posed in r columns depending on the Zech logarithm's structure [12]. We are studying this more general case in the works in progress [10, 11].

References

1. M.E. Alonso, M.G. Marinari, T. Mora, *The big Mother of all Dualities 2: Macaulay Bases*, Applicable Algebra in Engineering, Communication and Computing archive Vol. **17**, Issue 6, November 2006, 409–451.
2. D. Augot, M. Bardet, and J.-C. Faugère, *Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Groebner bases*, Proc. of ISIT 2003, 2003, 362.
3. D. Augot, M. Bardet, and J.-C. Faugère, *On formulas for decoding binary cyclic codes*, Proc. of ISIT 2007, 2007, 2646–2650.
4. E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill (1968)
5. M. Caboara, T. Mora *The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Groebner shape theorem*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 3, 209–232
6. F. Caruso, E. Orsini, C. Tinnirello and M. Sala *On the shape of the general error locator polynomial for cyclic codes* IEEE Transactions on Information Theory 63.6 (2017): 3641-3657.
7. M. Ceria, *A proof of the "Axis of Evil theorem" for distinct points*, Rendiconti del Seminario Matematico dell'Università e del Politecnico di Torino, Vol. 72 No. 3-4, pp. 213-233 (2014)
8. M. Ceria, *Bar Code for monomial ideals*, Journal of Symbolic Computation, Volume 91, March - April 2019, Pages 30-56.
9. M. Ceria, T. Mora *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game*, arXiv preprint, arXiv:1805.09165 [math.AC].
10. M. Ceria, *Half error locator polynomials for efficient decoding of binary cyclic codes*, in preparation.
11. M. Ceria, *Macaulay, Lazard and the Syndrome Variety*, arxiv preprint arXiv:1910.13189 [math.CO].
12. M. Ceria, T. Mora, M. Sala, *Zech tableaux as tools for sparse decoding*, submitted.
13. L. Cerlienco, M. Mureddu, *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* ≥ 2, Séminaire Lotharingien de Combinatoire 24 p. 39–76, 1990.
14. L. Cerlienco, M. Mureddu, *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. **139**, 73–87.
15. L. Cerlienco, M. Mureddu, *Multivariate Interpolation and Standard Bases for Macaulay Modules*, J. Algebra **251** (2002), 686–726.
16. X. Chen, I. S. Reed, T. Helleseth and T. K. Truong, *General principles for the algebraic decoding of cyclic codes*, EEE Trans. on Inf. Th. **40** (1994a), 1661–1663.
17. X. Chen, I. S. Reed, T. Helleseth and T. K. Truong, *Use of Groebner bases to decode binary cyclic codes up to the true minimum distance*, IEEE Trans. on Inf. Th. **40** (1994c), no. 5, 1654–1661
18. X. Chen, I. S. Reed, T. Helleseth and T. K. Truong, *Algebraic decoding of cyclic codes: a polynomial ideal point of view*, Contemp. Math., Vol. **168**, Amer. Math. Soc., Providence, 1994b,
19. A.B. III Cooper, *Direct solution of BCH decoding equations*, Comm., Cont. and Sign. Proc. (1990), 281–286.

20. A.B. III Cooper, *Finding BCH error locator polynomials in one step*, Electronic Letters **27** (1991), no. 22, 2090–2091.
21. B. Felszeghy, B. Ráth, L. Rónyai, *The lex game and some applications*, J. Symbolic Computation **41**(2006), 663-681
22. P. Gianni, *Properties of Gröbner Bases under Specialization*, L. N. Comp. Sci. **378** (1987), 293–297, Springer.
23. W.C. Huffman, V. Pless, *Fundamentals of error-correcting codes.* Cambridge university press (2010).
24. M. Kalkbrenner, *Solving Systems of Algebraic Equations by Using Groebner Bases*, L. N. Comp. Sci. 378 (1987), pagg. 282-292, Springer.
25. M. Kalkbrenner, *On the stability of Gröbner Bases under specialization*, J. Symb. Comp. **24** (1997), 51–58
26. R. Lidl, H. Niederreiter, *Finite Fields*, Volume 20, Parte 1 Volume 20 di Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997
27. P. Loustaunau, E. V. York, *On the decoding of cyclic codes using Gröbner bases*, AAECC 8 (1997), no. 6, 469–483
28. S. Lundqvist, *Vector space bases associated to vanishing ideals of points*, Journal of Pure and Applied Algebra, 214(4), 309-321 (2010).
29. T, Mora, L. Perret, S. Sakata, M. Sala, C. Traverso, *Groebner Bases, Coding, and Cryptography*, Springer, 2009.
30. E. Orsini, T. Mora,. *Decoding cyclic codes: the Cooper Philosophy*. in M.Sala et al., *Groebner Bases, Coding, and Cryptography*. Springer (2009), 62–92
31. T. Mora, E. Orsini, M. Sala, *General error locator polynomials for binary cyclic codes with* $t \leq 2$ *and* $n < 63$, BCRI preprint, `www.bcri.ucc.ie` 43, UCC, Cork, Ireland, 2006.
32. E. Orsini, M. Sala, *Correcting errors and erasures via the syndrome variety*, J. Pure Appl. Algebra, **200** (2005), 191–226.
33. T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016).
34. T. Mora, *An FGLM-like algorithm for computing the radical of a zero-dimensional ideal.* Journal of Algebra and Its Applications, 17(01) (2018).
35. B. Mourrain *A New Criterion for Normal Form Algorithms*. In: Fossorier M., Imai H., Lin S., Poli A. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1999. Lecture Notes in Computer Science, vol 1719. Springer, Berlin, Heidelberg (1999)
36. E. Orsini and M. Sala, *Correcting errors and erasures via the syndrome variety*, J. Pure Appl. Algebra 200 (2005), 191–226.
37. E. Orsini and M. Sala, *General error locator polynomials for binary cyclic codes with* $t \leq 2$ *and* $n < 63$, IEEE Trans. on Inf. Th. 53 (2007), 1095–1107.
38. M. Sala, *Groebner basis techniques to compute weight distributions of shortened cyclic codes*, Journal of Algebra and Its Applications 6 (03), 403-414 (2007).