University of Trento

Department of Mathematics

Ph.D. in Mathematics
Ciclo XXV

On structure and decoding of Hermitian codes

Chiara Marcolla

Supervisor: Prof. Massimiliano Sala

Head of PhD School: Prof. Alberto Valli

April, 2013

University of Trento

Department of Mathematics

Ph.D. in Mathematics
Ciclo XXV

On structure and decoding of Hermitian codes

Ph.D.Thesis of: Chiara Marcolla

Supervisor: Prof. Massimiliano Sala

Head of PhD School: Prof. Alberto Valli

April, 2013

Contents

I Preliminaries **1**

1 Coding Theory **3**

1.1 An overview on error correcting codes 3

1.2 Linear codes 4

1.2.1 Basic definitions 4

1.2.2 Decoding linear codes 6

1.2.3 Probability of the Undetected Error 8

1.3 Cyclic codes 9

1.3.1 An algebraic correspondence 9

1.3.2 Encoding and decoding with cyclic codes 12

2 Introduction to Gröbner bases **15**

2.1 Monomial ordering 15

2.2 Basic notions about ideals and Gröbner bases 18

2.3 Elimination Theory 24

3 Hermitian and Norm-Trace curves **27**

3.1 Known facts on Norm-Trace curve and Hermitian curve 27

3.2 Intersection between the Hermitian curve $\mathcal{H}$ and a line 28

3.3 Automorphisms of Hermitian curve 29

3.4 Automorphisms of Norm-Trace curve 30

4 Affine-variety codes **31**

4.1 Affine–variety codes 31

4.2 Norm-Trace codes and Hermitian codes 32

4.2.1 First results on words of given weight 33

4.3 The approach by Fitzgerald and Lax to decoding the affine-variety code 34

4.4 Base notion for decoding using our method 35

4.4.1 Stratified ideals 35

4.4.2 Root multiplicities and Hasse derivative 37

4.4.3 General error locator polynomials 38

5 The four phases of Hermitian codes **41**
5.1 Numerical semigroups 41
5.2 Analysing Hermitian codes using numerical semigroups 42
5.3 Phases intersections 46

II Main Results **53**

6 Intersections between the Hermitian curve $\mathcal{H}$ and parabolas **55**
6.1 Odd characteristic 58
6.1.1 Intersection between $\mathcal{H}$ and $y = ax^2 + c$ 58
6.1.2 Intersection between $\mathcal{H}$ and $y = ax^2 + bx + c$ 62
6.2 Even characteristic 68

7 Small-weight codewords of Hermitian codes **71**
7.1 Corner codes and edge codes 71
7.2 First results for the first phase 72
7.3 Minimum-weight codewords 74
7.4 Second-weight codewords 78
7.5 The complete investigation for $d = 3, 4$. 82
7.6 On the geometry of small weight codewords of AG codes 87

8 Decoding of affine-variety codes **95**
8.1 Decoding with ghost points 96
8.2 Weak locator polynomials 101
8.3 Results on some zero–dimensional ideals 110
8.4 Proof of Proposition 8.3.13 118
8.4.1 Preliminaries of proof 118
8.4.2 Sketch of proof 120
8.4.3 First part of the proof 121
8.4.4 Second part of proof 122
8.4.5 Third part of the proof 125
8.5 Multi-dimensional general error locator polynomials 127
8.6 Stuffed ideals 131
8.7 Families of affine–variety codes 135
8.7.1 SDG curves 135
8.7.2 SDG surfaces I 136
8.7.3 SDG surfaces II 137
8.7.4 Norm–trace curves 137

8.7.5 Hermitian curves 138

III Programs and Computations 141

9 Hermitian curve and Hermitian code 143

9.1 MAGMA programs to compute intersection between $\mathcal{H}$ and parabolas. 143

9.2 MAGMA programs to compute the number of minimum-weight words of Hermitian code. 148

9.3 Singular programs to compute the number of words of weight $d+1$. . 151

10 Decoding affine–variety code 155

10.1 Singular programs to find weak locators. 155

10.2 Singular programs to find the locators. 158

Bibliography 175

Introduction

Given a linear code, it is important both to identify fast decoding algorithms and to estimate the first terms of its weight distribution. Efficient decoding algorithms allow the exploitation of the code in practical situations, while the knowledge of the number of small-weight codewords allows to estimate its decoding performance. For affine-variety codes and its subclass formed by Hermitian codes, both problems are as yet unsolved. We investigate both and provide some solutions for special cases of interest.
The first problem is faced with use of the theory of Gröbner bases for zero-dimensional ideals.
The second problem deals in particular with small-weight codewords of high-rate Hermitian codes. We determine them by studying some geometrical properties of the Hermitian curve, specifically the intersection number of the curve with lines and parabolas.

This thesis is divided in two parts.

The first part contains preliminaries and known results except for some sections that contain original results, namely Section 3.4 where we find some automorphisms of Norm-Trace curve and Subsection 4.2.1 which is devoted to find a system that permits us to compute the number of words of a given weight. Finally in Section 5.3 we revisit the phases of Hermitian codes proposed by [HvLP98].
Known results include basic theory and notations of linear codes ([AE09],[HP03], [MS77]) and of Gröbner bases ([CLO07], [ST09]). Some material comes from the lecture notes of the course *Coding Theory* lectured by M. Sala and written by E. Bellini, D. Frapporti, O. Geil, M. Piva, M. Sala). In Chapter 4 we define the most important objects of this thesis, that is, the Affine-variety codes and Hermitian codes, explain the classical decoding and provide some preliminary results for our decoding method.

Part II contains our results. In particular, Chapter 6 and Chapter 7 describe our paper [MPS12], except for last section where we report our results in [FM11]. Chapter 8 comprises the results of our article [MOS12].

This part is organized as follows:

- In Chapter 6 the main result is Theorem 6.0.1, where we provide a complete classification of intersections between $\mathcal{H}$ and any parabola $y = ax^2 + bx + c$ ($a \neq 0$). The proof is divided in three main parts. In the first part of Chapter 6 we lay down some preliminary lemmas and we skecth our proving argument, that is, the use of the authomorphism group for $\mathcal{H}$. In Section 6.1 we deal with the odd-characteristic case and in Section 6.2 we deal with the even-characteristic case.

- In the beginning of Chapter 7 we analyse in depth the first-phase Hermitian codes (that is, codes such that $d \leq q$). We give our algebraic characterization in Section 7.2 and we use these results to completely classify geometrically the minimum-weight codewords for all first-phase codes in Section 7.3. In Section 7.4 we can count some special configurations of second-weight codewords for any first-phase code and finally in Section 7.5 we can count the exact number of second-weight codewords for the special case when $d = 3, 4$.

- In Chapter 8 we generalize the general error locator polynomials (that are polynomials introduced in [OS05] to decode cyclic codes) to cover also the multi-dimensional case and hence the affine-variety case. This chapter contains the following sections.

  - In Section 8.1 we introduce the notion of "ghost points", which are points added to the variety to play the role of non-valid error locations.
  - Using the definition of ghost point, in Section 8.2 we can define a first generalization of general error locator polynomials to the multivariate case (Definition 8.2.5), which provides a first decoding strategy. We also introduce evaluator polynomials (Definition 8.2.6) that permits a second strategy.
  - In Section 8.3 we study the "multi-dimensional case" of a stratified ideal, that is precisely the theoretical background that we need for any multivariate generalization of general locators. Unexpectedly, there is no obvious "natural" way to extend the core notion of stratified ideals. We present three generalizations in Definition 8.3.4 and Definition 8.3.5. We discuss their implications and provide some preliminary results. This section ends with the statement of Proposition 8.3.13, which is the main result claimed in this section (but not proved here). Proposition 8.3.13 is, in some sense, the multivariate analogue of Proposition 4.4.3 on stratified ideals.

- Section 8.4 is devoted to the long proof of Proposition 8.3.13. This proposition describes some features of the Gröbner basis of (the elimination ideals of) a zero-dimensional radical ideal J. The proof is constructive and relies on iterated applications of some versions of the Buchberger-Möller algorithm.
- Unfortunately, result in the multidimensional case, Proposition 8.3.13, is not as strong as our result in the one-variable case, Proposition 4.4.3. In Section 8.5, it does allow us to prove the existence of our first generalization of locators in Theorem 8.5.1, but we show that better locators can be found, as in Definition 8.5.2. We discuss with examples a new decoding strategy by applying these locators, but for the moment we are unable to prove their existence, since they use multiplicities. This will be done in the next section.
- In Section 8.6 we develop the theory for generalizing stratified ideals to the multivariate case with multiplicities.
  As usual, we are interested in suitable Gröbner bases of elimination ideals of some zero-dimensional ideals. First, we introduce the notion of *stuffed ideals* (Definition 8.6.1), which basically means that the roots of some polynomials in these Gröbner bases have the "expected" multiplicity. We give a constructive method ("stuffing") to obtain stuffed ideals from special classes of ideals (in particular, radical ideals will do). Our main results here are Theorem 8.6.4, that ensures that the desired shape of our Gröbner bases is unchanged under stuffing, and Theorem 8.6.6, that ensures the existence of our sought-after locators (in our Gröbner bases).
- In Section 8.7 we compute some examples from different families of affine-variety codes. In particular, we formally determine the shape for multivariate locator polynomials in the Hermitian case, for any $q \geq 2$ and $t = 2$ (Theorem 8.7.3), both in our weaker version and in our stronger version.

- In Chapter 9 we show how we computed specific examples and tested experimentally all our counting results.

An appendix with some explicit locators concludes this document.

Part I

Preliminaries

Coding Theory

In this chapter we summarize definitions and known results from [AE09, HP03, MS77].

We denote by $\mathbb{F}_q$ the field with q elements, where q is a power of a prime, and by $n \geq 1$ a natural number. Let $(\mathbb{F}_q)^n$ be the vector space of dimension n over $\mathbb{F}_q$. From now on, we denote by $\mathbb{K}$ any (not necessarily finite) field and by $\overline{\mathbb{K}}$ its algebraic closure.

1.1 An overview on error correcting codes

In 1948 Claude Shannon published a paper, *A mathematical theory of communication* [Sha48], that was the beginning of Coding Theory. In this paper Shannon defined a number Q called the *capacity of the channel* and proved that for any given degree of noise contamination of a communication channel, it is possible a communication nearly error-free up to Q.
This result guarantees that any data can be encoded before transmission so that the altered data can be decoded to the specified degree of accuracy. Hence the codes were invented to correct the errors that occur during the transmission. The basic idea of coding theory consists of adding some kind of redundancy to the message m which the *information source* A wants to send to a *destination* B.

In the Figure 1.1 the message m is encoded by the *encoder* into a *codeword* c and

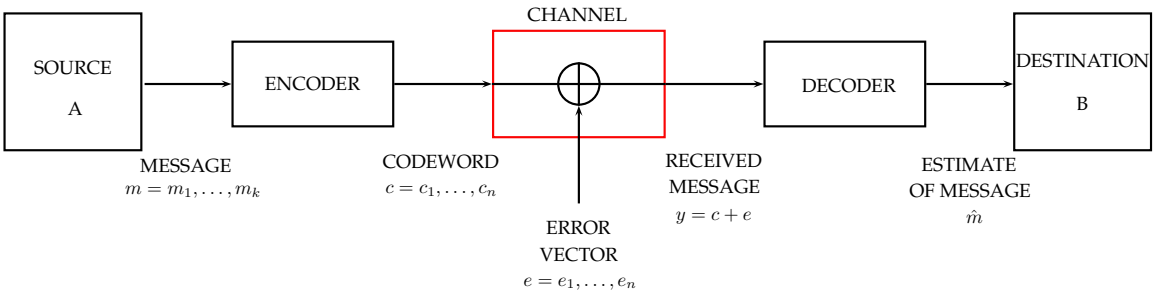


Figure 1.1: A communication schema

the information is sent through a *channel*. In this channel there is some interference (*noise*) and so a codeword c is changed to another vector $y = c + e$, where e is called

error vector. Finally the vector y is decoded using the *decoder*, but only if the occurred errors are not too many (in a sense that will be clear later), the receiver is able to recover the original message m.

In the next sections we will describe some basic concepts about coding theory considering the coding procedure as a linear function between vector spaces.

1.2 Linear codes

1.2.1 Basic definitions

Linear codes are widely studied because of their algebraic structure, which makes them easier to describe than non-linear codes.

Definition 1.2.1. *Let $k, n \in \mathbb{N}$ such that $1 \leq k \leq n$. A vector subspace of $(\mathbb{F}_q)^n$ of dimension k is a **linear code** C over $\mathbb{F}_q$ with length n and dimension k. An element of C is called a **word** of C.*

We indicate by $[n, k]_q$ a linear code over $\mathbb{F}_q$ with length n and dimension k and we call *binary code* a code over $\mathbb{F}_2$.

Note that if C is a linear code $[n, k]_q$, than C has q^k codewords.

Definition 1.2.2. *If C is an $[n, k]_q$ code, then any $k \times n$ matrix G whose rows form a basis for C is called a **generator matrix** for C.*

In general there are many generator matrices for a code. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an *information set* for C. The remaining $r = n - k$ coordinates forms a *redundancy set* and r is called the *redundancy* of C. If the first k coordinates form an information set, then C has a unique generator matrix $G = \big[I_k \mid A\big]$, where I_k is the $k \times k$ identity matrix. G is called a generator matrix in *standard form*.

Thanks to this algebraic description, to encode a message $m \in (\mathbb{F}_q)^k$ into the word $c \in (\mathbb{F}_q)^n$, it is sufficient to perform the matrix multiplication $mG = c$. When the generator matrix is in standard form $[I_k \mid A]$, m is encoded in $mG = (m, mA)$, where (x, y) denote the vector obtained by the concatenation of x and y. In this case the message m is formed by the first k components of the associated word. For this reason, the set formed by the first k columns of G is called information set and this type of encoding is called *systematic*.

Definition 1.2.3. *If C is an $[n,k]_q$ code, its **dual code** $C^\perp$ is the set of vectors orthogonal to all words of C:*

$$C^\perp = \{v \in (\mathbb{F}_q)^n \mid v \cdot c = 0, \forall c \in C\}.$$

Thus $C^\perp$ is an $[n, n-k]_q$ code.

A generator matrix of $C^\perp$ is called parity-check matrix of C.

Definition 1.2.4. *A **parity-check matrix** H for an $[n,k]_q$ code C is a generator matrix $(n-k) \times n$ for $C^\perp$.*

It is easy to see that C may be expressed as the null space of a parity-check matrix H, that is,

$$\forall x \in (\mathbb{F}_q)^n, \;\; Hx^T = 0 \iff x \in C.$$

Theorem 1.2.5. *If $G = \begin{bmatrix} I_k \mid A \end{bmatrix}$ is a generator matrix for the $[n,k]_q$ code C in standard form, then $H = \begin{bmatrix} A^T \mid I_{n-k} \end{bmatrix}$ is a parity check matrix for C*

Proof. See Theorem 1.2.1 of [HP03]. □

For any two vectors $x, y \in (\mathbb{F}_q)^n$, we define the *(Hamming) distance* $d(x,y)$ between x and y as the number of coordinates in which x and y differ.
Whereas, the *(Hamming) weight* $\mathrm{w}(x)$ of a vector $x \in (\mathbb{F}_q)^n$ is the number of its nonzero coordinates, that is,

$$\mathrm{w}(x) = d(x, 0).$$

Definition 1.2.6. *The **distance of a code** C is the smallest distance between distinct words, that is,*

$$d(C) = \min\{d(c_i, c_j) \mid c_i, c_j \in C, c_i \neq c_j\}.$$

If we know the distance $d = d(C)$ of an $[n,k]_q$ code, then we can refer to the code as an $[n,k,d]_q$ code.
It is simple to prove that following proposition.

Proposition 1.2.7. *Let C be a $[n,k,d]_q$ code, then*

$$d(C) = \min\{\mathrm{w}(c) \mid c \in C, \; c \neq 0\}.$$

Definition 1.2.8. *Let C be an $[n,k,d]_q$ code and let A_i be the number of codewords having weight i. The **weight distribution** of C is the sequence $\{A_i\}$ with $1 \leq i \leq n$. If for any i, $A_i = A_{n-i}$, then we have a **symmetric weight distribution**.*

It is simple to prove the following proposition.

Proposition 1.2.9. *Let C be an $[n,k,d]_q$ code and let H be a parity-check matrix of C. If H has w linearly dependent columns, then exists a codeword in C of weight less than or equal to w. As a consequence, if any subset of r columns of H is linearly independent, then $d(C) \geq r+1$.*

An immediate consequence of the previous proposition is an upper bound on the distance of a code in terms of the length and the dimension.

Proposition 1.2.10 (Singleton Bound)**.** *Let C be an $[n,k,d]_q$ code, then*

$$d \leq n-k+1.$$

A code achieving this bound is called *maximum distance separable* (*MDS*).
Finally, we define a *subcode* of a code C as a subspace of C.

1.2.2 Decoding linear codes

The distance of a code C is important to determine both the *error correction capability* of C, that is, the number of errors that the code can correct and its *error detection capability*, that is, the number of errors that the code can detect. In fact, we can see the noise as a perturbation that moves a word into some other vector. If the distance between the words is large, there is a low probability that the noise can move a codeword near to another one. To be more precise, we have the following theorem.

Theorem 1.2.11. *Let C be an $[n,k,d]_q$ code, then C has detection capability $d-1$ and it has correction capability $t = \lfloor \frac{d-1}{2} \rfloor$.*

Proof. See Theorem 1.11.4 of [HP03] or Theorem 2 of §3 of [MS77, 1]. □

Let $c \in C$ be the word transmitted and let $y \in (\mathbb{F}_q)^n$ be the vector received, then $e = y - c$ is the *error vector*. If we apply the parity-check matrix H to y, we get:

$$Hy^T = H(c+e)^T = He^T = s.$$

Definition 1.2.12. *The elements in $(\mathbb{F}_q)^{n-k}$, $s = Hy^T$, are called* ***syndromes****. We say that s is the syndrome corresponding to y.*

Note that if we transmit another word and the same error e occurs, we get the same syndrome. So the syndrome does not depend on the specific word sent, but only on the occurred error e.
We define a *coset* as the affine subspace associated to the vector subspace C, that is,

$$a + C = \{a + c \mid c \in C\} \text{ with } a \in (\mathbb{F}_q)^n.$$

Note that $(\mathbb{F}_q)^n$ can be partitioned into q^{n-k} cosets of size q^k.
Two vectors $a, b \in (\mathbb{F}_q)^n$ belong to the same coset if and only if $a - b \in C$. The following fact is just a reformulation of our arguments.

Theorem 1.2.13. *Let C be an $[n, k, d]_q$ code. Two vectors $a, b \in (\mathbb{F}_q)^n$ are in the same coset if and only if they have the same syndrome.*

Proof. Let $a, b \in (\mathbb{F}_q)^n$. Then a, b belong to the same coset if and only if

$$a - b \in C \iff H(a-b)^T = 0 \iff Ha^T = Hb^T.$$

□

Definition 1.2.14. *Let C be an $[n, k, d]_q$ code. For any coset $a + C$ and any vector $v \in a + C$, we say that v is a **coset leader** if it is an element of minimum weight in the coset.*

Definition 1.2.15. *If s is a syndrome corresponding to an error e of weight $\mathrm{w}(e) \leq t$, then we say that s is a **correctable syndrome** and e a **correctable vector error**.*

Theorem 1.2.16 (Correctable syndrome)**.** *If no more than t errors occurred (i.e. $\mathrm{w}(e) \leq t$), then there exists only one error e corresponding to the correctable syndrome $s = He$ and e is the unique coset leader of $e + C$.*

Proof. See Corollary 1.11.3 of [HP03] □

We are ready to describe the decoding algorithm of linear codes, that is the decoding using standard array. The **standard array** is a matrix that contains the 2^n vectors of $(\mathbb{F}_q)^n$ ordered by coset. Then the complexity of the decoding procedure is exponential in terms of memory occupancy.
The decoding procedure is the following.

1. After receiving a vector $y \in (\mathbb{F}_q)^n$, compute the syndrome $s = Hy^T$.
2. Find z, a coset leader of the corresponding coset.
   This is equivalent to finding a vector e of smallest weight in the coset containing y such that $y - e \in C$.
3. The decoded word is $c = y - z$.
4. Recover the message m from c (in case of systematic encoding m consists of first k components of c).

In [BKvT99], [BMvT78] and [Var97] it is shown that the general decoding problem for linear codes and the general problem of finding the distance of a linear code are both NP-complete. This suggests that no algorithm exists that decodes linear codes in a polynomial time.

1.2.3 Probability of the Undetected Error

When decoding using the standard array, the error vector e chosen by the decoder is always one of the coset leaders. The decoding is correct if and only if the true error vector is the coset leader. That is, if $\mathrm{w}(e) > t$, then the decoder may make an error and the output is another codeword. The probability that the decoder output is the wrong codeword is called *Probability of the Undetected Error* (PUE) or *word error rate*.

We will define the PUE in a *q-ary symmetric channel*. That is,

Definition 1.2.17. *A* **q-ary symmetric channel** (**SC**) *is a channel which has the following properties:*

1. *the component of a transmitted word (that we call "symbol") can be changed only to another element of $\mathbb{F}_q$.*
2. *The probability that a symbol becomes another one is the same for all symbols.*
3. *The probability that a symbol changes during the transmission does not depend on its position.*
4. *If the i-th component is changed, then this fact does not affect the probability of change for the j-th components.*

To these channel properties it is usually added a *source property*, that is,

5. *all words are equally likely to be transmitted.*

Obviously, the q-ary SC is a model that rarely can describe real channels, but it permits a simpler construction of the theory. Now we are going to see in which way. Let p be the probability that the symbol 1 become 0 or vice-versa where $1 \leq p < 1/q$. Suppose that during the transmission occurs an error e. The probability that e is the vector $v \in (\mathbb{F}_q)^n$ of weight i is

$$Prob\{e = v\} = p^i(1-p)^{n-i}. \tag{1.1}$$

Hence, if the code C has weight distribution $\{A_i\}$ with $0 \leq i \leq n$, then by (1.1)

$$PUE = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}.$$

Note that if p is very low, then the PUE is more influenced by the small weight codewords.

1.3 Cyclic codes

1.3.1 An algebraic correspondence

Definition 1.3.1. *An $[n, k, d]_q$ linear code C is a* ***cyclic code*** *if the cyclic shift of a word is also a word, that is,*

$$(c_0, \ldots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

A powerful instrument to describe algebraic properties of cyclic codes is to represent codewords in polynomial form. Detail can be found in Chapter 4 of [HP03]. Here we report an informal introduction of some tools that we will use in Section 2.2.

Let $\mathbb{F}_q[x]$ be a polynomial ring. For any $f \in \mathbb{F}_q[x]$ we denote

$$\langle f \rangle = \{fg \mid g \in \mathbb{F}_q[x]\}$$

and we say that $\langle f \rangle$ is an *ideal*. We construct a bijective correspondence between the vectors $\mathbf{c} = (c_0, \ldots, c_{n-1})$ of $(\mathbb{F}_q)^n$ and the polynomials $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]$ of degree at most $n-1$.
Note that if $c(x)$ is a word, then the shift to the right of $c(x)$ is $xc(x) \mod x^n - 1$. This suggests that the words of cyclic codes can be represented as polynomials in a residue class ring $R = \mathbb{F}_q[x]/I$, where I is the ideal $I = \langle x^n - 1 \rangle$. So we can identify C with a subset of R and thus, with a slight abuse of notation, we can multiply elements of C with polynomials modulo $x^n - 1$

Knowing that $x^i \cdot c \in C$ for any $c \in C$, it is simple to prove the following theorem.

Theorem 1.3.2. *Let C be an $[n, k, d]_q$ code. Then C is cyclic if and only if C is an ideal of R.*

Let C be an $[n, k, d]_q$ cyclic code. It is easy to prove (see Theorem 4.2.1 and Corollary 4.2.2 of [HP03]) that there exists a unique monic polynomial g of minimal degree that generates C as an ideal of R. Moreover,

$$\text{if } C = \langle g \rangle \implies g \text{ divides } x^n - 1 \text{ in } \mathbb{F}_q[x] \text{ and its degree is } \deg(g) = n - k.$$

We call g the *generator polynomial* of C.
A generator matrix can easily be given by using the coefficients of the generator polynomial $g = \sum_{i=0}^{n-k} g_i x^i$:

$$G = \begin{pmatrix} g \\ xg \\ \vdots \\ x^k g \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-k-1} & g_{n-k} & 0 & 0 \\ \vdots & & \ddots & \vdots & & \ddots & \ddots \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix}.$$

Previous observations imply that cyclic codes of length n over $\mathbb{F}_q$ are generated by divisors of $x^n - 1$. Let

$$x^n - 1 = \prod_{j=1}^{s} f_j, \qquad f_j \text{ irreducible over } \mathbb{F}_q.$$

Then to any cyclic code of length n over $\mathbb{F}_q$ corresponds a subset of $\{f_j\}_{j=1}^{s}$. So, to find all cyclic codes, we have to find the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. Let us put ourselves in the case $x^n - 1$ has no repeated factors which is when q and n are relatively prime. To factorize $x^n - 1$ over $\mathbb{F}_q$, we need to find all zeros of $x^n - 1$ in some extension field $\mathbb{F}_{q^r}$, for some $r \in \mathbb{N}$. The smallest field containing $\mathbb{F}_q$ and to which these roots belong is called the *splitting field* of $x^n - 1$ over $\mathbb{F}_q$.

Theorem 1.3.3. *Let n, q be coprime. Let $\mathbb{F}_{q^r}$ be the splitting field of $x^n - 1$ over $\mathbb{F}_q$. Then exist $\alpha \in \mathbb{F}_{q^r}$ such that*

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

This element α is called ***primitive n-th root of unity****.*

Proof. See Theorem 4.1.1 of [HP03]. □

Note that (see Theorem 3.7.4. of [HP03]) if $f(x)$ is a polynomial in $\mathbb{F}_q[x]$ and if α is a root of $f(x)$ in some extension field $\mathbb{F}_{q^r}$, then:

1. $f(x^q) = f(x)^q$
2. α^q is also a root of $f(x) \in \mathbb{F}_q$.

Hence, in this case the generator polynomial of C has powers of α as roots.

Definition 1.3.4. *Let n, q be coprime. Let C be an $[n, k, d]_q$ cyclic code with generator polynomial g. The set:*

$$S_{C,\alpha} = S_C = \{i_1, \ldots, i_{n-k} \mid g(\alpha^{i_j}) = 0,\ j = 1, \ldots, n-k\}$$

is called the ***complete defining set*** *of C.*
The ***q-cyclotomic class*** *of i, or q-cyclotomic coset of i, is the set*

$$C_i = \{i, qi, \ldots, q^m i\},$$

where m is the smallest positive integer such that $i \equiv iq^m \mod n$.

So the complete defining set of a cyclic code is the collection of q-cyclotomic classes.

From now on we fix a primitive n-th root of unity α and we write $S_{C,\alpha} = S_C$. A cyclic code is defined by its complete defining set, since

$$C = \{c \in R \mid c(\alpha^i) = 0,\ i \in S_C\} \iff g = \prod_{i \in S_C} (x - \alpha^i).$$

By this fact it follows that

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

is a parity-check matrix (defined over $\mathbb{F}_{q^m}$) for C.
In fact, if $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, then $c(\alpha^h) = \sum_{i=0}^{n-1} c_i \alpha^{ih}$, so

$$Hc^T = \begin{pmatrix} c(\alpha^{i_1}) \\ c(\alpha^{i_2}) \\ \vdots \\ c(\alpha^{i_{n-k}}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \iff c \in C.$$

Remark 1.3.5. We note that, since S_C is partitioned into cyclotomic classes, there are some subsets S'_C of S_C (containing at least one element for each cyclotomic coset of S_C) any of them sufficient to specify the code unambiguously and we call any such S'_C a **defining set**.

Theorem 1.3.6 (BCH bound)**.** *Let C be an $[n, k, d]_q$ cyclic code with complete defining set $S_C = \{i_1, \ldots, i_{n-k}\}$ and let $(n, q) = 1$. Suppose there are $\delta - 1$ consecutive numbers in S_C, say $\{m_0, m_0 + 1, \ldots, m_0 + \delta - 2\} \subset S_C$. Then*

$$d \geq \delta.$$

Proof. See Theorem 4.5.3 of [HP03]. □

Now we are able to define two particular cyclic codes, *BCH codes* and *Reed Solomon codes.*

Definition 1.3.7. *Let C be the $[n, k, d]_q$ cyclic code with defining set $S = (m_0, m_0 + 1, \ldots, m_0 + \delta - 2)$ such that*

$$0 \leq m_0 \leq \cdots \leq m_0 + \delta - 2 \leq n - 1$$

*Then, C is a **BCH code** of **designed distance** δ. The BCH code is called **narrow sense** if $m_0 = 1$ and it is called **primitive** if $n = q^m - 1$.*

Example 1.3.8. We consider the polynomial $x^9 - 1$ over $\mathbb{F}_2$:

$$x^9 - 1 = \underset{\uparrow f_1}{(x+1)}\underset{\uparrow f_2}{(x^6 + x^3 + 1)}\underset{\uparrow f_3}{(x^2 + x + 1)}$$

Let C be the cyclic code generated by $g = f_1 \cdot f_2$. Let α a primitive n-th root of unity such that $f_2(\alpha) = 0$, then $S_C = \{0, 1, 2, 4, 5, 7, 8\}$. Hence C is a $[9, 2, d]$ code over $\mathbb{F}_2$ with S_C as defining set and so it is a BCH code of designed distance $\delta = 6$. The BCH bound ensures that the minimum distance is at least 6. On the other hand, the generator polynomial

$$g(x) = x^7 + x^6 + x^4 + x^3 + x + 1$$

has weight 6, so the distance is exactly $d = 6$.

Definition 1.3.9. *A* **Reed Solomon** *code over $\mathbb{F}_q$, denoted by $RS(k, n, \mathbb{F}_q)$, is a BCH code with length $n = q - 1$.*

Note that if $n = q-1$ then $x^n - 1$ splits into linear factors. If the designed distance is d, then the generator polynomial of a Reed Solomon code has the form

$$g(x) = (x - \alpha^{i_0})(x - \alpha^{i_0+1}) \cdots (x - \alpha^{i_0+d-1})$$

and $k = n - d + 1$. It follows that RS codes are MDS codes.

In Section 4.1 we will see the Reed-Solomon codes as affine-variety codes.

1.3.2 Encoding and decoding with cyclic codes

In this section we study the encoding and decoding of a message in the case of cyclic codes.

Let C be an $[n, k, d]_q$ cyclic code with generator polynomial g of degree $n-k$. We recall that C will correct at most $t = \lfloor \frac{d-1}{2} \rfloor$ errors.

Let $m = (m_0, \ldots, m_{k-1})$ be a message, we consider its polynomial representation $m(x)$ in the polynomial ring R. We can encode the message in two ways, the simpler is to multiply $m(x)$ by the generator polynomial $g(x)$:

$$c(x) = m(x)g(x) \in C.$$

The other procedure exploits the proprieties of R and it is used to obtain a systematic encoding. We have to multiply $m(x)$ by x^{n-k} and divide the result by g, obtaining:

$$m(x)x^{n-k} = q(x)g(x) + r(x)$$

where $\deg(r(x)) < \deg(g(x)) = n - k$. So the polynomial representation of the remainder is an $(n-k)$-vector. Joining the k-vector m with the $(n-k)$-vector r we obtain an n-vector c, that is

$$c(x) = m(x)x^{n-k} + r(x).$$

In this way, the message is formed by the last k components of the received word.
In the last case, to verify that some error occurred, it is sufficient to check if the remainder of the division by g of the received polynomial c is different from zero. This procedure to compute the reminder is called Meggitt Decoding Algorithm (see Section 4.6 of [HP03]).

Suppose that during the transmission an error e occurs with $\mathrm{w}(e) \leq t$. Then, the remainder of the division by g in the procedure above gives exactly the syndrome associated to e. We can find e using the standard array which is described in Subsection 1.2.2.

Introduction to Gröbner bases

In this chapter we will introduce some basic notions and known results from [CLO07] and [ST09]. Some material comes from the lecture notes of the course *Coding Theory* lectured by M. Sala and written by E. Bellini, D. Frapporti, O. Geil, M. Piva, M. Sala.

We denote by $\mathbb{F}_q$ the field with q elements, where q is a power of a prime. Let $n \geq 1$ be a natural number and let $(\mathbb{F}_q)^n$ be the vector space of dimension n over $\mathbb{F}_q$.
We denote by $\mathbb{K}$ any (not necessarily finite) field and by $\overline{\mathbb{K}}$ its algebraic closure.

2.1 Monomial ordering

A *monomial* in $x_1, \ldots, x_m$ is a product of the form

$$x_1^{\alpha_1} \cdot \ldots \cdot x_m^{\alpha_m}$$

where all of the exponents α_j are non negative integers. The sum $\alpha_1 + \ldots + \alpha_m$ is defined to be the *total degree* of this monomial. We denote by $\mathcal{M}(X) = \mathcal{M}$ the set of all monomials in the variables $x_1, \ldots, x_m$.

A *polynomial* f in $x_1, \ldots, x_m$ with coefficients in $\mathbb{K}$ is a finite linear combination of monomials. That is,

$$f = \sum_{\alpha} a_\alpha x^\alpha, \qquad a_\alpha \in \mathbb{K},$$

where $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_m^{\alpha_m}$ and the sum is over a finite number of m-uples $\alpha = (\alpha_1, \ldots, \alpha_m)$. Then we call a_α the *coefficient* of the monomial x^α and we denote by $\deg(f)$ the *total degree* of f which is the maximum $|\alpha| = \alpha_1 + \ldots + \alpha_m$ such that the coefficient a_α is nonzero.

Note that the sum and product of two polynomials is again a polynomial. It is simple to prove that under addition and multiplication, $\mathbb{K}[x_1, \ldots, x_m] = \mathbb{K}[X]$ satisfies all field axioms except for the existence of multiplicative inverses (since, for example, $1/x$ is not a polynomial). For this reason $\mathbb{K}[X]$, the set of all polynomials

in $x_1, \ldots, x_m$ with coefficients in $\mathbb{K}$, is called a *polynomial ring.*

Since a polynomial is a sum of monomials, we would like to be able to arrange the terms in a polynomial unambiguously in descending (or ascending) order. To do this, we have to define a *monomial ordering* $\prec$.

Definition 2.1.1. *A **monomial ordering** $\prec$ is a binary relation on $\mathcal{M}$ such that:*

1. $\forall\ m_1 \neq m_2 \in \mathcal{M}$, *either* $m_1 \prec m_2$ *or* $m_2 \prec m_1$.
   $\forall\ m_1, m_2, m_3 \in \mathcal{M}$, *if* $m_1 \prec m_2$ *and* $m_2 \prec m_3$, *then* $m_1 \prec m_3$.

2. $\forall\ m_1, m_2, m \in \mathcal{M}$ *if* $m_1 \prec m_2$ *then* $m_1 \cdot m \prec m_2 \cdot m$.

3. $\prec$ *is a well-ordering, i.e. every non-empty subset of* $\mathcal{M}$ *has a least element.*

Note that for every monomial ordering: $1 \prec m$.
Now that we have defined monomial ordering, we report some examples. We can suppose that $x_1 \succ \ldots \succ x_m$ and let $m_1, m_2 \in \mathcal{M}$ such that $m_1 = x_1^{\alpha_1} \cdot \ldots \cdot x_m^{\alpha_m}$ and $m_2 = x_1^{\beta_1} \cdot \ldots \cdot x_m^{\beta_m}$.

Lex that is a *lexicographic order.* We say that $m_1 \prec_{lex} m_2$ if there exists j such that $\alpha_j < \beta_j$ and $\alpha_i = \beta_i$ for $1 \leq i < j \leq m$.

Example 2.1.2. Let $\mathcal{M} = \mathcal{M}[x, y, z]$ and $x \succ y \succ z$. Then

$$x^2 \succ y^4 \text{ and } x^2yz^3 \succ xy^4z.$$

GrLex that is a *graded lexicographic order* and it is also call *total lexicographic order.* We say that $m_1 \prec_{GrL} m_2$ if $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and $m_1 \prec_{lex} m_2$.

Example 2.1.3. Let $\mathcal{M} = \mathcal{M}[x, y, z]$ and $x \succ y \succ z$. Then

$$x^2 \prec y^4 \text{ and } x^2yz^3 \succ xy^4z.$$

DegRevLex that is a *graded reverse lexicographic order.* To say that $m_1 \prec_{DRL} m_2$, first of all we compare their total degrees: if $|\alpha| < |\beta|$ then $m_1 \prec_{DRL} m_2$, otherwise we have to compare the total degree of $n_1 = x_1^{\alpha_1} \cdot \ldots \cdot x_{m-1}^{\alpha_{m-1}}$ and $n_2 = x_1^{\beta_1} \cdot \ldots \cdot x_{m-1}^{\beta_{m-1}}$, and so on.

Example 2.1.4. Let $\mathcal{M} = \mathcal{M}[x, y, z]$ and $x \succ y \succ z$. Then

$$x^2 \prec y^4 \text{ and } x^2yz^3 \prec xy^4z \text{ since } x^2y \prec xy^4.$$

Note that DegRevLex is the same to reverse the lexicographic order, that is, $m_1 \prec_{DRL} m_2$ if there exists j that $\alpha_j > \beta_j$ and $\alpha_j = \beta_j$ for $1 \leq j < i \leq m$.

Weighted Degree. We assign a weight $w_i \in \mathbb{N}^*$ to each variable x_i and we denote by $\mathrm{w}(m_1) = \sum_i \alpha_i w_i$ and by $\mathrm{w}(m_2) = \sum_i \beta_i w_i$. We say that $m_1 \prec_w m_2$ if either $\mathrm{w}(m_1) < \mathrm{w}(m_2)$ or $\mathrm{w}(m_1) = \mathrm{w}(m_2)$ and $m_1 \prec_{lex} m_2$.

Example 2.1.5. Let $\mathcal{M} = \mathcal{M}[x, y, z]$ and $x \succ y \succ z$. We assign the weight to each variables $w_x = 2$, $w_y = 1$ $w_z = 3$. Then

$$x^2 \prec y^4 \text{ and } x^2yz^3 \succ xy^4z.$$

Block Order. Let $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_r\}$ be two variable sets. Let $\prec_X$ and $\prec_Y$ be two orders, on the monomials of X and on the monomials of Y, respectively. That is m_1, m_2 as previous and $n_1 = y_1^{\gamma_1} \cdot \ldots \cdot y_r^{\gamma_r}$ and $n_1 = y_1^{\delta_1} \cdot \ldots \cdot y_r^{\delta_r}$. Let $<$ as $(\prec_X, \prec_Y)$ a *block order* on the monomials of $X \cup Y$. We say that $m_1 n_1 < m_2 n_2$ if $n_1 \prec_Y n_2$ or if $n_1 = n_2$ and $m_1 \prec_X m_2$. The definition of a block order for more variable sets is a direct generalization.

Example 2.1.6. Let $\mathcal{M} = \mathcal{M}[x_1, x_2, y_1, y_2, y_3]$ and let $<= (\prec_{lex}, \prec_{GrL})$ and $x_1 \succ x_2 \succ y_1 \succ y_2 \succ y_3$. Then

$$x_1^2 \prec x_2y_3^2 \text{ and } x_1y_1y_2^3 \succ x_2^3y_1y_2^3 \text{ since } x_1 \succ x_2^3.$$

We will use the following terminology.

Definition 2.1.7. *Let $\Omega \in \mathbb{N}^m$. Let $f = \sum_{\alpha \in \Omega} a_\alpha x^\alpha$ be a non zero polynomial in $\mathbb{K}[X]$ and let $\prec$ be a monomial ordering. We say that x^β is the **leading monomial** of f if $x^\beta \succ x^\alpha$ for all $\alpha \neq \beta$ such that $\alpha \in \Omega$ and it is denoted by $lm(f) = x^\beta$. We denote by $\mathbf{T}(f) = a_\beta x^\beta$ the **leading term** of f and by $lc(f) = a_\beta$ the **leading coefficient** of f.*

Using a monomial ordering, it can be proven that the leading monomial, the leading term and the leading coefficient of f are well defined and unique.

Example 2.1.8. Let $f = 4x^2y + xy^3z + 5z$ in $\mathbb{R}[x, y, z]$ and let $\succ_{lex}$ be a lex order. Then $lm(f) = x^2y$, $lc(f) = 4$ and $\mathbf{T}(f) = 4x^2y$.

2.2 Basic notions about ideals and Gröbner bases

In this section we consider the ideals and the classic results of these algebraic objects.

Definition 2.2.1. *A subset $I \subset \mathbb{K}[X]$ is an **ideal** if*

1. $0 \in I$.
2. *If $f, g \in I$ then $f + g \in I$.*
3. *If $f \in I$ and $h \in \mathbb{K}[X]$ then $fh \in I$.*

Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[X]$. If

$$I = \Big\{ \sum_{i=1}^{s} \lambda_i f_i \mid \lambda_i \in \mathbb{K}[X] \Big\}$$

then I is *finitely generated* by $f_1, \ldots, f_s$ and it is denoted by $I = \langle f_1, \ldots, f_s \rangle$.

An ideal generated by one element is called a *principal ideal*.
A commutative ring A is a *Noetherian* ring if any ideal $I \subset A$ is finitely generated.

Definition 2.2.2. *We define a **semigroup ideal** T as a subset of $\mathcal{M}$ such that for all $t \in T$, $m \in \mathcal{M}$ we have $t \cdot m \in T$.*

Let $t_1, \ldots, t_k \in \mathcal{M}$ and set:

$$T = \bigcup_{i=1}^{k} \{\lambda t_i \mid \lambda \in \mathcal{M}\}.$$

Then T is a semigroup ideal of $\mathcal{M}$. We say that T is *generated* by $\{t_1, \ldots, t_k\}$ and we write $T = \langle t_1, \ldots, t_k \rangle$.

Lemma 2.2.3. *Let $M \subset \mathcal{M}$ and $I = \langle m_i \mid m_i \in M \rangle$ be an ideal. Then a monomial m lies in I if and only if m is divisible by m_i for some $m_i \in M$.*

Proof. See Lemma 2 of chapter 2 of [CLO07, §4]. □

Theorem 2.2.4 (Dickson's Lemma)**.** *Every semigroup ideal is generated by a finite set.*

Proof. See Theorem 5 of chapter 2 of [CLO07, §4]. □

In the previous section, we defined the leading term of $f \in I$. For any ideal I, we can define its *ideal of leading terms* $\mathbf{T}(I)$ as the set of leading terms of elements of I. That is,

$$\mathbf{T}(I) = \{\lambda m \mid \text{ there exists } f \in I \text{ with } \mathbf{T}(f) = \lambda m\}.$$

And we denote by $\langle \mathbf{T}(I) \rangle$ the ideal generated by the elements of $\mathbf{T}(I)$.
In a similar way we can define the *ideal of leading monomials* of I, that is,

$$lm(I) = \{lm(f) \mid f \in I\} \subset \mathcal{M}.$$

It is clear that $lm(I)$ is a semigroup ideal.

Note that, if $I = \langle f_1, \ldots, f_k \rangle$, then $\langle \mathbf{T}(f_1), \ldots, \mathbf{T}(f_k) \rangle \subseteq \langle \mathbf{T}(I) \rangle$, but these two ideals may be different and it is the same for $lm(I)$.

Example 2.2.5. Let $I = \langle f_1, f_2 \rangle$ where $f_1 = x^2 - x$ and $f_2 = xy - y + 1$. We use lexicographic ordering on the monomials in $\mathbb{K}[x, y]$. Then $xf_2 - yf_1 = x$, so $x \in I$. Thus $x = \mathbf{T}(x) \in \langle \mathbf{T}(I) \rangle$ but x is not divisible by $\mathbf{T}(f_1) = x^2$ or $\mathbf{T}(f_2) = xy$. Hence, by Lemma 2.2.3, $x \notin \langle \mathbf{T}(f_1), \mathbf{T}(f_2) \rangle$.

Proposition 2.2.6. *Let $I \subset \mathbb{K}[X]$ be an ideal. Then $\langle \mathbf{T}(I) \rangle$ is a monomial ideal and there are $g_1, \ldots, g_k \in I$ such that $\langle \mathbf{T}(I) \rangle = \langle \mathbf{T}(g_1), \ldots, \mathbf{T}(g_k) \rangle$.*

Proof. See Proposition 3 of chapter 2 of [CLO07, §5]. □

Theorem 2.2.7 (Hilbert Basis Theorem)**.** *Any ideal $I \subset \mathbb{K}[X]$ has a finite generating set.*

Proof. See Theorem 4 of chapter 2 of [CLO07, §5]. □

We just noted, in Example 2.2.5, that not all bases $\{f_1, \ldots, f_k\}$ of an ideal I have the special property that $\langle \mathbf{T}(I) \rangle = \langle \mathbf{T}(f_1), \ldots, \mathbf{T}(f_k) \rangle$. Those bases for which the equality holds give rise to the following definition.

Definition 2.2.8. *Let I be an ideal and $\prec$ be a monomial ordering. We say that $\mathcal{G} = \{g_1, \ldots, g_k\}$ is a **Gröbner basis** for I if $\langle \mathbf{T}(I) \rangle = \langle \mathbf{T}(g_1), \ldots, \mathbf{T}(g_k) \rangle$. We denote by* $\mathrm{GB}(I)$.

Equivalently, $\mathcal{G}$ is a Gröbner basis of I if $\mathcal{G} \subseteq I$ and if for all $f \in I$ there exist $g_i \in \mathcal{G}$ such that $lm(g_i)$ divides $lm(f)$.

Theorem 2.2.9 (Buchberger Theorem)**.** *For every ideal $I \subseteq \mathbb{K}[X]$ and for every monomial ordering $\prec$ on $\mathcal{M}$, there exist a Gröbner basis $\mathcal{G}$ for I.*

Proof. See Corollary 6 of chapter 2 of [CLO07, §5]. □

Moreover, there exists an algorithm, that is, Buchberger algorithm [Buc06, Buc98] [CLO07, 2§7] that transforms any finite set of generators for I into a Gröbner basis.

Actually, Gröbner bases computed using the Buchberger algorithm are often bigger than necessary. We can eliminate some unneeded generators by using the following lemma.

Lemma 2.2.10. *Let $\mathcal{G}$ be a Gröbner basis for the polynomial ideal I. Let $g \in \mathcal{G}$ be a polynomial such that $\mathbf{T}(g) \in \langle \mathbf{T}(\mathcal{G} \backslash \{g\}) \rangle$. Then $\mathcal{G} \backslash \{g\}$ is also a Gröbner basis for I.*

Proof. See Lemma 3 of chapter 2 of [CLO07, §7]. □

Because of Lemma 2.2.10, we can define a *minimal Gröbner basis* for $I \subseteq \mathbb{K}[X]$ as a Gröbner basis $\mathcal{G}$ for I such that for all $g \in \mathcal{G}$ we have that $lc(g) = 1$ and $\mathbf{T}(g) \notin \langle \mathbf{T}(\mathcal{G} \backslash \{g\}) \rangle$.
Unfortunately, a given ideal I may have many minimal Gröbner bases. But we can define a *special* minimal basis, that we call a *reduced basis*. In this way to any ideal we can associate a unique basis.

Definition 2.2.11. *Let $\mathcal{G} = \{g_1, \ldots, g_k\}$ be a Gröbner basis for I. We say that $\mathcal{G}$ is* ***reduced*** *if for all $g \in \mathcal{G}$, $lc(g) = 1$ and no monomial of g divides $\mathbf{T}(g_i)$ where $g_i \neq g$ and $g_i \in \mathcal{G}$.*

Proposition 2.2.12. *Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Gröbner basis.*

Proof. See Proposition 6 of chapter 2 of [CLO07, §7]. □

For any ideal I in a polynomial ring $\mathbb{K}[X]$, $X = \{x_1, \ldots, x_m\}$, we denote by $\mathcal{V}(I)$ the *variety of* I in $\overline{\mathbb{K}}$, that is the set of all zeros of I in $\overline{\mathbb{K}}$

$$\mathcal{V}(I) = \{P \in \overline{\mathbb{K}}^m \mid f(P) = 0 \quad \forall\, f \in I\}.$$

Theorem 2.2.13. *Let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal in $\mathbb{K}[X]$ and let $P \in \overline{\mathbb{K}}^m$. Then*

$$f_1(P) = \ldots = f_k(P) = 0 \iff g(P) = 0 \quad \forall\, g \in I.$$

Proof. See Proposition 9 of chapter 2 of [CLO07, §5]. □

Definition 2.2.14. *Let I be an ideal. If the cardinality of $\mathcal{V}(I)$ is finite, then I is called a* 0***-dimensional ideal****.*

Theorem 2.2.15 (The Weak Nullstellensatz)**.** *Let $\overline{\mathbb{K}}$ be an algebraically closed field and let $I \subseteq \mathbb{K}[X]$ be an ideal satisfying $\mathcal{V}(I) = \emptyset$. Then $I = \mathbb{K}[X]$.*

Proof. See Theorem 1 of chapter 4 of [CLO07, §2]. □

Definition 2.2.16. *For any $Z \subset \overline{\mathbb{K}}^m$ a set of points, we denote by $\mathcal{I}(Z)$ the* ***vanishing ideal*** *of Z, $\mathcal{I}(Z) \subset \mathbb{K}[X]$, that is, $\mathcal{I}(Z) = \{f \in \mathbb{K}[X] \mid f(P) = 0 \ \forall P \in Z\}$.*

Theorem 2.2.17 (Buchberger-Möller)**.** *Let Z be a finite set of points in $\mathbb{K}^m$. Let $\mathcal{G} = \{g_1, \ldots, g_k\}$ be a strictly ordered reduced Gröbner basis of $I = \mathcal{I}(Z)$, that is $lm(g_1) \prec \ldots \prec lm(g_k)$. Let $P = (p_1, \ldots, p_m)$ be a point that does not belong to Z, then a Gröbner basis for $I' = \mathcal{I}(Z \cup \{P\})$ is $\mathcal{G}' = G_1 \cup G_2 \cup G_3$, with*

- $G_1 = \{g \in \mathcal{G} \mid lm(g) \prec lm(g^*)\}$,
- $G_2 = \{(x_i - p_i)g^* \mid 1 \leq i \leq m\}$,
- $G_3 = \{g - \frac{g(P)}{g^*(P)} g^* \mid lm(g) \succ lm(g^*)\}$.

where g^* is the first polynomial in I such that does not vanish in P. That is, $g^*(P) \neq 0$ and $g(P) = 0$ for all $g \in \mathcal{G}$ such that $lm(g) \prec lm(g^*)$.

Proof. See [MB82, Mor09] or [CLO07, 2§7]. □

Definition 2.2.18. *Let I be an ideal in a polynomial ring $\mathbb{K}[X]$, the* ***radical of*** *I, denote by $\sqrt{I}$ is the set $\sqrt{I} = \{f \in \mathbb{K}[X] \mid f^n \in I \text{ for some } n \geq 1\}$.*

Note that $I \subseteq \sqrt{I}$. If $I = \sqrt{I}$, then I is *radical*, that is, $f^n \in I$ implies that $f \in I$, for some $n \geq 1$.

It is easy to prove that $\mathcal{I}(Z)$ is radical (Corollary 3 of chapter 4 of [CLO07, §2]).

Theorem 2.2.19 (Hilbert Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraically closed field. If $I \subseteq \mathbb{K}[X]$ is an ideal, then*

$$\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$$

Proof. See Theorem 6 of chapter 4 of [CLO07, §2]. □

Theorem 2.2.20 (The Ideal-Variety Correspondence)**.** *Let $\mathbb{K}$ be an arbitrary field. If $I_1 \subset I_2$ are ideals, then $\mathcal{V}(I_2) \subset \mathcal{V}(I_1)$ and, similarly, if $\mathcal{V}(I_2) \subset \mathcal{V}(I_1)$ are varieties, then $\mathcal{I}(\mathcal{V}(I_1)) \subset \mathcal{I}(\mathcal{V}(I_2))$*

Proof. See Theorem 7 of chapter 4 of [CLO07, §2]. □

Theorem 2.2.21. *Let $I \subset \mathbb{F}_q[X]$ be an ideal such that $\{x_i^q - x_i \mid 1 \leq i \leq m\} \subseteq I$, then I is 0-dimensional and radical.*

Proof. If $\{x_i^q - x_i \mid 1 \leq i \leq m\} \subseteq I$ it means that $\mathcal{V}(I) \subset \mathbb{F}_q^m$ and then $\#\mathcal{V}(I) \leq |\mathbb{F}_q^m| = q^m$. Thus I is 0−dimensional.
Since $I \subseteq \sqrt{I}$, to prove that I is radical it is sufficient to show that $\sqrt{I} \subseteq I$.
Let $f = a_1 m_1 + \ldots a_n m_n$ where $a_i \in \mathbb{K}$, $m_i \in \mathcal{M}$ such that $m_i = x_1^{\alpha_{1,i}} \cdot \ldots \cdot x_m^{\alpha_{m,i}}$ with $1 \leq i \leq n$. First of all note that $f^q = f \mod I$. In fact, since $a \in \mathbb{F}_q$ we have $a^q = a$ and $m_i^q = m_i \mod I$ since the field equations are in the ideal and so

$$m_i^q = (x_1^{\alpha_{1,i}} \cdot \ldots \cdot x_m^{\alpha_{m,i}})^q = (x_1^q)^{\alpha_{1,i}} \cdot \ldots \cdot (x_m^q)^{\alpha_{m,i}} = x_1^{\alpha_{1,i}} \cdot \ldots \cdot x_m^{\alpha_{m,i}} = m_i$$

If $f \in \sqrt{I}$ then $f^r \in I$ by definition of radical of I, $f^r \in I$ is equivalent to say that $f^r = 0 \mod I$. We can always consider that $r < q$ since, otherwise, we reduce r module q. So $f^r \in I \implies f^r \cdot f^{q-r} \in I$, that is, $f^q = 0 \mod I$ but $f^q = f \mod I$ and so we can conclude that $f \in I$ and $\sqrt{I} \subseteq I$. □

Finally we define the *Hilbert staircase* $\mathrm{N}(I)$, which is an important tool also for affine-variety codes, the central argument of Chapter 4. $\mathrm{N}(I)$ is the set of all the monomials that are not leading monomial of any polynomial in I:

Definition 2.2.22. *The set $\mathrm{N}(I) = \mathcal{M} \backslash lm(I)$ is called the **Hilbert staircase** or **footprint** of I.*

Example 2.2.23. Let $I \subset \mathbb{F}_q[x, y]$, let $\prec$ be lexicographic order $y \prec x$.

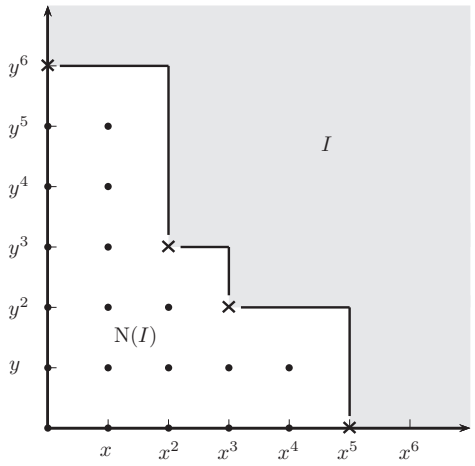
Let

$$I = \langle x^5, x^3y^2, x^2y^3, y^6 \rangle$$

Since $\langle lm(I) \rangle = \langle I \rangle$, then, as we see in the figure, the Hilbert staircase has the following form:

$$\{y^i, xy^i, x^2y^j, x^3, x^3y, x^4, x^4y\}$$

where $0 \leq i \leq 5$ and $0 \leq j \leq 2$.



Let $I \subset \mathbb{K}[X]$ there is a nice and natural connection between the number of zeros of I and the number of points in its footprint w.r.t. any ordering.

Theorem 2.2.24. *Let I be a 0-dimensional radical ideal in $\mathbb{F}_q$. For any monomial ordering we have: $\#\mathcal{V}(I) = \#\mathrm{N}(I)$.*

Proof. We prove this corollary by induction on variety cardinality and using the Buchberger-Möller algorithm. Let $I \subseteq \mathbb{F}_q[X]$, with $x_1 \succ x_2 \succ \ldots \succ x_m$.
If $\#\mathcal{V}(I) = 1$, then $\mathcal{V}(I) = \{P\}$, where $P = (p_1, \ldots, p_m) \in \overline{\mathbb{F}}_q^m$. By Theorem 2.2.17 we can find a Gröbner basis $\mathcal{G}$ for $\mathcal{I}(\mathcal{V}(I))$, which is

$$\mathcal{G} = \{x_1 - p_1, \ldots, x_m - p_m\}.$$

Since I is radical we can use Theorem 2.2.19 and so we have that $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$. Hence $N(I) = \{1\}$, that is, $\#N(I) = 1$.
Let us suppose that $\#\mathcal{V}(I) = n - 1 \implies \#N(I) = n - 1$ and we want to prove that $\#\mathcal{V}(I') = n \implies \#N(I') = n$. Let $\#\mathcal{V}(I') = n$, then $\mathcal{V}(I') = \{P_1, \ldots, P_n\}$, with $P_i \in \overline{\mathbb{F}}_q^m$ for $1 \leq i \leq n$. We consider $Z = \{P_1, \ldots, P_{n-1}\}$ and $I = \mathcal{I}(Z)$.
By inductive hypothesis $\#N(I) = \#\mathcal{V}(Z) = n - 1$. Let $\mathcal{G}$ be a Gröbner basis for I. Applying Buchberger-Möller Theorem for $\mathcal{G}$ and the point $P_n = (p_1, \ldots, p_m)$ we obtain a Gröbner basis $\mathcal{G}'$ for the $0-$dimensional radical ideal $I' = \mathcal{I}(Z \cup P_n)$, which is: $\mathcal{G}' = G_1 \cup G_2 \cup G_3$, where

$$\begin{aligned} G_1 &= \{g \in \mathcal{G} \mid lm(g) \prec lm(g^*)\} \\ G_2 &= \{(x_i - p_i)g^* \mid 1 \leq i \leq m\} \\ G_3 &= \{g - \frac{g(P_n)}{g^*(P_n)}g^* \mid lm(g) \succ lm(g^*)\} \end{aligned}$$

where g^* is the first polynomial in I such that does not vanish in P_n. That is, $g^*(P_n) \neq 0$ and $g(P_n) = 0$ for all $g \in \mathcal{G}$ such that $lm(g) \prec lm(g^*)$. Now, by construction, we have

$$lm(I') = \{lm(g_1) \mid g_1 \in G_1\} \cup \{lm(g^* x_i) \mid 1 \leq i \leq m\} \cup \{lm(g) \mid g \in G_3\}$$

and

$$lm(I) = \{lm(g_1) \mid g_1 \in G_1\} \cup \{lm(g^*)\} \cup \{lm(g) \mid g \in G_3\}.$$

Since $\mathcal{V}(I) \subset \mathcal{V}(I')$, by Theorem 2.2.20, we have that $I' \subset I$. Hence $lm(g^* x_i) \in lm(I)$ and

$$lm(I) = lm(I') \cup \{lm(g_*)\} \implies \#N(I') = \#N(I) + 1 = n. \qquad \square$$

We consider $I \subset \mathbb{K}[X]$ an ideal such that $\{x_i^q - x_i \mid 1 \leq i \leq m\} \subset I$ and let $R = \mathbb{K}[X]/I$.

Theorem 2.2.25. *Let I be an ideal in $\mathbb{K}[X]$ and let $\prec$ a monomial ordering. The set*

$$\mathcal{B} = \{m + I \mid m \in \mathrm{N}(I)\}$$

constitutes a basis for R as a vector space over $\mathbb{K}$

Proof. See Theorem 5 of [Gei09]. $\square$

2.3 Elimination Theory

In this section we see a theorem about the structure of the Gröbner basis of a 0-dimensional ideal w.r.t lex monomial ordering. Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_m]$, as monomial ordering we use the lex ordering induced by $x_1 \prec \ldots \prec x_m$.

Definition 2.3.1. *Let $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[x_1, \ldots, x_m]$. The **$i$-th elimination ideal** I_i is the ideal of $\mathbb{K}[x_1, \ldots, x_i]$ defined by*

$$I_i = I \cap \mathbb{K}[x_1, \ldots, x_i].$$

Note that conventionally $x_1 \succ \ldots \succ x_m$ and the i-th elimination ideal I_i is the ideal of $\mathbb{K}[x_{i+1}, \ldots, x_m]$ defined by $I_i = I \cap \mathbb{K}[x_{i+1}, \ldots, x_m]$.

Theorem 2.3.2 (The Elimination Theorem)**.** *Let $I \subset \mathbb{K}[X]$ be an ideal and let $\mathcal{G}$ be a Gröbner basis of I with respect to lex order where $x_1 \prec \ldots \prec x_m$. Then, for every $0 < i < m$, the set*

$$G_i = \mathcal{G} \cap \mathbb{K}[x_1, \ldots, x_i]$$

is a Gröbner basis of the i-th elimination ideal I_i.

Proof. see Theorem 2 of chapter 3 of [CLO07, §1]. □

Let $g = a_t x_i^t + a_{t-1} x_i^{t-1} + \ldots + a_0 \in G_i$, where the a_j's belong to $\mathbb{K}[x_1, ..., x_{i-1}]$, then $a_t = lp(g)$ is called the *leading polynomial* of g.

Theorem 2.3.3 (Gianni-Kalkbrener Theorem)**.** *Let $\mathcal{G}$ be the reduced Gröbner basis of the 0-dimensional ideal I in $\mathbb{K}[X]$ w.r.t. lex ordering with $x_1 \prec \ldots \prec x_m$. Then:*

1. *There exists exactly one $g \in \mathcal{G}$ such that $g \in \mathbb{K}[x_1]$, i.e. $G_1 = \{g\}$.*

2. *For all $1 \leq i \leq m$, we have that $G_i \neq \emptyset$ and that G_i is the Gröbner basis of the elimination ideal I_i.*

3. *Let $A = (a_1, \ldots, a_m) \in \mathcal{V}(I)$ and let $\bar{a} = (a_1, \ldots, a_{i-1})$. Let $g \in G_i$, then $a_i \in \mathcal{V}(g(\bar{a}, x_i))$, and the following equivalence holds*

$$lp(g)(\bar{a}, x_i) = 0 \text{ in } \mathbb{K} \iff g(\bar{a}, x_i) \equiv 0 \text{ in } \mathbb{K}[x_i].$$

Moreover, there exists $h \in G_i$ such that $h(\bar{a}, x_i) \not\equiv 0$ in $\mathbb{K}[x_i]$.
Conversely, if $g(\bar{a}, \alpha) = 0$, then there exists $A = (\bar{a}, \alpha, a_{i+1}, \ldots, a_m) \in \mathcal{V}(I)$.

Proof. see [Gia89, Kal89] □

Theorem 2.3.3 allows us to compute the set $\mathcal{V}(I)$ of zeros of a given 0-dimensional ideal I in $\mathbb{K}$. We compute the reduced Gröbner basis G for I w.r.t. lex $x_1 \prec \ldots \prec x_m$.

By Theorem 2.3.3 there exists exactly one polynomial g_1 in the first variable x_1. So we can compute its roots. Then we evaluate all polynomials of G_2 in these roots, obtaining polynomials in only one variable, that is x_2. So we can compute their roots, and so on.

Example 2.3.4. We consider three polynomials in $\mathbb{F}_9[x, y, z]$

$$f_1 = x^2 + 2xy \quad f_2 = xz - y \quad f_3 = z - y^2 z$$

Let $I = \langle f_1, f_2, f_3 \rangle$, we want to compute $\mathcal{V}(I)$. We consider the lex order $x \succ y \succ z$, then the reduced Gröbner basis $\mathcal{G}$ of I is

$$\begin{aligned} g_1 &= z^2 - z = z(z-1) \\ g_2 &= yz - y = y(z-1) \\ g_3 &= y^2 - z \\ g_4 &= xz - y \\ g_5 &= xy - z \\ g_6 &= x^2 - z \end{aligned}$$

So $G_1 = \mathcal{G} \cap \mathbb{F}_9[z] = \{g_1\}$ and $G_2 = \mathcal{G} \cap \mathbb{F}_9[y, z] = \{g_2, g_3\}$. By Theorem 2.3.3, G_1 is a Gröbner basis of $I_1 = I \cap \mathbb{F}_9[z]$ and G_2 is a Gröbner basis of $I_2 = I \cap \mathbb{F}_9[y, z]$.
We compute the roots of g_1 and we find $z_1 = 1$ and $z_2 = 0$. Now we evaluate all polynomials of G_2 in z_i. An we obtain $g_2(y, z_1) = 0$ but $g_3(y, z_1) = y^2 - 1$, so y must be $1, 2$. Whereas, $g_2(y, z_2) = -y$ and $g_3(y, z_2) = y^2$ so y must be 0. Finally we evaluate g_4, g_5, g_6 in $(0, 0)$, $(1, 1)$ and $(2, 1)$. And we obtain

$$\begin{array}{llll} g_4(x,0,0) = 0 & g_5(x,0,0) = 0 & g_6(x,0,0) = x^2 & \implies x = 0 \\ g_4(x,1,1) = x - 1 & g_5(x,1,1) = x - 1 & g_6(x,1,1) = x^2 - 1 & \implies x = 1 \\ g_4(x,2,1) = x - 2 & g_5(x,2,1) = -x - 1 & g_6(x,2,1) = x^2 - 1 & \implies x = 2 \end{array}$$

So the solutions are

$$P_1 = (0, 0, 0), \; P_2 = (1, 1, 1), \; P_3 = (2, 2, 1).$$

Hermitian and Norm-Trace curves

3.1 Known facts on Norm-Trace curve and Hermitian curve

From now on we consider $\mathbb{F}_{q^r}$ the finite field with q^r elements, where q is a power of a prime. We consider $r = 2$ and we let α be a fixed primitive element of $\mathbb{F}_{q^2}$, and we consider $\beta = \alpha^{q+1}$ as a primitive element of $\mathbb{F}_q$. From now on q, q^2, α and β are understood as above.

We consider the norm and the trace, the two functions defined as follows.

Definition 3.1.1. *The* ***norm*** $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ *and the* ***trace*** $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ *are two functions from* $\mathbb{F}_{q^r}$ *to* $\mathbb{F}_q$ *such that*

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x^{1+q+\cdots+q^{r-1}} \text{ and } \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x + x^q + \cdots + x^{q^{r-1}}.$$

The *Norm-Trace curve* χ is the curve defined over $\mathbb{F}_{q^r}$ by the following affine equation [Gei03]

$$x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y \text{ where } x, y \in \mathbb{F}_{q^r}. \tag{3.1}$$

We can note that the points $(\bar{x}, \bar{y}) \in (\mathbb{F}_{q^r})^2$ such that $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\bar{x}) = \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(\bar{y})$ are the zeros of χ. So, it is possible to prove (Appendix A of [Gei03]) the following lemma.

Lemma 3.1.2. *The Norm-Trace curve* χ *has exactly* q^{2r-1} $\mathbb{F}_{q^r}$*-rational affine points.*

The genus of χ is $g = \frac{1}{2}(q^{r-1} - 1)(\frac{q^r-1}{q-1} - 1)$.

If we consider $r = 2$, we obtain a famous curve, that is, a Hermitian curve. The *Hermitian curve* $\mathcal{H} = \mathcal{H}_q$ is defined over $\mathbb{F}_{q^2}$ by the affine equation

$$x^{q+1} = y^q + y \text{ where } x, y \in \mathbb{F}_{q^2}. \tag{3.2}$$

This curve has genus $g = \frac{q(q-1)}{2}$ and has $n = q^3$ rational affine points, denoted by $P_1, \ldots, P_n$. For any $x \in \mathbb{F}_{q^2}$, the equation (3.2) has exactly q distinct solutions in $\mathbb{F}_{q^2}$. $\mathcal{H}$ contains also one point at infinity P_∞, so it has q^3+1 rational points over $\mathbb{F}_{q^2}$ [RS94].

We denote with N and Tr, respectively, the norm and the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. It is clear that $\mathcal{H} = \{\mathrm{N}(x) = \mathrm{Tr}(y) \mid x, y \in \mathbb{F}_{q^2}\}$.
We can define a similar curve $\mathcal{H}' = \{\mathrm{N}(x) = -\mathrm{Tr}(y) \mid x, y \in \mathbb{F}_{q^2}\}$ and, using the next lemma, it is easy to see that also $\mathcal{H}'$ contains q^3 $\mathbb{F}_{q^2}$-affine rational points. A well-known fact is the following [LN86].

Lemma 3.1.3. *For any $t \in \mathbb{F}_q$, the equation $\mathrm{Tr}(y) = y^q + y = t$ has exactly q distinct solutions in $\mathbb{F}_{q^2}$. The equation $\mathrm{N}(x) = x^{q+1} = t$ has exactly $q+1$ distinct solutions, if $t \neq 0$, otherwise it has just one solution.*

Proof. The trace is a linear surjective function between two $\mathbb{F}_q$-vector spaces of dimension, respectively, 2 and 1. Thus, $\dim(\ker(\mathrm{Tr})) = 1$, and this means that for any $t \in \mathbb{F}_q$ the set of solutions of the equation $\mathrm{Tr}(y) = y^q + y = t$ is non-empty and then it has the same cardinality of $\mathbb{F}_q$, that is, q.

The equation $x^{q+1} = 0$ has obviously only the solution $x = 0$. If $t \neq 0$, since $t \in \mathbb{F}_q$, we can write $t = \beta^i$, so that $x = \alpha^{i+j(q-1)}$ are all solutions. We can assign $j = 0, \ldots, q$, and so we have $q+1$ distinct solutions. □

3.2 Intersection between the Hermitian curve $\mathcal{H}$ and a line

In this section we analyse the intersection between the Hermitian curve $\mathcal{H}$ and any line.

Lemma 3.2.1. *Let $\mathcal{L}$ be any vertical line $\{x = t\}$, with $t \in \mathbb{F}_{q^2}$. Then $\mathcal{L}$ intersects $\mathcal{H}$ in q affine points.*

Proof. For any $t \in \mathbb{F}_{q^2}$, $t^{q+1} \in \mathbb{F}_q$, and so the equation $y^q + y = t^{q+1}$ has exactly q distinct solutions by applying Lemma 3.1.3. □

Lemma 3.2.2. *In the affine plane $\mathbb{A}^2(\mathbb{F}_{q^2})$, the total number of non-vertical lines is q^4. Of these, $(q^4 - q^3)$ intersect $\mathcal{H}$ in $(q+1)$ points and q^3 are tangent to $\mathcal{H}$, i.e. they intersect $\mathcal{H}$ in only one point.*

Proof. Let $\mathcal{L}$ any non-vertical line, then $\mathcal{L} = \{y = ax + b\}$, with $a, b \in \mathbb{F}_{q^2}$. We have q^2 choices for both a and b, so the total number is q^4. Then

$$\mathcal{H} \cap \mathcal{L} = \{(x, ax + b) \mid a^q x^q + b^q + ax + b = x^{q+1},\ x \in \mathbb{F}_{q^2}\}.$$

Let $c = c(a, b) = a^{q+1} + b^q + b$, then $c \in \mathbb{F}_q$. We have two distinct cases:

- $c = 0$. Then $a^q x^q + b^q + ax + b = x^{q+1}$ becomes $a^q x^q - a^{q+1} + ax = x^{q+1}$, which gives $x = a^q$, that is, $\mathcal{L}$ is tangent.

- $c \neq 0$. Then $a^q x^q + b^q + ax + b = x^{q+1}$ becomes $x^{q+1} - a^q x^q + a^{q+1} - ax = c$, which gives $(x - a^q)^{q+1} = c$. Since $c = (\alpha^{q+1})^r$ for $1 \leq r \leq q-1$, we have $x = a^q + \alpha^{r+i(q-1)}$ for any $0 \leq i \leq q$.

The number of pairs (a, b) satisfying $c(a, b) = 0$ is q^3, because they correspond to the affine points of $\mathcal{H}'$, and those satisfying $c \neq 0$ are $(q^4 - q^3)$. □

Corollary 3.2.3. *Let $\mathcal{L}$ be any horizontal line $\{y = b\}$, with $b \in \mathbb{F}_{q^2}$. Then if $\mathrm{Tr}(b) = 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in one affine point, otherwise, if $\mathrm{Tr}(b) \neq 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in $q+1$ affine points.*

Proof. Apply Lemma 3.2.2 with $a = 0$. □

3.3 Automorphisms of Hermitian curve

We consider an automorphism group $Aut(\mathcal{H}/\mathbb{F}_{q^2})$ of the Hermitian curve over $\mathbb{F}_{q^2}$. $Aut(\mathcal{H}/\mathbb{F}_{q^2})$ contain a subgroup Γ, such that any $\sigma \in \Gamma$ has the following form, as in [Xin95] and in Section 8.2 of [Sti93]:

$$\sigma \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \epsilon x + \gamma \\ \epsilon^{q+1} y + \epsilon \gamma^q x + \delta \end{pmatrix}$$

with $(\gamma, \delta) \in \mathcal{H}$, $\epsilon \in \mathbb{F}_{q^2}^*$. Note that Γ is also a subset of group of affine transformation preserving the set of $\mathbb{F}_{q^2}$-rational affine points of $\mathcal{H}$.
If we choose $\epsilon = 1$ we obtain the following automorphisms

$$\begin{cases} x \longmapsto x + \gamma \\ y \longmapsto y + \gamma^q x + \delta \end{cases} \qquad \text{with } (\gamma, \delta) \in \mathcal{H}, \tag{3.3}$$

that form a subgroup Λ with q^3 elements, see Section II of [Sti88].
The reason why we are interested in the curve automorphisms is the following. If we apply any σ to any curve $\mathcal{X}$ in the affine plane, then the planar intersections between $\sigma(\mathcal{X})$ and $\mathcal{H}$ will be the same as the planar intersections between $\mathcal{X}$ and $\mathcal{H}$. So, if we find out the number of intersections between $\mathcal{X}$ and $\mathcal{H}$, we will automatically have the number of intersection between $\sigma(\mathcal{X})$ and $\mathcal{H}$ for all $\sigma \in \Gamma$. This is convenient because we can isolate special classes of parabolas that act as representatives in the orbit $\{\sigma(\mathcal{X})\}_{\sigma \in \Gamma}$. These special types of parabolas may be easier to handle.

3.4 Automorphisms of Norm-Trace curve

Similarly, we find an automorphism subgroup of $Aut(\chi/\mathbb{F}_{q^r})$ of the Norm-Trace curve, where χ is as (3.1).

We consider $(\gamma, \delta) \in \chi$. For any $\epsilon \in \mathbb{F}_{q^r}^*$ we obtain the following automorphisms

$$\begin{cases} x \longmapsto \epsilon x + \gamma \\ y \longmapsto \epsilon^{q^{r-1}+q^{r-2}+\ldots+1} y + \delta + \sum_i \epsilon^{\alpha_i} \gamma^{\beta_i} x^{\alpha_i} \end{cases} \tag{3.4}$$

where for any subset $A_i \subseteq S$ with $S = \{1, \ldots, r-2\}$, we have

$$\alpha_i = 1 + \sum_{i \in A_i} q^i \qquad \text{and} \qquad \beta_i = q^{r-1} + \sum_{i \in S \setminus A_i} q^i.$$

That is,

$$\alpha_i + \beta_i = 1 + q + q^2 + \ldots + q^{r-1}$$

and

$$\begin{aligned} \sigma(x) = \;& \epsilon x + \gamma \\ \sigma(y) = \;& \epsilon^{q^{r-1}+q^{r-2}+\ldots+1} y + \delta + \epsilon^{1+q} \gamma^{q^2+q^3+\ldots+q^{r-1}} x^{1+q} + \\ & \epsilon^{1+q^2} \gamma^{q+q^3+\ldots+q^{r-1}} x^{1+q^2} + \ldots + \epsilon^{1+q+\ldots+q^{r-2}} \gamma^{q^{r-1}} x^{1+q+\ldots+q^{r-2}}. \end{aligned}$$

Since $(\gamma, \delta) \in \chi$, then there exists an automorphism σ satisfying (3.4). In fact $\sigma(y)$ and $\sigma(x)$ verify the equation $\sigma(y)^{q^{r-1}} + \ldots + \sigma(y) = \sigma(x)^{q^{r-1}+\ldots+1}$.
Furthermore these automorphisms fix the point at infinity.

This set of automorphisms constitutes a group of order $q^{2r-1}(q^r - 1)$. In fact $\epsilon \neq 0$ and δ are arbitrary, so we have q^r possible δ, and for each δ there are q^{r-1} possible values of γ. We have proved:

Proposition 3.4.1. *The automorphism group of the Norm-Trace code contains a subgroup of order* $q^{2r-1}(q^r - 1)$.

In particular, if we choose $\epsilon = 1$ we obtain the following automorphisms

$$\begin{cases} x \longmapsto x + \gamma \\ y \longmapsto y + \delta + \sum_i \gamma^{\beta_i} x^{\alpha_i} \end{cases} \qquad \text{with } (\gamma, \delta) \in \chi, \tag{3.5}$$

with α_i and β_i as before. That is

$$\begin{cases} x \longmapsto x + \gamma \\ y \longmapsto y + \delta + \gamma^{q^2+q^3+\ldots+q^{r-1}} x^{1+q} + \gamma^{q+q^3+\ldots+q^{r-1}} x^{1+q^2} + \ldots + \gamma^{q^{r-1}} x^{1+q+\ldots+q^{r-2}} \end{cases}$$

Affine-variety codes

In this section we fix some notation and recall some known results.

Recall that $\mathbb{F}_q$ is a field with q elements, where q is a power of a prime, and $(\mathbb{F}_q)^n$ is a vector space of dimension n over $\mathbb{F}_q$. Any vector subspace $C \subset (\mathbb{F}_q)^n$ is a linear code (over $\mathbb{F}_q$).

4.1 Affine–variety codes

We present the Reed-Solomon codes (see Definition 1.3.9) as evaluation codes. Let $\{P_1, \ldots, P_q\}$ be all elements of $\mathbb{F}_q$ and define (again) the Reed Solomon codes as follows:

$$RS(k, n, \mathbb{F}_q) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{K}[X], \deg(f) \leq k-1\}.$$

If $k \leq n$ then $\dim(RS) = k$ and it is simple to prove that the distance is $d = n-k+1$.

These codes are a particular case of a larger family of codes, that is, affine-variety codes.

Let $m \geq 1$ and $I \subseteq \mathbb{F}_q[X] = \mathbb{F}_q[x_1, \ldots, x_m]$ be an ideal such that

$$\{x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\} \subset I.$$

Let $\mathcal{V}(I) = \mathcal{P} = \{P_1, P_2, \ldots, P_n\} \subset (\overline{\mathbb{F}}_q)^m$ its variety, that is, the set of its common roots. Let $g_1, \ldots, g_s \in \mathbb{F}_q[X]$ be generators of $I = \langle g_1, \ldots, g_s \rangle$.

Since I is a zero-dimensional radical ideal (by Theorem 2.2.21), we have an isomorphism of $\mathbb{F}_q$ vector spaces, that we call the *evaluation map*:

$$\begin{array}{rccc} ev_{\mathcal{P}} : R = & \mathbb{F}_q[x_1, \ldots, x_m]/I & \longrightarrow & (\mathbb{F}_q)^n \\ & f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array} \tag{4.1}$$

Let $L \subseteq R$ be an $\mathbb{F}_q$ vector subspace of R with dimension r.

Definition 4.1.1 ([FL98]). *The* **affine–variety code** $C(I, L)$ *is the image of* L *under the evaluation map* $ev_{\mathcal{P}}$ *and the affine–variety code* $C^{\perp}(I, L)$ *is its dual code.*

If $b_1, \ldots, b_r$ is a linear basis for L over $\mathbb{F}_q$, then the matrix

$$H = \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

is a generator matrix for $C(I, L)$ and a parity-check matrix for $C^{\perp}(I, L)$.

Theorem 4.1.2. *Every linear code may be represented as an affine–variety code.*

Proof. See Proposition 1.4 of [FL98] □

Examples of affine-variety codes are Norm-Trace codes and, in particular, Hermitian codes, which we study in the following section.

4.2 Norm-Trace codes and Hermitian codes

We consider a Norm-Trace polynomial over $\mathbb{F}_{q^r}$

$$y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y - x^{\frac{q^r-1}{q-1}}$$

Let $I = \langle y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y^q - x^{q^{r-1}+q^{r-2}+\ldots+q+1}, x^{q^r} - x, y^{q^r} - y \rangle$ and let $R = \mathbb{F}_{q^r}[x, y]/I$. We take $L \subseteq R$ generated by

$$\mathcal{B}_{m,q} = \{x^i y^j + I \mid q^{r-1}i + \frac{(q^r-1)}{q-1}j \leq m,\ 0 \leq j < q^{r-1},\ 0 \leq i \leq q^r - 1\},$$

where m is an integer such that $0 \leq m \leq q^{2r-1} + \ldots + q^r - q^{r-1} - \ldots - q - 2$.

For simplicity, we also write $x^r y^s$ for $x^r y^s + I$.
We consider the evaluation map (4.1) $ev_{\mathcal{P}} : R \to (\mathbb{F}_{q^r})^n$, where $n = q^{2r-1}$. We have the following affine–variety codes: $C(I, L) = \mathrm{Span}_{\mathbb{F}_{q^r}} \langle ev_{\mathcal{P}}(\mathcal{B}_{m,q}) \rangle$ and its dual $(C(I, L))^{\perp}$ is a *Norm-Trace code.*

If we consider $r = 2$, we have a special case of a Norm-Trace code, that is, a Hermitian code. In this case $I = \langle y^q + y - x^{q+1}, x^{q^2} - x, y^{q^2} - y \rangle \subset \mathbb{F}_{q^2}[x, y]$ and $R = \mathbb{F}_{q^2}[x, y]/I$. We take $L \subseteq R$ generated by

$$\mathcal{B}_{m,q} = \{x^r y^s + I \mid qr + (q+1)s \leq m,\ 0 \leq s \leq q-1,\ 0 \leq r \leq q^2 - 1\},$$

where m is an integer such that $0 \leq m \leq q^3 + q^2 - q - 2$.
Then the affine-variety code $C(m, q) = (C(I, L))^{\perp}$, where $C(I, L) = \mathrm{Span}_{\mathbb{F}_{q^2}} \langle ev_{\mathcal{P}}(\mathcal{B}_{m,q}) \rangle$,

is called the *Hermitian code* with parity-check matrix H.

$$H = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \dots & f_i(P_n) \end{pmatrix} \text{ where } f_j \in \mathcal{B}_{m,q}, \tag{4.2}$$

where, for Hermitian codes, $n = q^3$.
As we will see in Chapter 5, the Hermitian codes have specific explicit formulae linking their dimension and their distance.

4.2.1 First results on words of given weight

Let $0 \leq w \leq n$ and C be a linear code. We recall (see Subsection 1.2.1) that

$$A_w(C) = |\{c \in C \mid \mathrm{w}(c) = w\}|.$$

Let $\bar{z} \in (\mathbb{F}_q)^n$, $\bar{z} = (\bar{z}_1, \dots, \bar{z}_n)$. Then

$$\bar{z} \in C(I,L)^\perp \iff H\bar{z}^T = 0 \iff \sum_{i=1}^{n} \bar{z}_i b_j(P_i) = 0, \quad j = 1, \dots, r. \tag{4.3}$$

Proposition 4.2.1. *Let $1 \leq w \leq n$.*
Let J_w be the ideal in $\mathbb{F}_q[x_{1,1}, \dots x_{1,m}, \dots, x_{w,1}, \dots x_{w,m}, z_1, \dots, z_w]$ generated by

$$\sum_{i=1}^{w} z_i b_j(P_i) \text{ for } \quad j = 1, \dots, r \tag{4.4}$$

$$g_h(x_{i,1}, \dots x_{i,m}) \text{ for } \quad i = 1, \dots, w \text{ and } h = 1, \dots, s \tag{4.5}$$

$$z_i^{q-1} - 1, \quad i = 1, \dots, w \tag{4.6}$$

$$\prod_{1 \leq l \leq m} ((x_{j,l} - x_{i,l})^{q-1} - 1), \quad 1 \leq j < i \leq w. \tag{4.7}$$

Then any solution of J_w corresponds to a codeword of $C^\perp(I,L)$ with weight w. Moreover,

$$A_w(\mathcal{C}^\perp(I,L)) = \frac{|\mathcal{V}(J_w)|}{w!}.$$

Proof. Let σ be a permutation, $\sigma \in S_w$. It induces a permutation $\hat{\sigma}$ acting on $\{x_{1,1}, \dots, x_{1,m}, \dots, x_{w,1}, \dots x_{w,m}, z_1, \dots, z_w\}$ as $\hat{\sigma}(x_{i,l}) = x_{\sigma(i),l}$ and $\hat{\sigma}(z_i) = z_{\hat{\sigma}(i)}$. It is easy to show that J_w is invariant w.r.t. any $\hat{\sigma}$, since each of (4.4), (4.5), (4.6) and (4.7) is so.
Let $Q = (\overline{x}_{1,1}, \dots \overline{x}_{1,m}, \dots, \overline{x}_{w,1}, \dots \overline{x}_{w,m}, \overline{z}_1, \dots, \overline{z}_w) \in \mathcal{V}(J_w)$. We can associate a codeword to Q in the following way. For each $i = 1, \dots, w$, $P_{r_i} = (\overline{x}_{i,1}, \dots \overline{x}_{i,m})$ is in $\mathcal{V}(I)$, by (4.5). We can assume $r_1 < r_2 < \dots < r_w$, via a permutation $\hat{\sigma}$ if necessary.

Note that (4.7) ensures that for each (i,j), with $i \neq j$, we have $P_{r_i} \neq P_{r_j}$, since there is a l such that $x_{i,l} \neq x_{j,l}$. Since $\overline{z}_i^{q-1} = 1$ (4.6), $\overline{z}_i \in \mathbb{F}_q \setminus \{0\}$. Let $c \in (\mathbb{F}_q)^n$ be

$$c = (0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_1}}}{\overline{z}_1}, 0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_i}}}{\overline{z}_i}, 0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_w}}}{\overline{z}_w}, 0, \ldots, 0).$$

We have that $c \in \mathcal{C}^{\perp}(I, L)$, since (4.4) is equivalent to (4.3).
Reversing the previous argument, we can associate to any codeword a solution of J_w. By invariance of J_w, we actually have $w!$ distinct solutions for any codeword. So, to get the number of codewords of weight w, we divide $|\mathcal{V}(J_w)|$ by $w!$. □

Note that this approach is a generalization of the approach in [Sal07] to determinate the number of words having given weight for a cyclic code.

4.3 The approach by Fitzgerald and Lax to decoding the affine-variety code

In [FL98] a decoding technique was proposed following what is known as the "Cooper philosophy". Although this terminology has been established only recently ([MO09]), this decoding approach has a quite wide literature, e.g. [Coo90],[Coo93], [CM02a],[Coo91], [CRHT94a]. We describe this technique for affine-variety codes, as follows. Let $C^{\perp}(I, L)$ be an affine-variety code with dimension $n - r$ and let $I = \langle g_1, \ldots, g_\gamma \rangle$. Let L be linearly generated by $b_1, \ldots, b_r$. Then we can denote by $J_{\mathcal{FL}}^{C,t}$ the ideal ($\mathcal{FL}$ is for "FitzgeraldLax")

$$J_{\mathcal{FL}}^{C,t} \subset \mathbb{F}_q[s_1, \ldots, s_r, x_{t,1}, \ldots, x_{t,m}, \ldots, x_{1,1}, \ldots, x_{1,m}, e_1, \ldots, e_t] = \mathbb{F}_q[S, X_t, \ldots, X_1, E]$$

where[1]

$$J_{\mathcal{FL}}^{C,t} = \left\langle \begin{array}{l} \left\{ \sum_{j=1}^{t} e_j b_\rho(x_{j,1}, \ldots, x_{j,m}) - s_\rho \right\}_{1 \leq \rho \leq r}, \\ \left\{ e_j^{q-1} - 1 \right\}_{1 \leq j \leq t}, \{ g_h(x_{j,1}, \ldots, x_{j,m}) \}_{\substack{1 \leq h \leq \gamma, \\ 1 \leq j \leq t}} \end{array} \right\rangle \quad . \tag{4.8}$$

Let $<_S$ be any term ordering on the variables $s_1, \ldots, s_r$ and $\prec_{\text{lex}}$ be the lexicographic ordering on the variables $X_t, \ldots, X_1$, such that

$$x_{t,1} \prec_{\text{lex}} \cdots \prec_{\text{lex}} x_{t,m} \prec_{\text{lex}} \cdots \prec_{lex} x_{1,1} \prec_{\text{lex}} \cdots \prec_{\text{lex}} x_{1,m}.$$

Let $<_E$ be any term ordering on the variables $e_1, \ldots, e_t$.
Then let $<$ be the block order $(<_S, \prec_{\text{lex}}, <_E)$. We denote by $\mathcal{G}_{\mathcal{FL}}^{C,t}$ a Gröbner basis of $J_{\mathcal{FL}}^{C,t}$ with respect to $<$. In [FL98] we can find a method describing how to find the error locations and values, by applying elimination theory to the polynomials in $\mathcal{G}_{FL}^{C,t}$.

[1] To speed up the basis computation we can add $\left\{ x_{j,\iota}^q - x_{j,\iota} \right\}_{\substack{1 \leq j \leq t, \\ 1 \leq \iota \leq m}}$ to the ideal.

Example 4.3.1. Let $C = C^{\perp}(I, L)$ be the Hermitian code from the curve $y^2+y = x^3$ over $\mathbb{F}_4$ and with defining monomials $\{1, x, y, x^2, xy\}$. The eight points of the variety defined by I are

$$P_1 = (0,0), P_2 = (0,1), P_3 = (1,\alpha), P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), P_6 = (\alpha,\alpha^2), P_7 = (\alpha^2,\alpha), P_8 = (\alpha^2,\alpha^2),$$

where α is any primitive element of $\mathbb{F}_4$. It is well–known that C corrects up to $t = 2$ errors. The ideal $J^{C,2}_{\mathcal{FL}} \subset \mathbb{F}_4[s_1, \ldots, s_5, x_2, y_2, x_1, y_1, e_1, e_2]$ is

$$\begin{aligned} J^{C,2}_{\mathcal{FL}} = \langle \{ & x_1^4 - x_1, x_2^4 - x_2, y_1^4 - y_1, y_2^4 - y_2, e_1^3 - 1, e_2^3 - 1, y_1^2 + y_1 - x_1^3, \\ & y_2^2 + y_2 - x_2^3, e_1 + e_2 - s_1, e_1x_1 + e_2x_2 - s_2, e_1y_1 + e_2y_2 - s_3, \\ & e_1x_1^2 + e_2x_2^2 - s_4, e_1x_1y_1 + e_2x_2y_2 - s_5\}\rangle. \end{aligned}$$

Typically the Gröbner basis of $J^{C,t}_{\mathcal{FL}}$ that has been obtained using the block order $<$ contains a large number of polynomials and most are not useful for decoding purposes. We would have to choose a polynomial in $\mathbb{F}_q[S, x_{t,1}]$ that, once specialized in the received syndrome, could be used to find the first coordinates of all the errors. It is important to observe that in this situation we do not know which polynomial is the right one, because after the specialization we can obtain a polynomial which vanishes identically.

4.4 Base notion for decoding using our method

4.4.1 Stratified ideals

In this subsection we summarize some definitions and results from [GS09].

Let $J \subset \mathbb{K}[\mathcal{S}, \mathcal{A}, \mathcal{T}]$ be a zero–dimensional radical ideal, with variables $\mathcal{S} = \{\mathsf{s}_1, \ldots, \mathsf{s}_N\}$, $\mathcal{A} = \{\mathsf{a}_1, \ldots, \mathsf{a}_L\}$, $\mathcal{T} = \{\mathsf{t}_1, \ldots, \mathsf{t}_K\}$. We fix a term ordering $<$ on $\mathbb{K}[\mathcal{S}, \mathcal{A}, \mathcal{T}]$, with $\mathcal{S} < \mathcal{A} < \mathcal{T}$, such that $\mathsf{a}_L < \mathsf{a}_{L-1} < \ldots < \mathsf{a}_1$ is the order of the variables in $\mathcal{A}$. Let us recall the elimination ideals (see Section 2.3)

$$J_{\mathcal{S}} = J \cap \mathbb{K}[\mathcal{S}], J_{\mathcal{S},\mathsf{a}_L} = J \cap \mathbb{K}[\mathcal{S}, \mathsf{a}_L], \ldots, J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_1} = J \cap \mathbb{K}[\mathcal{S}, \mathsf{a}_L, \ldots, \mathsf{a}_1] = J \cap \mathbb{K}[\mathcal{S}, \mathcal{A}].$$

We want to view $\mathcal{V}(J_{\mathcal{S}})$ as a disjoint union of some sets. The way we define these sets is linked to the fact that any point P in $\mathcal{V}(J_{\mathcal{S}})$ can be extended to at least one point in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L})$. But the number of all possible extensions of P in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L})$ is finite, since the ideal is zero-dimensional, so we can partition $\mathcal{V}(J_{\mathcal{S}})$ in sets such that all points in the same set share the same number of extensions. We denote by $\lambda(L)$ the maximum number of extensions in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L})$ for any $P \in \mathcal{V}(J_{\mathcal{S}})$. The same principle applies when we consider the variety of another elimination ideal, e.g. $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_h})$. We can partition it into subsets such that all points in the same subset share the

same number of extensions in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_h,\mathsf{a}_{h-1}})$. The maximum number of extensions is denoted by $\lambda(h-1)$.

We write our partitioning in a formal way, as follows:

$$\begin{aligned}\mathcal{V}(J_{\mathcal{S}}) =& \sqcup_{l=1}^{\lambda(L)} \Sigma_l^L, \text{ with}\\ \Sigma_l^L =& \{(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N) \in \mathcal{V}(J_{\mathcal{S}}) \mid \exists \text{ exactly } l \text{ distinct values } \bar{\mathsf{a}}_L^{(1)},\ldots,\bar{\mathsf{a}}_L^{(l)}\\ & \text{s.t. } (\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_L^{(\ell)}) \in \mathcal{V}(J_{\mathcal{S},\mathsf{a}_L}), 1 \le \ell \le l\};\end{aligned}$$

$$\begin{aligned}&\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_h}) = \sqcup_{l=1}^{\lambda(h-1)} \Sigma_l^{h-1},\ 2 \le h \le L, \text{ with}\\ &\Sigma_l^{h-1} = \{(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_L,\ldots,\bar{\mathsf{a}}_h) \in \mathcal{V}(J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_h}) \mid \exists \text{ exactly } l \text{ distinct values}\\ &\qquad \bar{\mathsf{a}}_{h-1}^{(1)},\ldots,\bar{\mathsf{a}}_{h-1}^{(l)} \text{ s.t. } (\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_L,\ldots,\bar{\mathsf{a}}_h,\ \bar{\mathsf{a}}_{h-1}^{(\ell)}) \in \mathcal{V}(J_{\mathcal{S},\mathsf{a}_L,\ldots,\mathsf{a}_{h-1}}),\ 1 \le \ell \le l\}.\end{aligned}$$

For an arbitrary zero-dimensional ideal J, nothing can be said about $\lambda(h)$, except that $\lambda(h) \ge 1$ for any $1 \le h \le L$.

Definition 4.4.1 ([GS09])**.** *With the above notation, let J be a zero-dimensional radical ideal. We say that J is **stratified**, with respect to the $\mathcal{A}$ variables, if:*

(a) $\lambda(h) = h$, $1 \le h \le L$, *and*

(b) $\sum_l^h \neq \emptyset$, $1 \le h \le L$, $1 \le l \le h$.

To explain conditions (a) and (b) in the above definition, let us consider $h = L$ and think of the projection

$$\pi : \mathcal{V}(J_{\mathcal{S},\mathsf{a}_L}) \to \mathcal{V}(J_{\mathcal{S}}). \tag{4.9}$$

In this case, (a) in Definition 4.4.1 is equivalent to saying that any point in $\mathcal{V}(J_{\mathcal{S}})$ has at most L pre-images in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_L})$ via π, and that there is at least one point with (exactly) L pre-images. On the other hand, (b) implies that, if for a point $P \in \mathcal{V}(J_{\mathcal{S}})$ we have $|\pi^{-1}(P)| = m \ge 2$, then there is at least another point $Q \in \mathcal{V}(J_{\mathcal{S}})$ such that $|\pi^{-1}(Q)| = m - 1$.

Example 4.4.2. Let $\mathcal{S} = \{\mathsf{s}_1\}$, $\mathcal{A} = \{\mathsf{a}_1,\mathsf{a}_2,\mathsf{a}_3\}$ $(L = 3)$ and $\mathcal{T} = \{\mathsf{t}_1\}$ such that $\mathcal{S} < \mathcal{A} < \mathcal{T}$ and $\mathsf{a}_3 < \mathsf{a}_2 < \mathsf{a}_1$. Let us consider $\mathcal{J} = \mathcal{I}(Z) \subset \mathbb{C}[\mathsf{s}_1,\mathsf{a}_3,\mathsf{a}_2,\mathsf{a}_1,\mathsf{t}_1]$ with $Z = \{(1,2,1,0,0),(1,2,2,0,0),\ (1,4,0,0,0),\ (1,6,0,0,0),\ (2,5,0,0,0),\ (3,1,0,0,0),\ (3,3,0,0,0),\ (5,2,0,0,0)\}$. Then:

$$\begin{aligned}\mathcal{V}(J_{\mathcal{S}}) &= \{1,2,3,5\}\\ \mathcal{V}(J_{\mathcal{S},\mathsf{a}_3}) &= \{(1,2),(1,4),(1,6),(2,5),(3,1),(3,3),(5,2)\}\\ \mathcal{V}(J_{\mathcal{S},\mathsf{a}_3,\mathsf{a}_2}) &= \{(1,2,1),(1,2,2)(1,4,0),(1,6,0),(2,5,0),(3,1,0),(3,3,0),(5,2,0)\}\\ \mathcal{V}(J_{\mathcal{S},\mathsf{a}_3,\mathsf{a}_2,\mathsf{a}_1}) &= \{(1,2,1,0),(1,2,2,0)(1,4,0,0),(1,6,0,0),(2,5,0,0),(3,1,0,0),(3,3,0,0),(5,2,0,0)\}\end{aligned}$$

Let us consider the projection $\pi : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathsf{a}_3}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}})$. Then:

$$|\pi^{-1}(\{5\})| = 1,\ |\pi^{-1}(\{2\})| = 1,\ |\pi^{-1}(\{3\})| = 2,\ |\pi^{-1}(\{1\})| = 3\,,$$

so $\sum_1^3 = \{2,5\}$, $\sum_2^3 = \{3\}$, $\sum_3^3 = \{1\}$ and $\sum_i^3 = \emptyset$, $i > 3$. This means that $\lambda(L) = \lambda(3) = 3$ and $\sum_l^3$ is not empty, for $l = 1,2,3$. Thus the conditions of Definition 4.4.1 are satisfied for $h = L = 3$ (see Fig. 4.1). In the same way, it is easy to verify said conditions also for $h = 1,2$, and hence the ideal $\mathcal{J}$ is stratified with respect to the $\mathcal{A}$ variables.

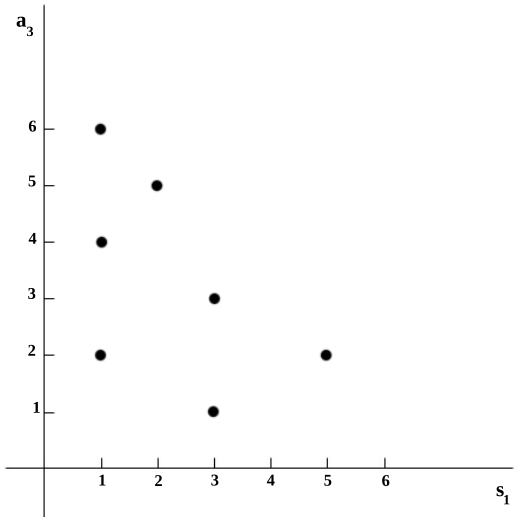


Figure 4.1: A variety in a stratified case

With the above notation, an immediate consequence of Theorem 3.6 in [GS06] (Theorem 32 in [GS09]) is the following proposition.

Proposition 4.4.3. *Let $<$ be any lexicographic term order with $\mathcal{S} < \mathcal{A} < \mathcal{T}$ and $\mathsf{a}_L < \mathsf{a}_{L-1} < \cdots < \mathsf{a}_1$. Let J be a stratified ideal with respect to the $\mathcal{A}$ variables. Let $G = \mathrm{GB}(J)$. Then G contains one and only one polynomial g such that:*

$$g \in \mathbb{K}[\mathcal{S}, \mathsf{a}_L], \qquad \mathbf{T}(g) = \mathsf{a}_L^L.$$

4.4.2 Root multiplicities and Hasse derivative

Definition 4.4.4. *Let $g = \sum_i a_i x^i \in \mathbb{K}[x]$. Then the* **n-*th* *Hasse derivative*** *of g is $\varphi^{(n)}(g)$ and the* **n-*th* *formal derivative*** *of g is $g^{(n)}$, where*

$$\varphi^{(n)}(g) = \sum_i \binom{i}{n} a_i x^{i-n} \ \text{ and } \ g^{(n)} = n! \sum_i \binom{i}{n} a_i x^{i-n}.$$

We can note that $g^{(n)} = n!\varphi^{(n)}(g)$. In a field with characteristic p, it is more convenient to use the Hasse derivative, because $n! = 0$ for all $n \geq p$.

Note that $\varphi^{(2)}(g) \neq \varphi^{(1)}\left(\varphi^{(1)}(g)\right)$.

Definition 4.4.5. *Let $g \in \mathbb{K}[x]$, $g \neq 0$, $P \in \mathbb{K}$ and $g(P) = 0$. The* ***multiplicity*** *of P as a root of g is the largest integer $r \geq 1$ such that*

$$\varphi^{(k)}(g)(P) = \varphi^{(k)}(g)\Big|_{x=P} = 0, \quad \text{for } 0 \leq k \leq r-1.$$

The following theorem is well-known, see e.g. [LN97].

Theorem 4.4.6. *Let $g, f \in \mathbb{K}[x]$ and let g be irreducible. Then*

$$g^r | f \qquad \Longleftrightarrow \qquad g | \varphi^{(k)}(f) \ \text{ for } 0 \leq k \leq r-1\,.$$

As a consequence of the previous theorem when $g = (x - P)$ for any $P \in \mathbb{K}$, we have

$$(x-P)^r | f \quad \Longleftrightarrow \quad \varphi^{(k)}(f)\Big|_{x=P} = 0 \ \text{ for } 0 \leq k \leq r-1\,.$$

4.4.3 General error locator polynomials

Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with correction capability $t \geq 1$. Choose any parity-check matrix with entries in an appropriate extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, $m \geq 1$. Its syndromes lie in $(\mathbb{F}_{q^m})^{n-k}$ and form a vector space of dimension $r = n - k$ over $\mathbb{F}_q$. Let α be a primitive n-th root of unity in $\mathbb{F}_{q^m}$.

Definition 4.4.7. *Let $\mathcal{L}$ be a polynomial in $\mathbb{F}_q[S, x]$, where $S = (s_1, \ldots, s_r)$. Then $\mathcal{L}$ is a* **general error locator polynomial** *of C if*

1. *$\mathcal{L}(S, x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[S]$, $0 \leq j \leq t-1$, that is, $\mathcal{L}$ is a monic polynomial with degree t with respect to the variable x and its coefficients are in $\mathbb{F}_q[S]$;*

2. *given a syndrome $\mathbf{s} = (\overline{s}_1, \ldots \overline{s}_r) \in (\mathbb{F}_{q^M})^r$, corresponding to an error vector of weight $\mu \leq t$ and error positions $\{k_1, \ldots, k_\mu\}$, if we evaluate the S variables at $\mathbf{s}$, then the roots of $\mathcal{L}(\mathbf{s}, x)$ are exactly $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, 0\}$, where the multiplicity of 0 is $t - \mu$.*

Given any (correctable) linear code C, the existence of a general error locator polynomial is not known. In [OS05] the authors prove its existence for any cyclic code and recently in [GS06, GS09, Gio06] its existence has been proved for a large class of linear codes.

We can extend Definition 4.4.7 to the case when there are also erasures.

Definition 4.4.8. *Let $\mathcal{L}$ be a polynomial in $\mathbb{F}_q[S, W, x]$, $S = (s_1, \ldots, s_r)$ and $W = (w_1, \ldots, w_\nu)$, where ν is the number of occurred erasures. Let $2\tau + \nu < d$. Then $\mathcal{L}$ is a* **general error locator polynomial of type $\boldsymbol{\nu}$** *of C if*

1. *$\mathcal{L}(S, W, x) = x^\tau + a_{\tau-1}x^{\tau-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[S, W]$, for any $0 \leq j \leq \tau - 1$, that is, $\mathcal{L}$ has degree τ w.r.t. x and coefficients in $\mathbb{F}_q[S, W]$;*

2. *for any syndrome $\mathbf{s} = (\overline{s}_1, \ldots, \overline{s}_r)$ and any erasure location vector $\mathbf{w}$= $(\overline{w}_1, \ldots, \overline{w}_\nu)$, corresponding to an error vector of weight $\mu \leq \tau$ and error locations $\{k_1, \ldots, k_\mu\}$, if we evaluate the S variables at $\mathbf{s}$ and the W variables at $\mathbf{w}$, then the roots of $\mathcal{L}(\mathbf{s}, \mathbf{w}, x)$ are $\{\alpha^{k_1}, \ldots, \alpha^{k_\mu}, 0\}$, where the multiplicity of 0 is $\tau - \mu$.*

For the benefit of readers unfamiliar with simultaneous correction of errors and erasures, we sketch how it works. When some (say ν) symbols are not recognised by the receiver, the decoder treats them as *erasures*. The decoder knows the positions of these erasures $i_1, \ldots, i_\nu$, which means in our notation that the decoders knows the erasure locations grouped for convenience in the *erasure location vector* $\mathbf{w} = (\bar{w}_1, \ldots, \bar{w}_\nu) = (\alpha^{i_1}, \ldots, \alpha^{i_\nu})$. A standard result in coding theory is that it is possible to correct simultaneously ν erasures and τ errors, provided that $2\tau + \nu < d$.

To be consistent with our notation, we may refer to a polynomial in Definition 4.4.7 also as a *general error locator polynomial of type 0.*

For a code C, the possession of a polynomial of each type $0 \leq \nu < d$ might be a stronger condition than the possession of a polynomial of type 0, but in [OS05] the authors prove that any cyclic code admits a polynomial of any type ν, for $0 \leq \nu < d$. In [GS09] the existence of general error locator polynomials (of any type) for a large class of linear codes was proved, but it is still unknown whether such a result holds for general linear codes.

The four phases of Hermitian codes

In this chapter we analyse the four phases of Hermitian codes.
We recall the notion of numerical semigroup and we report some technical results that we find in Chapter 5 of [HvLP98]. We describe the four Hermitian phases that span the Hermitian codes, focusing at the first phase. We also note that the first phase could be extended to include a portion of the second phase and there is also an intersection between the third and fourth phase.

5.1 Numerical semigroups

We define a subset $\Lambda \subset \mathbb{N}$ to be a *numerical semigroup* if $0 \in \Lambda$ and for all $x, y \in \Lambda$ then also $x + y \in \Lambda$.
The elements of Λ are called *nongaps* of Λ, whereas the elements in $\mathbb{N}\backslash\Lambda$ are called *gaps*. The number of gaps is called the *genus* and it is denoted by g. The *conductor* c of Λ is the smallest $n \in \mathbb{N}$ such that $\{x \in \mathbb{N} \mid x \geq n\}$ is contained in Λ. So $c - 1$ is the largest gap of Λ if $g > 0$.

Let $A = \{a_1, \ldots, a_k\}$ be a subset of a semigroup Λ. If for any element $s \in \Lambda$ there exist $x_1, \ldots, x_k \in \mathbb{N}$ such that $s = \sum_{i=1}^{k} x_i a_i$, the semigroup Λ is said to be *generated* by A and written $\Lambda = \langle A \rangle$.

The elements of a semigroup Λ will be enumerated by the sequence $(\rho_i \mid i \in \mathbb{N})$ such that $\rho_i < \rho_{i+1}$ for all i. The number of gaps smaller than ρ_i will be denoted by $g(i)$.

Lemma 5.1.1. *Let Λ be a semigroup with finitely many gaps.*

(1) If $i \in \mathbb{N}$, then $g(i) = \rho_i - i + 1$.

(2) If $i \in \mathbb{N}$, then $\rho_i \leq i + g - 1$ and equality holds if and only if $\rho_i \geq c$.

(3) If $i > c - g$, then $\rho_i = i + g - 1$.

(4) If $i \leq c - g$, then $\rho_i < c - 1$.

Proof. See Lemma 5.6 of [HvLP98]. □

Proposition 5.1.2. *Let g a finite number. Then $c \leq 2g$.*

Proof. See Proposition 5.7 of [HvLP98] □

A semigroup is called *symmetric* if $c = 2g$.

Proposition 5.1.3. *Let $a, b \in \mathbb{N}$ such that $gcd(a, b) = 1$. The semigroup generated by a and b is symmetric. Furthermore $c = (a-1)(b-1)$ and $g = \frac{1}{2}(a-1)(b-1)$.*

Proof. See Proposition 5.11 of [HvLP98] □

5.2 Analysing Hermitian codes using numerical semigroups

Now we specialize to the case of Hermitian codes.

We consider a Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$, i.e. $x^{q+1} = y^q + y$. Let $R = \mathbb{F}_{q^2}[x, y]/I$, where $I = \langle x^{q+1} - y^q - y, x^{q^2} - x, y^{q^2} - y \rangle$ and $\mathcal{P} = \{P_1, \ldots, P_n\}$ is the set that contains the affine points of $\mathcal{H}$.

Let $\prec$ be a weighted degree ordering with $w_x = q$ and $w_y = q+1$ and $x \prec_{lex} y$. Let $\rho : \mathcal{M} \subset R \longrightarrow \mathbb{N}$ be a *weight function* such that $\rho(x^r y^s) = qr + (q+1)s$. We recall that the Hilbert staircase $\mathrm{N}(I)$ is the set of all the monomials that are not leading monomial of any polynomial in I (Definition 2.2.22).
Note that $\langle lm(I) \rangle = \{y^q, x^{q^2}, y^{q^2}\}$. A reduced Gröbner basis for I is $\mathcal{G} = \{y^q + y - x^{q+1}, x^{q^2} - x\}$ and the leading terms of $\mathcal{G}$ are $lm(\mathcal{G}) = \{y^q, x^{q^2}\}$. Hence, the footprint $\mathrm{N}(I)$ of I is

$$N(I) = \{x^r y^s \mid r \leq q^2 - 1,\ s \leq q - 1\}.$$

Remark 5.2.1. The weights of the elements in the footprint are exactly the elements of the semigroup, and there are no repetitions. That is, $\rho_{i+1} \in \Lambda$ is nothing else than the weight function of f_{i+1}. This is the $(i+1)$-th elements of $N(I)$, where the monomials in the footprint is ordered by $\prec$, the weighted degree ordering.

As we have seen in Section 2.2 the number of affine points of $\mathcal{H}$, is related to the Hilbert staircase of I. In fact, by Theorem 2.2.21, I is a 0-dimensional and radical ideal. Hence, by Theorem 2.2.24 the number of affine points of $\mathcal{H}$ is $\#\mathcal{V}(I) = \#\mathrm{N}(I) = q \cdot q^2 = q^3$.

By Theorem 2.2.25 a base of R is

$$\mathcal{B} = \{m + I \mid m \in \mathrm{N}(I)\}$$

We consider $\mathcal{L}_i \subset \mathcal{B}$ such that $\mathcal{L}_i = \{f \in \mathcal{B} \mid \rho(f) \leq \rho_i\}$ where ρ_i is the i-th element of Λ. Then a Hermitian code C_i could be seen as the dual of an *evaluation code*

$$E_i = \{ev_{\mathcal{P}}(f) \mid f \in \mathcal{L}_i\},$$

where $ev_{\mathcal{P}}$ is the evaluation map as in (4.1). In fact in Section 4.2 we saw that a Hermitian code is $C(m,q) = (C(I,L))^{\perp}$ where $L \subset R$ and a base of L is

$$B_{m,q} = \{x^r y^s + I \mid qr + (q+1) \leq m \text{ with } s \leq q-1,\ r \leq q^2 - 1\}.$$

Since $\rho(x^r y^s) = qr + (q+1)$, then the semigroup Λ of the weight function of Hermitian curve $\mathcal{H}$ is generated by $\langle q, q+1\rangle$ and it is denoted by $\Lambda_{\mathcal{H}}$. Hence, by Proposition 5.1.3, $\Lambda_{\mathcal{H}}$ is a symmetric semigroup and $g = q(q-1)/2$.

Example 5.2.2. We consider a Hermitian curve with $q = 4$.
The semigroup $\Lambda_{\mathcal{H}}$ is generated by $\langle q, q+1\rangle = \langle 4, 5\rangle$. The genus is $g = 6$ and the gaps are $\{1, 2, 3, 6, 7, 11\}$.

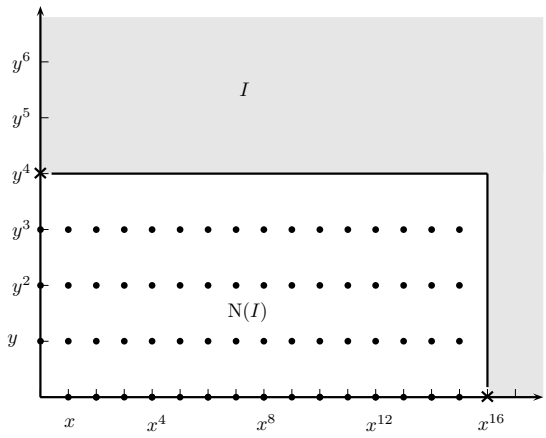
i	1	2	3	4	5	6	7	8
f_i	1	x	y	x^2	xy	y^2	x^3	x^2y
ρ_i	0	4	5	8	9	10	12	13

The ideal

$$I = \langle x^5 - y^4 - y, x^{16} - x, y^{16} - y\rangle$$

by Theorem 2.2.21 is a 0-dimensional and radical ideal.
The number of affine points of $\mathcal{H}$ is

$$\#\mathcal{V}(I) = \#\mathrm{N}(I) = 4 \cdot 16 = 4^3.$$



Theorem 5.2.3. *The minimum distance of E_i is $d_i \geq n - \rho_i$.*
If $\rho_i < n$, then $\dim(E_i) = i$.

Proof. See Theorem 5.18 of [HvLP98]. □

To describe the phases of Hermitian codes we need some technical lemmas.
We denote with N_i the set defined in the following way:

$$N_i = \{(j,k) \in \mathbb{N}^2 \mid \rho_j + \rho_k = \rho_{i+1}\}.$$

The number of elements of N_i is denoted by ν_i and let $d(i) = \min\{\nu_m \mid m \geq i\}$.

Theorem 5.2.4. *Let $d(C_i)$ be the minimum distance of C_i. Then $d(C_i) \geq d(i)$.*

Proof. See Theorem 4.13 of [HvLP98]. □

For the Hermitian codes, Theorem 5.2.4 gives the true minimum distance [YK92], that is, the distance of Hermitian code C_i is $d(i)$.

Lemma 5.2.5. *Let $i \geq 3g-1$, then $\nu_i = d(i) = i+1-g$. In general we have $d(i) \geq i+1-g$.*

Proof. See Theorem 5.24 of [HvLP98]. □

Lemma 5.2.6. *Let $\rho_{i+1} \in \Lambda_{\mathcal{H}}$ such that $\rho_{i+1} = qr + (q+1)s$.*
If $\rho_{i+1} < q^2 - 1$ then $\nu_i = (r+1)(s+1)$ and there is at least one gap in the interval $[\rho_{i+1} - \nu_i, \rho_{i+1}]$.

Proof. See Lemma 5.27 of [HvLP98]. □

Lemma 5.2.7. *Let $\rho_{i+1} \in \Lambda_{\mathcal{H}}$. If $i < g$ and $(j-1)(q+1) < \rho_{i+1} < j(q+1)$ then $d(i) = j+1$.*

Proof. See Proposition 5.28 of [HvLP98]. □

Lemma 5.2.8. *Let $\Lambda_{\mathcal{H}}$ the semigroup of the weight function of Hermitian curve $\mathcal{H}$. If $i \geq g$ then $d(i) = \min\{\rho_t \mid \rho_t \geq i+1-g\}$.*

Proof. See Theorem 5.30 of [HvLP98]. □

Lemma 5.2.9. *Let $\Lambda_{\mathcal{H}}$ the semigroup of the weight function of Hermitian curve $\mathcal{H}$. If $i = g$ then $\rho_i = 2g-2$.*

Proof. Note that $c-2$ is not a gap. In fact we can write $c-2 = q^2-q-2 = (q+1)(q-2) \in \Lambda_{\mathcal{H}}$. Since $\rho_{g+1} = c$, then $\rho_g = c-2$ as $c-2$ is a nongap. □

Finally, we define the *Goppa bound* $d_G(i)$ on the minimum distance of C_i as

$$d_G(i) = i+1-g.$$

So $d(C_i) \leq d_G(i)$.

We now report the five phases of Hermitian codes found in [HvLP98] and we analyse, for each phase, the distance and the dimension of C_i. Note that the last phase is composed only by trivial codes. So we can consider just the first four phases.

In the next section we analyse the intersection between the first two phases and the last two and we rewrite the formulae for the distance and dimension.

By Theorem 5.2.3, if $\rho_i < n$ then $\dim(C_i) = n - i = n + g - \rho_i - 1$. Otherwise, if $\rho_i \geq n$, we have that $\dim(E_i) \leq i$ so $\dim(C_i) \geq n - i$ but also $k \leq n - d + 1$ by the singleton bound.

(1) $1 \leq i < g$ and $\rho_i < 2g - 2$ by Lemma 5.2.9 and by (4) of Lemma 5.1.1.
Write $i = a(a+1)/2 + b + 1$ with $0 \leq b \leq a \leq q - 2$ and $b \neq q - 2$. Then $\rho_i = aq + b$.

If $b < a$ then we have $\rho_{i+1} = aq + b + 1$, so $(a-1)(q+1) < \rho_{i+1} < a(q+1)$, so by Lemma 5.2.7 $d(i)$ is $a + 1$.

If $a = b$ then $\rho_{i+1} = (a+1)q$. In fact $f_i = y^a$ and so $f_{i+1} = x^{a+1}$. Therefore $a(q+1) < \rho_{i+1} < (a+1)(q+1)$, so by Lemma 5.2.7 $d(i)$ is $a + 2$.

(2) $g \leq i \leq 3g - 2$ and $2g - 2 \leq \rho_i \leq 4g - 3$ by (3) of Lemma 5.1.1 and by Lemma 5.2.9.
Write $i = 3g - 1 - (a-1)q - b$ with $1 \leq a, b \leq q - 1$. By Lemma 5.2.8, we have that $d(i) = \min\{\rho_t \mid \rho_t \geq i + 1 - g = (q - a - 1)q + (q - b)\}$.

If $a < b$ then $(q - a - 1) > (q - b)$, so $(q-a-1)q + (q-b) = (r+s)q + s$ with $r = b - a - 1$ and $s = q - b$. So the smallest nongap is $d(i) = (q-a)q - b$.

If $a \geq b$ then $(q-a-1)q+(q-a) \leq (q-a-1)q+(q-b) \leq (q-a-1)q+(q-1)$, so, if we call $r = q-a$, we have that $(r-1)(q+1)+1 \leq (q-a-1)q+(q-b) \leq qr-1$. Since $1 \leq r \leq q-1$, then all integers in the interval $[(r-1)(q+1)+1, qr-1]$ are gaps. So the smallest nongap is $d(i) = (q-a)q$.

(3) $3g - 2 < i < n - g$ and $4g - 2 \leq \rho_i < n - 1$ by (3) of Lemma 5.1.1.
By Lemma 5.2.5, $d(i) = i + 1 - g = \rho_i + 2 - 2g$.

(4) $n - g \leq i < n + g$ and $n - 1 \leq \rho_i < n + 2g - 1$ by (3) of Lemma 5.1.1.
Write $i = n - g + aq + b$ with $0 \leq a \leq q - 2$, $0 \leq b \leq q - 1$.
Then $\rho_{i+1} = i + g = q(q^2 + a - b) + b(q+1)$, which means that $f_{i+1} = x^{q^2+a-b}y^b$.

If $a < b$ then $q^2 + a - b > q^2 - 1$, so by Lemma 5.2.5, $d(i) = i + 1 - g = n - 2g + aq + b + 1$.

If $a \geq b$ then the exponent of x is at least q^2, so $ev_{\mathcal{P}}(f_{i+1}) \in E_i$ and $C_i = C_{i+1}$. By Lemma 5.2.8, the minimum is

$$d(i) = d(i+1) = \{\rho_t \mid \rho_t \geq (i+1)+1-g = n-2g+aq+b+2 \geq n-2g+aq+a+2\},$$

that is, $d(i) = n - 2g + aq + a + 2$.

In this case we have that $k \leq n - d + 1 \leq n - i + g$ by singleton bound, but also $k \geq n - i$, since $\dim(E_i) \leq i$. So $1 \leq k \leq 2g$.

(5) $i \geq n + g$, then $C_i = 0$.
In fact ρ_i is at most $(q^2-1)q + (q-1)(q+1) - 1 = q^3 - q + q^2 - 2 = n + 2g - 2$, so by Lemma 5.1.1 $i \leq n + g - 1$.

5.3 Phases intersections

In this section we analyse in detail the four phases and we consider the intersection between the first and the second phase and the intersection between the last two. After that we modify the range of the first and second phase found in [HvLP98] and the formulae to compute the distance and dimension of each code with respect to the phase.

Now we focus on the intersection between the first and the second phase. We consider $i \leq g + q$, then we can write

$$i = \frac{1}{2}\alpha(\alpha+1) + \beta + 1 \quad 0 \leq \beta \leq \alpha \leq q - 1.$$

Then $\rho_i = \alpha q + \beta$ and, by (1) of Lemma 5.1.1, the number of gap $g(i) = \alpha q + \beta - i$.

We note that if $\alpha \leq q - 2$, we are in the first phase. So we just study the case $\alpha = q - 1$ and $0 \leq \beta \leq q - 1$.

We want to prove that $d(C_i) = \alpha + 1 = q$ if $i = g + \beta + 1$ with $0 \leq \beta < q - 1$, whereas if $\beta = \alpha = q - 1$, then $d(C_i) = \alpha + 2 = q + 1$.

Let $\beta \leq q - 3$ then $\rho_{i+1} = \alpha q + \beta + 1 < q^2 - 1$ so we can apply Lemma 5.2.6. We obtain $\rho_{i+1} = \alpha q + \beta + 1 = qr + (q+1)s$ where $r + s = \alpha$ and $s = \beta + 1$ and

$$\nu_i = (r+1)(s+1) = (\alpha - \beta - 1 + 1)(\beta + 1 + 1) = (q - 1 - \beta)(\beta + 2).$$

Therefore $d(i) = \min\{\nu_m \mid m \geq i\} = \min\{(q-1-\beta)(\beta+2) \mid \beta \leq q-2\} = q$. In fact we have to study the function $f(x) = (q - 1 - x)(x + 2)$ in $[0, q - 2]$, which is a concave parabola that intersects the x-axis in $q-1$ and the y-axis in $2(q-1)$. So the minimum value of $f(x)$ in the interval is exactly $f(q-2) = q$.
If $\beta = q - 2$, we have $i = g + q - 1$ and, by Lemma 5.2.8, $d(i) = \min\{\rho_t \mid \rho_t \geq i + 1 - g\} = q$, whereas if $\beta = q - 1$, we have that $i = g + q$ and so $d(i) = \min\{\rho_t \mid \rho_t \geq i + 1 - g\} = q + 1$.

We have proved that there is an intersection between the first and the second phase. In Section 7.1 we are going to study the Hermitian codes of the above mentioned extension of the first phase. For our theorems and results we need to consider the first phase as $i \leq g+q-2$ and $\rho_{i+1} < q^2-1$, that is, $\beta \leq q-2$.

So, from now on, we consider the first phase as $i \leq g+q-2$ and $\rho_{i+1} \leq q^2-2$.

Since we changed the parameters of first phase, we have to modify also the second phase. Let $g+q \leq i \leq 3g-2$ and $q^2-1 \leq \rho_i \leq 4g-3$ by (3) of Lemma 5.1.1.
Let $i = 3g-2-(a-1)q-b$ with $1 \leq a \leq q-2$ and $0 \leq b \leq q-2$. By Lemma 5.2.8, we have that $d(i) = \min\{\rho_t \mid \rho_t \geq i+1-g = (q-a-1)q+(q-b-1)\}$. The proof to find the distance is similar to the above proof. In fact

If $a \leq b$ then $(q-a-1) \geq (q-b-1)$, so $(q-a-1)q+(q-b-1) = (r+s)q+s$ with $r = b-a-1$ and $s = q-b-1$. So $d(i) = (q-a)q-b-1$.

If $a > b$ then $(q-a-1)q+(q-a) < (q-a-1)q+(q-b-1) \leq (q-a-1)q+(q-1)$, so, if we call $r = q-a$, we have that $(r-1)(q+1)+1 \leq (q-a-1)q+(q-b) \leq qr-1$. Since $1 \leq r \leq q-2$, then all integers in the interval $[(r-1)(q+1)+1, qr-1]$ are gaps. So the smallest nongap is $d(i) = qr = (q-a)q$.

We know that the dual of a Hermitian code it is also a Hermitian code. In particular $(C(m,q))^{\perp} = C(m_{\perp}, q)$, where $m_{\perp} = n+2g-2-m$.

So we analyse codes of the fourth phase as dual of Hermitian codes of the first one. In this way we find an intersection between third and fourth phase and a single formula for the distance.

We consider $i_{\perp}$ the index of our first phase, that is, $i_{\perp} = a(a+1)/2+b+1$ with $0 \leq b \leq a \leq q-1$ and $b \neq q-1$. Then $\rho_{i_{\perp}} = aq+b$. So

$$\rho_i = n+2g-2-\rho_{i_{\perp}} = n+2g-2-aq-b$$

and i, by (3) of Lemma 5.1.1, is $i = n+g-1-aq-b$.

Note that, since fourth phase codes are dual of first phase codes, we have that, for $n-g \leq i < n+g$, there are not $n+g-(n-g) = 2g$ but only $2g-2 = g$ codes. For this reason, even if we do not obtain all values of i, we can write $i = n+g-1-aq-b$ with $0 \leq b \leq a \leq q-1$ and $b \neq q-1$. So in this case we can apply Lemma 5.2.5 obtaining $d(i) = n-aq-b$.
As regards the dimension of these Hermitian codes it is exactly $i_{\perp} = a(a+1)/2+b+1$.

Note that the third phase has some regularity, that is, for any step the dimension is decreasing by one and the distance is increasing by one.
To study these codes, it is better to have the third phase as large as possible. For this reason we restrict the range of our fourth phase and we consider the fourth phase as $n - g \leq i < n + g$ and $n - 1 \leq \rho_i < n + 2g - 1$ where

$$\rho_i = n + 2g - 2 - aq - b \text{ with } 0 \leq b \leq a \leq q - 2.$$

We can do that since the codes $C(n, q)$ and $C(n - 1, q)$ are the same.
Obviously the minimum distance and the dimension do not change.

We report in Table 5.1 the explicit formulae linking the dimension and the distance of Hermitian Codes $C_i = C(m, q)$.

From Figure 5.1 and Figure 5.2 it is easy to understand our decision for the classification of Hermitian codes. In particular in Figure 5.1 all Hermitian codes over $\mathbb{F}_q$ with $q = 3$, divided by phases, are represented. Whereas, in Figure 5.2 we plotted some Hermitian codes over $\mathbb{F}_q$ with $q = 4$. In this figure we do not report all codes of phase 3 since they all stand on a single line.

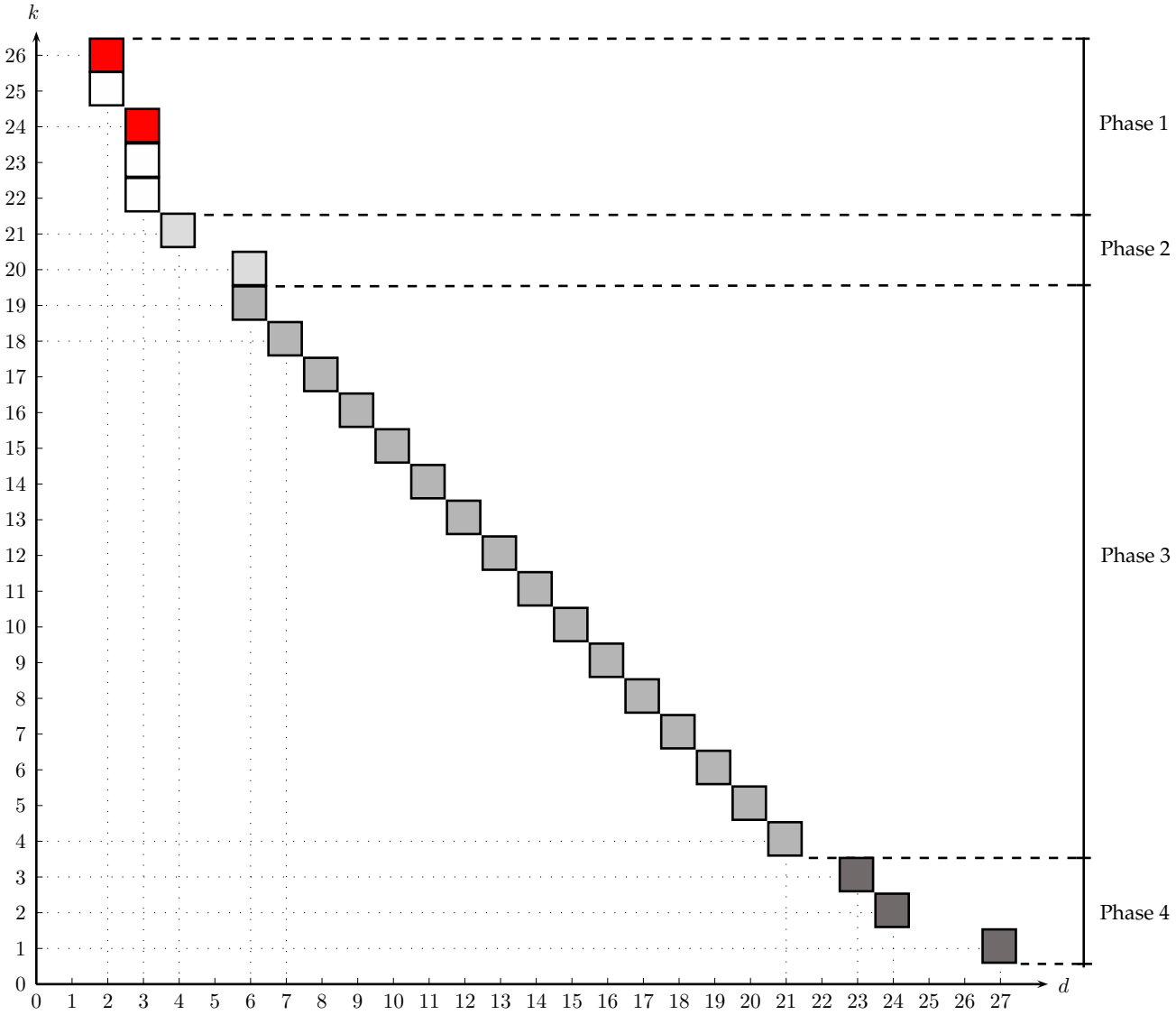


Figure 5.1: Hermitian codes with $q = 3$.

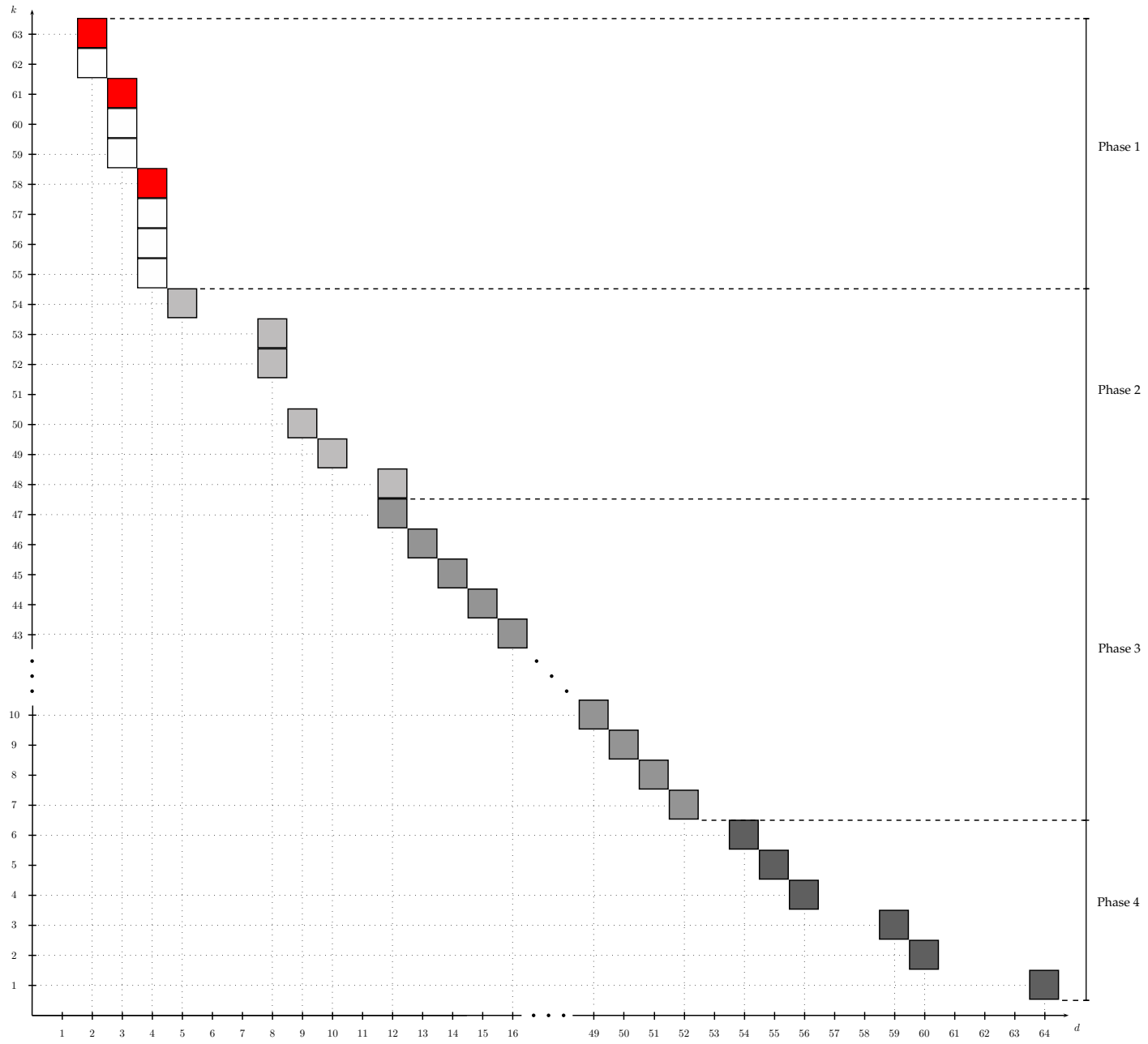


Figure 5.2: Hermitian codes with $q = 4$.

Phase	**i**	$\rho_i = \mathbf{m}$	**Distance d**	**Dimension k**
1	$1 \leq i \leq g+q-1$	$0 \leq m \leq q^2-2$ $m = aq+b$ $0 \leq b \leq a \leq q-1$ $b \neq q-1$	$\begin{matrix} a+1 & \text{if } a > b \\ a+2 & \text{if } a = b \end{matrix} \implies d \leq q$	$n - \frac{a(a+1)}{2} - b - 1$
2	$g+q \leq i \leq 3g-2$	$q^2-1 \leq m \leq 4g-3$ $m = 2q^2-q-aq-b-3$ $1 \leq a \leq q-2$ $0 \leq b \leq q-2$	$\begin{matrix} (q-a)q-b-1 & a \leq b \\ (q-a)q & a > b \end{matrix}$	$n-g-q^2+aq+b+2$
3	$3g-1 \leq i \leq n-g-1$	$4g-2 \leq m \leq n-2$	$m-2g+2$	$n-m+g-1$
4	$n-g \leq i \leq n+g-1$	$n-1 \leq m \leq n+2g-2$ $m = n+2g-2-aq-b$ $0 \leq b \leq a \leq q-2,$	$n-aq-b$	$\frac{a(a+1)}{2}+b+1$

Table 5.1: The four phases of Hermitian codes

Part II

Main Results

Intersections between the Hermitian curve $\mathcal{H}$ and parabolas

In this chapter, we report our results in [MPS12].

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, and let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime. We call α a primitive element of $\mathbb{F}_{q^2}$, and we consider $\beta = \alpha^{q+1}$ as a primitive element of $\mathbb{F}_q$.
We recall the definition of the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$ (Section 3.1), i.e.

$$x^{q+1} = y^q + y.$$

Given two curves X and Y lying in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ it is interesting to know the number of (affine plane) points that lie in both curves, disregarding multiplicity. We call this number *their planar intersection*. This knowledge may have applications for the codes constructed from X and Y. As regards $\mathcal{H}$, it is interesting for coding theory applications [Cou11, BR12a, BR12b, FM11] to consider an arbitrary parabola $y = ax^2 + bx + c$ over $\mathbb{F}_{q^2}$ and to compute their planar intersection. Moreover, it is essential to know precisely the number of parabolas having a given planar intersection with $\mathcal{H}$. Only partial results were known [DD10, DDK09], we present here for the first time a complete classification in the following theorem.

Theorem 6.0.1. *For q odd, the only possible planar intersections of $\mathcal{H}$ and a parabola are $\{0, 1, q-1, q, q+1, 2q-1, 2q\}$. For any possible mutual intersection we provide in the next tables the exact number of parabolas sharing that value.*

$\#\mathcal{H} \cap$ parabola	0	1	$q-1$
# parabolas	$q^2(q+1)\frac{(q-1)}{2}$	$q^2(q+1)\frac{q(q-3)}{2}$	$q^2(q+1)\frac{q(q-1)^2}{2}$

$\#\mathcal{H} \cap$ parabola	q	$q+1$
# parabolas	$q^2(q+1)(q^2-q+1)$	$q^2(q+1)\frac{q(q-1)(q-3)}{2}$

$\#\mathcal{H}\cap$ parabola	$2q-1$	$2q$
# parabolas	$q^2(q+1)\frac{q(q-1)}{2}$	$q^2(q+1)\frac{(q-1)}{2}$

For q even, the only possible planar intersections of $\mathcal{H}$ and a parabola are $\{1, q-1, q+1, 2q-1\}$. For any possible mutual intersection we provide in the next tables the exact number of parabolas sharing that value.

$\#\mathcal{H}\cap$ parabola	1	$q-1$
# parabolas	$q^3(q+1)(\frac{q}{2}-1)$	$q^3(q+1)(q-1)\frac{q}{2}$

$\#\mathcal{H}\cap$ parabola	$q+1$	$2q-1$
# parabolas	$q^3(q+1)(q-1)(\frac{q}{2}-1)$	$q^3(q+1)\frac{q}{2}$

We begin with some simple lemmas.

First of all, we recall (Section 3.1) that the *Norm* N and the *Trace* Tr are two functions $\mathrm{N}, \mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ such that $\mathrm{N}(x) = x^{q+1}$ and $\mathrm{Tr}(x) = x^q + x$.

Using these functions, we define the map $F_a : \mathbb{F}_{q^2} \to \mathbb{F}_q$ such that

$$F_a(x) = \mathrm{N}(x) - \mathrm{Tr}(ax^2). \tag{6.1}$$

We can note that the following property holds for the function F_a:

Lemma 6.0.2. *If $\omega \in \mathbb{F}_q$, then $F_a(\omega x) = \omega^2 F_a(x)$.*

Proof. Since $\omega \in \mathbb{F}_q$, we have $F_a(\omega x) = \mathrm{N}(\omega x) - \mathrm{Tr}(a(\omega x)^2) = \omega^{q+1}x^{q+1} - a^q\omega^{2q}x^{2q} - a\omega^2x^2 = \omega^2(x^{q+1} - a^qx^{2q} - ax^2) = \omega^2 F_a(x)$. □

Lemma 6.0.3. *Let $t \in \mathbb{F}_{q^2}^*$, then there is a solution of $x^{q-1} = t$ if and only if $\mathrm{N}(t) = 1$. In this case, $x^{q-1} = t$ has exactly $(q-1)$ distinct solutions in $\mathbb{F}_{q^2}$.*

Proof. We consider the function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that $f(x) = x^{q-1}$. We want to prove that $t \in \mathrm{Im}(f) \iff \mathrm{N}(t) = 1$.
We can note that if $t = \alpha^{\lambda(q-1)}$ for any λ, then $x = \alpha^\lambda$ is a solution of $x^{q-1} = t$. We claim that the solutions are:

$$x = \alpha^{\lambda + k(q+1)} \text{ with } 0 \le k \le q-2.$$

In fact $(\alpha^{\lambda+k(q+1)})^{q-1} = \alpha^{\lambda(q-1)} = t$ for $0 \le k \le q-2$. So if the equation $x^{q-1} = t$ has at least one solution, then it has at least $q-1$ distinct solutions. Since the equation

degree is $q-1$, then it has exactly $q-1$ distinct solutions.
Further we can note that if $t \in \mathrm{Im}(f) \implies \mathrm{N}(t) = 1$. In fact $\mathrm{N}(t) = t^{q+1} = (x^{q-1})^{q+1} = 1$. So $\mathrm{Im}(f) \subset \{t \mid \mathrm{N}(t) = 1\}$. But $|\mathrm{Im}(f)| = q+1$ and $|\{\mathrm{N}(t) = 1\}| = q+1$ hence $\mathrm{Im}(f) = \{t \mid \mathrm{N}(t) = 1\}$. □

Remark 6.0.4. We note that $4\mathrm{N}(a) = \mathrm{N}(2a)$ for any $a \in \mathbb{F}_{q^2}$.

Lemma 6.0.5. *If q is odd and $4\mathrm{N}(a) = 1$ then a is a square in $\mathbb{F}_{q^2}$.*

Proof. Let $a = \alpha^k$, so that $4\mathrm{N}(a) = 1 \implies 4\alpha^{k(q+1)} = 1 \implies 4\beta^k = 1$. Since 4 is a square in $\mathbb{F}_q$, we have

$$4 = \beta^{2t} \implies \beta^{2t+k} = 1 \implies 2t + k \equiv 0 \mod q-1,$$

so that k is even and a is a square. □

We recall a well-known result in linear algebra:

Lemma 6.0.6. *Let $f : V \to W$ be a linear function and $f(\bar{a}) = a \in \mathrm{Im}(f)$. Then $f^{-1}(a) = \bar{a} + \ker(f)$ and*

$$\dim \ker(f) + \dim \mathrm{Im}(f) = \dim V.$$

Lemma 6.0.7. *For any $a \in \mathbb{F}_{q^2}$, let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, $f(x) = 2ax - x^q$. Then f is $\mathbb{F}_q$-linear.*

Proof.

$$\begin{array}{lrcl} \forall\, c, d \in \mathbb{F}_{q^2}, & f(c+d) & = & 2ac - c^q + 2ad - d^q = f(c) + f(d). \\ \forall\, c \in \mathbb{F}_{q^2}, \quad \forall\, k \in \mathbb{F}_q \text{ then} & f(kc) & = & 2akc - k^q c^q = 2akc - kc^q = kf(c). \end{array}$$

□

Because of Lemma 6.0.7 and Lemma 6.0.6 we have the following corollary:

Corollary 6.0.8. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that $f(x) = 2ax - x^q$. Then the equation $f(x) = k$ has q distinct solutions if $k \in \mathrm{Im}(f)$, otherwise it has 0 solutions.*

Lemma 6.0.9. *Let $y = ax^2 + bx + \bar{c}$ and $y = ax^2 + bx + c$ be two parabolas. If $\mathrm{Tr}(\bar{c}) = \mathrm{Tr}(c)$, then the planar intersections between the Hermitian curve $\mathcal{H}$ and the parabolas are the same.*

Proof. From a set $\{y = ax^2 + bx + \bar{c}\} \cap \mathcal{H}$ and another set $\{y = ax^2 + bx + c\} \cap \mathcal{H}$ we obtain by direct substitution respectively $x^{q+1} = a^q x^{2q} + ax^2 + b^q x^q + bx + \mathrm{Tr}(\bar{c})$ and $x^{q+1} = a^q x^{2q} + ax^2 + b^q x^q + bx + \mathrm{Tr}(c)$. If $\mathrm{Tr}(\bar{c}) = \mathrm{Tr}(c)$, the two equations are identical. □

For the proof of Theorem 6.0.1, we will need to apply the automorphism of Hermitian curve to the parabolas. We recall the automorphism of Hermitian curve (3.3) (Section 3.3):

$$\begin{cases} x \longmapsto x + \gamma \\ y \longmapsto y + \gamma^q x + \delta \end{cases} \qquad \text{with } (\gamma, \delta) \in \mathcal{H}.$$

If we apply (3.3) to $y = ax^2$, we obtain

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta, \tag{6.2}$$

while if we apply (3.3) to $y = ax^2 + c$ we obtain

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta + c. \tag{6.3}$$

In the general case, if we have $y = ax^2 + bx + c$ and apply the automorphism (3.3) we obtain

$$y = ax^2 + (2a\gamma - \gamma^q + b)x + a\gamma^2 + b\gamma - \delta + c. \tag{6.4}$$

To prove Theorem 6.0.1, we have to study two distinct cases depending on the field characteristic. Section 6.1 is devoted to the proof of Theorem 6.0.1 when the characteristic is odd, while Section 6.2 is devoted to the proof of Theorem 6.0.1 when the characteristic is even.

6.1 Odd characteristic

In this section, q is always odd.

6.1.1 Intersection between $\mathcal{H}$ and $y = ax^2 + c$

Intersecting a parabola of the form $y = ax^2 + c$ with the Hermitian curve, we obtain $x^{q+1} = a^q x^{2q} + ax^2 + \mathrm{Tr}(c)$ which is equivalent to

$$\mathrm{N}(x) - \mathrm{Tr}(ax^2) = F_a(x) = \mathrm{Tr}(c). \tag{6.5}$$

We have to study the number of solutions of (6.5). From this equation we get $a^q x^{2q} - x^{q+1} + ax^2 = -\mathrm{Tr}(c)$, that is,

$$x^2(a^q x^{2q-2} - x^{q-1} + a) = -\mathrm{Tr}(c). \tag{6.6}$$

Now we set $x^{q-1} = t$ and we factorize the polynomial $a^q t^2 - t + a$ in $\mathbb{F}_{q^2}[t]$, obtaining

$$t_{1,2} = \frac{1 \pm \sqrt{1 - 4\mathrm{N}(a)}}{2a^q} = \frac{1 \pm \sqrt{\Delta}}{2a^q}$$

where $\Delta = 1 - 4\mathrm{N}(a)$. So equation (6.6) becomes

$$a^q x^2 \left(x^{q-1} - \frac{1+\sqrt{\Delta}}{2a^q} \right) \left(x^{q-1} - \frac{1-\sqrt{\Delta}}{2a^q} \right) = -\mathrm{Tr}(c). \tag{6.7}$$

Since $\Delta \in \mathbb{F}_q$, there is $z \in \mathbb{F}_{q^2}$ such that $\Delta = z^2$, and so the equation (6.7) is in $\mathbb{F}_{q^2}[x]$. Note that

$$\Delta = 0 \iff \mathrm{N}(2a) = 1.$$

So, in this special case, (6.7) becomes $a^q x^2 (x^{q-1} - 2a)^2 = -\mathrm{Tr}(c)$. We have proved the following lemma:

Lemma 6.1.1. *By intersecting a parabola $y = ax^2 + c$, where $\mathrm{N}(2a) = 1$, and the Hermitian curve, we obtain the following equation*

$$a^q x^2 (x^{q-1} - 2a)^2 = -\mathrm{Tr}(c).$$

Recall that α is a primitive element of $\mathbb{F}_{q^2}$ and $\beta = \alpha^{q+1}$ is a primitive element of $\mathbb{F}_q$.

Lemma 6.1.2. *Let $x = \alpha^j \beta^i$, with $j = 0, \ldots, q$ and $i = 0, \ldots, q-2$. Then*

- *If $4\mathrm{N}(a) \neq 1$, then the non-zero values $F_a(\alpha^j \beta^i)$ give us all the elements of $\mathbb{F}_q^*$.*
- *If $4\mathrm{N}(a) = 1$, then the non-zero values $F_a(\alpha^j \beta^i)$ give us half of the elements of $\mathbb{F}_q^*$.*

Proof. We fix an index j such that $F_a(\alpha^j) \neq 0$. The set of the values

$$\{F_a(\alpha^j \beta^i)\}_{0 \leq i \leq q-2} = \{\beta^{2i} F_a(\alpha^j)\}_{0 \leq i \leq q-2}$$

contains half of the elements of $\mathbb{F}_q^*$, since q is odd (and $\frac{q-1}{2}$ is an integer) and so $\beta^{2(\frac{q-1}{2})} = \alpha^{q^2-1} = 1$.
If $4\mathrm{N}(a) = 1$, by Lemma 6.1.1, $F_a(x)$ becomes $-a^q x^2 (x^{q-1} - 2a)^2$, so $\beta^{2i} F_a(\alpha^j) = -a^q \beta^{2i} (\alpha^{jq} - 2a\alpha^j)^2$, and give us half of the elements of $\mathbb{F}_q^*$, that are all square of $\mathbb{F}_q^*$.
If $4\mathrm{N}(a) \neq 1$, by varying j, we can obtain every element of $\mathbb{F}_q^*$.
In fact, $F_a(x) = -x^2 (a^q x^{2q-2} + a - x^{q-1})$, so

$$F_a(\alpha^j) = \mathrm{N}(\alpha^j) - \mathrm{Tr}(a(\alpha^j)^2) = \beta^j - a\alpha^{2j} - a^q \alpha^{2jq} = \beta^j - \beta^{r_j},$$

where $0 \leq r_j \leq q-2$ and $\beta^{2i} F_a(\alpha^j) = \beta^{2i+j} - \beta^{2i+r_j}$, that are all elements of $\mathbb{F}_q^*$.

□

Now we study the number of solutions of equation (6.5), analysing two cases: when $\mathrm{Tr}(c) = 0$ and when $\mathrm{Tr}(c) \neq 0$.

$*$ Case $\mathrm{Tr}(c) = 0$. By Lemma 6.0.9, it is enough to study the case $c = 0$, which is the intersection between $\mathcal{H}$ and $y = ax^2$. By (6.7) we have

$$a^q x^2 \left(x^{q-1} - \frac{1+\sqrt{\Delta}}{2a^q} \right) \left(x^{q-1} - \frac{1-\sqrt{\Delta}}{2a^q} \right) = 0.$$

We must differentiate our argument depending on Δ. Recall that $\Delta \in \mathbb{F}_q$.

- $\Delta = 0$. By Lemma 6.1.1, (6.7) becomes

  $$a^q x^2 (x^{q-1} - 2a)^2 = 0.$$

  So we have always one solution $x = 0$ and the solutions of $x^{q-1} = 2a$. Since $\mathrm{N}(2a) = 1$, by Lemma 6.0.3, the number of solutions of $x^{q-1} = 2a$ are $q-1$. Therefore, in this case, we have q points of intersections between the parabola and the Hermitian curve $\mathcal{H}$.

  By condition on a, i.e. $\mathrm{N}(2a) = 1$, we have $(q+1)$ distinct a's.

- $\Delta = 1$. That is, $\mathrm{N}(2a) = 0 \iff a = 0$, which is impossible.

- $\Delta \in \mathbb{F}_q \backslash \{0, 1\}$. We note that any element in $\mathbb{F}_q$ can always be written as z^2 with $z^2 \in \mathbb{F}_{q^2}$. In order to study the solutions of (6.7), we can consider the solutions of the following equations

  $$x^{q-1} = \frac{1 \pm z}{2a^q}. \tag{6.8}$$

  By Lemma 6.0.3 we know that $x^{q-1} = \frac{1+z}{2a^q}$ has some solutions if and only if $\mathrm{N}\left(\frac{1+z}{2a^q}\right) = 1$. Note that

  $$\mathrm{N}\left(\frac{1+z}{2a^q}\right) = 1 \iff \frac{(1+z)^{q+1}}{1-z^2} = 1 \iff 1 - z = (1+z)^q \iff -z = z^q$$

  We obtain the same result for $x^{q-1} = \frac{1-z}{2a^q}$.
  If (6.8) has a solution x and $z \in \mathbb{F}_q$, then z simultaneously satisfies $z^q = z$ and $z^q = -z$. Since q is odd, this is possible only when $z = 0$, which implies $\Delta = 0$, which is not admissible.

  Returning to count the intersection points, thanks to the previous discussion of the solution of (6.8), we have to consider two distinct cases:

  1. $z = z^q$, that is, $z \in \mathbb{F}_q$. Since $z \neq 0, 1$, there are $\frac{q-1}{2} - 1 = \frac{q-3}{2}$ possible values of z^2, and so we have $(q+1)\frac{q-3}{2}$ values of a. In this case, the parabola $y = ax^2 + c$ intersects $\mathcal{H}$ in only *one* point (with $x = 0$).

2. $z = -z^q$. The equation $-z = z^q$ has only one solution in $\mathbb{F}_q$, so the other $q-1$ solutions are in $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$. For such z, we have $2(q-1)+1 = 2q-1$ points of intersection. That is, $q-1$ solutions from equation $x^{q-1} = \frac{1-z}{2a^q}$, $q-1$ solutions from equation $x^{q-1} = \frac{1+z}{2a^q}$ and one point from $x = 0$.
It is simple to verify that the number of z^2 such that $z \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ is $\frac{q-1}{2}$. So we have $(q+1)\frac{q-1}{2}$ values of a for which we have exactly $2q-1$ points of intersection between $y = ax^2 + c$ and $\mathcal{H}$.

Now we apply the automorphism (3.3) and we want to compute how many different parabolas we can obtain. Applying (3.3) to $y = ax^2$ we obtain (6.2):

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta.$$

For the moment, we restrict our counting argument to the case $\Delta \neq 0$. We note that if $\Delta \neq 0$, we have a maximal orbit, that is, all possible parabolas are distinct (there are q^3 because Γ has q^3 elements). In other words, we claim that it is impossible that we obtain two equal parabolas with $(\gamma, \delta) \neq (\bar{\gamma}, \bar{\delta})$. To prove that, we have to solve the following system:

$$\begin{cases} 2a\bar{\gamma} - \bar{\gamma}^q = 2a\gamma - \gamma^q \\ a\bar{\gamma}^2 - \bar{\delta} = a\gamma^2 - \delta \\ \gamma^{q+1} = \delta^q + \delta \\ \bar{\gamma}^{q+1} = \bar{\delta}^q + \bar{\delta} \\ 1 - 4a^{q+1} \neq 0. \end{cases}$$

However, $2a\bar{\gamma} - \bar{\gamma}^q = 2a\gamma - \gamma^q \iff 2a(\bar{\gamma} - \gamma) = \bar{\gamma}^q - \gamma^q = (\bar{\gamma} - \gamma)^q \implies 4a^{q+1}(\bar{\gamma} - \gamma)^q(\bar{\gamma} - \gamma) = (\bar{\gamma} - \gamma)(\bar{\gamma} - \gamma)^q \iff 4a^{q+1} = 1$. And it is impossible, since $\Delta \neq 0$.
Hence, when $\Delta \neq 0$, we have exactly q^3 distinct parabolas that have the same planar intersections with $\mathcal{H}$ as $y = ax^2$ has.

* Case $y = ax^2 + c$, with $\mathrm{Tr}(c) \neq 0$. As in previous case, we have to differentiate depending on Δ.

  - If $\Delta = z^2$ and $z \in \mathbb{F}_q$, we know that $F_a(x)$ vanishes only if $x = 0$. If $x \neq 0$, then by Lemma 6.1.2, $F_a(\beta^i\alpha^j) = \beta^{2i}F_a(\alpha^j) = t$ assumes every value of $\mathbb{F}_q^*$. But $x = \beta^i\alpha^j$ assumes q^2-1 distinct values, varying i and j. So every t is obtained $q+1$ times ($F_a(x)$ is a polynomial of degree $q+1$). Hence, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q+1$ solutions.

- If $\Delta = z^2$ and $z \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, we know that $F_a(x) = 0$ has $2q-1$ solutions. So there are exactly two distinct values of j such that $F_a(\alpha^j) = 0$, one for each equation $x^{q-1} = \frac{1 \pm z}{2a^q}$ (to find the $q-1$ solutions, we vary i). So every value in $\mathbb{F}_q^*$ is obtained $q-1$ times. Hence, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q-1$ solutions.

- If $\Delta = 0$ we have $4a^{q+1} = 1$.
  So (6.1) can be written as $a^q x^2 (x^{q-1} - 2a)^2 = -\mathrm{Tr}(c)$, that is,

$$x^2 (x^{q-1} - 2a)^2 = -4a\mathrm{Tr}(c) = -4a\beta^r \tag{6.9}$$

  for some fixed r with $1 \leq r \leq q-1$.
  Note that (6.9) can be written as $f(x)^2 = -4a\mathrm{Tr}(c)$, where f is as in Lemma 6.0.7, that is, $f(x) = x^q - 2ax$.
  We note that $-4a\beta^r$ is always a square in $\mathbb{F}_{q^2}$. In fact $-4\beta^r$ is a square because it lies in $\mathbb{F}_q$, and also a is a square by Lemma 6.0.5. Let us write $-4a\beta^r = \alpha^{2h}$, so (6.9) becomes $x(x^{q-1} - 2a) = \pm\, \alpha^h$ where $0 \leq h \leq \frac{q^2-1}{2}$.
  We consider the "positive" case:

$$f(x) = x^q - 2ax = \alpha^h. \tag{6.10}$$

  It is simple to prove that if x is a solution of equation (6.10), then $-x$ is a solution of the equation $x^q - 2ax = -\alpha^h$. So by Corollary 6.0.8 the equation $F_a(x) = \mathrm{Tr}(c)$ has 0 solutions if α^h is not in $\mathrm{Im}(f)$ or $2q$ solution if α^h is in $\mathrm{Im}(f)$.

6.1.2 Intersection between $\mathcal{H}$ and $y = ax^2 + bx + c$

We consider a parabola $y = ax^2 + bx + c$, apply the automorphism (3.3) and we obtain (6.4).
Note that, for any $k \in \mathbb{F}_{q^2}$,

$$2a\gamma - \gamma^q + b = k \implies 2ab^q + b = 2ak^q + k, \tag{6.11}$$

because $b^q = (k - 2a\gamma + \gamma^q)^q = k^q - \frac{1}{2a}\gamma^q + \gamma = k^q + \frac{1}{2a}(-\gamma^q + 2a\gamma) = k^q + \frac{1}{2a}(k - b)$.

A consequence is that $2a\gamma - \gamma^q + b = 0 \implies 2ab^q + b = 0$.

We consider two distinct cases $2a\gamma - \gamma^q + b = 0$ and $2a\gamma - \gamma^q + b \neq 0$.

$\boxed{2a\gamma - \gamma^q + b \neq 0.}$

Theorem 6.1.3. *Let $y = ax^2 + bx + c$ be a parabola with $2ab^q + b \neq 0$ and $\mathrm{N}(2a) = 1$. Then there exists γ such that for any δ, applying the automorphism (3.3), we obtain $y = ax^2 + (2a\gamma - \gamma^q + b)x + a\gamma^2 + b\gamma - \delta + c$, with $2a\gamma - \gamma^q + b \neq 0$. We can write any such parabola as $y = (ux + uv)^2$ where $a = u^2$ and $v^q + 2av \neq 0$.*

Proof. Because of (6.11) with $k \neq 0$ we have that, since $2ab^q + b \neq 0$, then $\exists\, \gamma$ such that $2a\gamma - \gamma^q + b \neq 0$.
Let $k \in \mathbb{F}_{q^2}$ such that $2a\gamma - \gamma^q + b = k \neq 0$. By Corollary 6.0.8, if there exists at least one solution of $2a\gamma - \gamma^q = k - b$, then there exists q solutions. So we have at least q different γ's that verify the previous equation.
To prove that any parabola as in (6.4) can be written as $y = (ux + uv)^2$ with $a = u^2$ and $v^q + 2av \neq 0$, it is sufficient to prove that the solutions of the following system contain all c's.

$$\begin{cases} 2a\gamma - \gamma^q + b = 2av \neq 0 \\ a\gamma^2 + b\gamma - \delta + c = av^2 \neq 0 \\ \gamma^{q+1} = \delta^q + \delta \\ 1 - 4a^{q+1} = 0 \end{cases}$$

Using (6.11) the first equation of system $2a\gamma - \gamma^q + b = 2av$ implies that $v^q + 2av \neq 0$. In fact if we consider (6.11) with $k = 2av$, we have $0 \neq 2ab^q + b = 2ak^q + k = 2a(2av)^q + 2av = v^q + 2av$.
By the second equation we have $c = \delta + av^2 - a\gamma^2 - b\gamma$. So for any γ (and there are q possible γ's), there are q distinct δ's (by the curve equation). So we have q^2 different c's, that is, all possible c's.
Finally, we can write (6.4) as $y = a(x + v)^2$. By Lemma 6.0.5, $a = u^2$ is a square so $y = (ux + uv)^2$. □

Theorem 6.1.4. *Let $a, v \in \mathbb{F}_{q^2}$ such that $\mathrm{N}(2a) = 1$ and $v^q + 2av \neq 0$. Then the Hermitian curve $\mathcal{H}$ intersects the parabola $y = a(x + v)^2$ in q points.*

Proof. We have to solve the system

$$\begin{cases} y = (ux + uv)^2 \\ x^{q+1} = y^q + y \end{cases} \implies x^{q+1} = (ux + uv)^{2q} + (u + uv)^2$$

By a change of variables $z = ux + uv$, we obtain $(\frac{z - uv}{u})^{q+1} = z^{2q} + z^2$, so we have

$$-(uv)z^q - (uv)^q z + (uv)^{q+1} = u^{q+1}z^{2q} + u^{q+1}z^2 - z^{q+1} = u^{q+1}(z^q - 2u^{q+1}z)^2.$$

Since $\mathrm{N}(2a) = 1$ and $a = u^2$, we have $u^{q+1} = \pm\frac{1}{2}$ and so

$$\frac{1}{2}(z^q - z)^2 = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) \tag{6.12}$$

$$-\frac{1}{2}(z^q + z)^2 = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) \tag{6.13}$$

We consider two cases:

* If $u^{q+1} = \frac{1}{2}$, we can note that $(z^q - z)^2$ is not a square in $\mathbb{F}_q$ if $z^q - z \neq 0$.
  In fact, suppose by contradiction that $(z^q - z)^2 = \beta^{2r}$, then $z^q - z = \beta^r \in \mathbb{F}_q$ but also $z^q + z \in \mathbb{F}_q$, so $-2z \in \mathbb{F}_q \iff z \in \mathbb{F}_q$ and so $z^q - z = 0$, which is impossible.

* If $u^{q+1} = -\frac{1}{2}$, we can note that $(z^q + z)^2$ is a square in $\mathbb{F}_q$, because $z^q + z \in \mathbb{F}_q$.

Let $t = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q)$. So $t \in \mathbb{F}_q$. Due to (6.12) we have $2t = (z^q - z)^2$, while (6.13) becomes $-2t = (z^q + z)^2$.

When $u^{q+1} = \frac{1}{2}$, we have $\frac{q-1}{2}$ values of t (that are all the non-squares) and $t = 0$, whereas when $u^{q+1} = -\frac{1}{2}$, we have $\frac{q-1}{2}$ values of t (that are all the squares) and $t = 0$.
Now we consider separately the cases $t = 0$ and $t \neq 0$.

- We claim that if $t = 0$ and $u^{q+1} = \pm\frac{1}{2} \implies z \in \mathbb{F}_q$. Whereas if $t = 0$ and $u^{q+1} = -\frac{1}{2} \implies z \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. We show only the case $u^{q+1} = \frac{1}{2}$. With these assumptions (6.12) becomes

  $$-(uv)z^q - (uv)^q z + (uv)^{q+1} = 0 \iff z = \frac{(uv)^{q+1}}{(uv)^q + uv}.$$

  We can note that since $v^q + 2av \neq 0$, then $(uv)^q + uv \neq 0$. In fact, suppose that $v^q + 2av = 0$, then $(uv)^q + uv = -\frac{1}{2u}2av + uv = 0$.
  We have to verify that $z^q = z$. Indeed $z^q = \frac{(uv)^{q+1}}{uv+(uv)^q} = z$.
  Similar computations (here omitted) show the case $u^{q+1} = -\frac{1}{2}$.

- We claim that if $t \neq 0$ and $u^{q+1} = \pm\frac{1}{2} \implies z \notin \mathbb{F}_q$. With these assumptions, we show only the case $u^{q+1} = \frac{1}{2}$. We have $(z^q - z)^2 = 2t = \alpha^{2r}$, that is, $z^q = z \pm \alpha^r$. Now we substitute z^q in $-(uv)z^q - (uv)^q z + (uv)^{q+1} = t$ and we obtain $-(uv)(\pm\alpha^r + z) - (uv)^q z + (uv)^{q+1} = \frac{1}{2}\alpha^{2r}$, that is,

  $$z = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \mp uv\alpha^r}{\mathrm{Tr}(uv)} \tag{6.14}$$

We can note that $\alpha^{qr} = -\alpha^r$, in fact $2t = \alpha^{2r} \in \mathbb{F}_q$, so $(\alpha^{2r})^q = \alpha^{2r}$, that is, $\alpha^{rq} = \pm\alpha^r$ but $\alpha^r \notin \mathbb{F}_q$ (since $2t$ is not a square in $\mathbb{F}_q$) so $\alpha^{qr} = -\alpha^r$. We have thus proved

$$z = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \mp uv\alpha^r}{\mathrm{Tr}(uv)} \text{ and } z^q = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \pm (uv)^q\alpha^r}{\mathrm{Tr}(uv)}$$

Now we have to verify that the two z's as in (6.14) are solutions of (6.12). We have $z^q - z = \pm\alpha^r$ and $\mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) = t$. So

$$\pm\alpha^r = z^q - z \iff \pm\mathrm{Tr}(uv)\alpha^r = \pm(uv)^q\alpha^r \pm uv\alpha^r$$

and

$$\begin{aligned}
& (uv)^{q+1} - z(uv)^q - z^q(uv) = t \\
\iff\ & (uv)^{q+1}\mathrm{Tr}(uv) - (uv)^q((uv)^{q+1} - \tfrac{1}{2}\alpha^{2r} \mp uv\alpha^r) + \\
& -uv((uv)^{q+1} - \tfrac{1}{2}\alpha^{2r} \pm uv\alpha^r) = \mathrm{Tr}(uv)t \\
\iff\ & (uv)^{q+1}\mathrm{Tr}(uv) + t\,\mathrm{Tr}(uv) - (uv)^{2q+1} - (uv)^{q+2} = \mathrm{Tr}(uv)t \\
\iff\ & (uv)^{q+1}\mathrm{Tr}(uv) - (uv)^{2q+1} - (uv)^{q+2} = 0.
\end{aligned}$$

So the z's are solutions of (6.12).
Similar computations (omitted here) show the case $u^{q+1} = -\frac{1}{2}$.

Therefore, we have two solutions for any t not a square in $\mathbb{F}_q^*$ and we have only one solution when $t = 0$. That is, we get a total of $\frac{q-1}{2}2 + 1 = q$ intersections.

The same holds for the case with $u^{q+1} = -\frac{1}{2}$. □

Now we consider the second case.

$\boxed{2a\gamma - \gamma^q + b = 0.}$

We note that if $2a\gamma - \gamma^q + b = 0$ then $2ab^q + b = 0$, and so (6.4) is actually $y = ax^2 + c$. Now we apply the automorphism (3.3) to the parabola $y = ax^2 + c$ and we obtain (6.3). Now if

- $\Delta \neq 0$, the parabolas in (6.3) are all distinct.

  The number of values of c such that $\mathrm{Tr}(c) \neq 0$ are exactly $q^2 - q$, but we must be careful and not count twice the same parabola. In particular, if two parabolas share a and b, then they are in the same orbit if $\mathrm{Tr}(c) = \mathrm{Tr}(c')$. So we must consider only one of these for any non-zero $\mathrm{Tr}(c)$. Thus there are $q - 1$ values.

Summarizing:

* If $\Delta = z^2$ and $z \in \mathbb{F}_q$ (and $\mathrm{Tr}(c) \neq 0$), then the number of parabolas with $q+1$ intersections is

$$\underbrace{(q+1)\frac{q-3}{2}}_{a}\underbrace{q^3(q-1)}_{b,c} = \frac{1}{2}q^3(q^2-1)(q-3).$$

* If $\Delta = z^2$ and $z^q + z = 0$ (and $\mathrm{Tr}(c) \neq 0$), then the number of parabolas with $q-1$ intersections is

$$\underbrace{(q+1)\frac{q-1}{2}}_{a}\underbrace{q^3(q-1)}_{b,c} = \frac{1}{2}q^3(q+1)(q-1)^2.$$

- $\Delta = 0$, that is, $4a^{q+1} = 1$, we want to understand how many different parabolas of the type $y = ax^2 + bx + \bar{c}$ (with a fixed) we can obtain. So we have to study the number of pairs $(b, \bar{c})$.

  We note that

$$\mathrm{Tr}(\bar{c}) = a^q b^2 + \mathrm{Tr}(c). \tag{6.15}$$

  In fact

$$\begin{aligned} \mathrm{Tr}(\bar{c}) &= (a\gamma^2 - \delta)^q + a\gamma^2 - \delta + \mathrm{Tr}(c) \\ &= (a\gamma^2)^q + a\gamma^2 - \gamma^{q+1} + \mathrm{Tr}(c) = a^q\gamma^2(\gamma^{q-1} - 2a)^2 + \mathrm{Tr}(c). \end{aligned}$$

  Let $\mathrm{Tr}(c) = k$, with $k \in \mathbb{F}_q^*$. Let us consider two distinct cases:

  - $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c})$. By (6.15) we have that $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c}) \iff b = 0$.
    So the number of pairs $(0, \bar{c})$ are exactly $q^2 - q$, because they correspond to all $\bar{c} \in \mathbb{F}_{q^2}$ such that $\mathrm{Tr}(\bar{c}) \neq 0$.
  - $\mathrm{Tr}(c) \neq \mathrm{Tr}(\bar{c})$. Then $\mathrm{Tr}(\bar{c}) = a^q b^2 + k$.
    Since $b = 2a\gamma - \gamma^q$, then, by considering all possible γ's, we obtain $q-1$ distinct b's.
    In fact, we can consider the function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that $f(\gamma) = 2a\gamma - \gamma^q$. By Corollary 6.0.8, for any $t \in \mathrm{Im}(f)$, the equation $f(\gamma) = t$ has q distinct solutions.
    Since we are interested in the case $b \neq 0$, we have $\frac{(q^2-q)}{q} = q-1$ different b's. We can note that if b is a solution of the equation $2a\gamma - \gamma^q = 0$, then $-b$ is also a solution.
    Since we are interested in the pairs $(b^2, \bar{c})$, we note that we have to consider the equation $\mathrm{Tr}(\bar{c}) = a^q b^2 + k$, so the pairs $(b^2, \bar{c})$ are exactly $\frac{q-1}{2}(q^2 - q)$.

In fact there are exactly $\frac{q-1}{2}$ distinct b^2 and for any pairs (b^2, k) we have exactly q distinct $\bar{c}$'s. While the possible k's are exactly $q-1$ (because $\mathrm{Tr}(c) \neq 0$).
All possible pairs $(b, \bar{c})$ are $2\frac{q-1}{2}(q^2-q) = (q-1)(q^2-q)$.

We fix a and we obtain exactly $(q-1)(q^2-q) + q^2 - q = q^2(q-1)$ parabolas of the type $y = ax^2 + bx + \bar{c}$.

In conclusion if $\Delta = 0$ and $\mathrm{Tr}(c) \neq 0$, then we have $q^2(q+1)\frac{q-1}{2}$ parabolas with $2q$ or 0 intersections.

The last type of parabolas cannot be easily counted and so we obtain their number by difference.

Claim 6.1.5. *The number of parabolas that have q intersections with the Hermitian curve $\mathcal{H}$ is $q^2(q+1)(q^2-q+1)$.*

Proof. The number of total parabolas is $q^4(q^2-1)$. By summing all parabolas that we already counted we obtain

$$q^2(q+1)\left(2\frac{q-1}{2} + q\frac{q-1}{2}(q-1+q-3) + \frac{q}{2}(q-1+q-3)\right) =$$

$$= q^2(q+1)(q-1+q^2(q-2)).$$

So the number of parabolas that have q intersections with $\mathcal{H}$ is

$$q^4(q^2-1) - q^2(q+1)(q-1+q^2(q-2)) =$$

$$q^2(q+1)(q^2(q-1) - q + 1 - q^2(q-2)) = q^2(q+1)(q^2-q+1).$$

□

We have proved the following theorems, depending on the condition $\mathrm{Tr}(c) = 0$ or $\mathrm{Tr}(c) \neq 0$.

Theorem 6.1.6. *Let q be odd. A parabola $y = ax^2 + c$ with $\mathrm{Tr}(c) = 0$ intersects the Hermitian curve $\mathcal{H}$ in $2q-1, q$ or 1 points.*
Moreover, we have

$(q+1)\frac{q-1}{2}q^3$ parabolas that intersect $\mathcal{H}$ in $2q-1$ points.

$q^2(q+1)(q^2-q+1)$ parabolas that intersect $\mathcal{H}$ in q points.

$(q+1)\frac{q-3}{2}q^3$ parabolas that intersect $\mathcal{H}$ in one point.

Theorem 6.1.7. *Let q be odd. A parabola $y = ax^2 + c$ with $\mathrm{Tr}(c) \neq 0$ intersects the Hermitian curve $\mathcal{H}$ in $2q, q+1, q-1$ or 0 points.*
Moreover, we have

$q^2(q+1)\frac{q-1}{2}$ *parabolas that intersect $\mathcal{H}$ in $2q$ points.*

$q^3(q+1)(q-1)\frac{q-3}{2}$ *parabolas that intersect $\mathcal{H}$ in $q+1$ points.*

$q^3(q+1)\frac{(q-1)^2}{2}$ *parabolas that intersect $\mathcal{H}$ in $q-1$ points.*

$q^2(q+1)\frac{q-1}{2}$ *parabolas that intersect $\mathcal{H}$ in 0 point.*

Therefore, thanks to Theorem 6.1.6 and to Theorem 6.1.7, we obtain the first half of Theorem 6.0.1.

6.2 Even characteristic

In this section, q is always even.

We claim that it is enough to consider just two special cases: $y = ax^2$ and $y = ax^2 + c$. Before studying these two cases, we consider the following lemma:

Lemma 6.2.1. *Let $x = \alpha^j\beta^i$, with $j = 0, \dots, q$ and $i = 0, \dots, q-2$; then the values $F_a(\alpha^j\beta^i)$ that are not zero are all the elements of $\mathbb{F}_q^*$.*

Proof. Fixing a index j, by Lemma 6.0.2 we have $F_a(\alpha^j\beta^i) = \beta^{2i}F_a(\alpha^j)$. If $F_a(\alpha^j) = 0$ we have finished, otherwise $\beta^{2i}F_a(\alpha^j)$ are all elements of $\mathbb{F}_q^*$, because also β^2 is a primitive element of $\mathbb{F}_q$. □

We divide the study into two parts.

* Case $y = ax^2$. We intersect $\mathcal{H}$ with $y = ax^2$ and we obtain $x^2(a^q x^{2q-2} - x^{q-1} + a) = 0$, as in (6.6). We set $x^{q-1} = t$ and we have to solve the equation $a^q t^2 - t + a = 0$. Setting $z = ta^q$ we obtain

$$z^2 + z + a^{q+1} = 0.$$

It is known that this equation has solutions in a field of characteristic even if and only if $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{q^2}}(a^{q+1}) = 0$ (by special case of Artin - Schreier Theorem, see Theorem 6.4 of [S.02]). And this latter condition holds, since we have

$$\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{q^2}}(a^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(a^{q+1})) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(0) = 0.$$

We also have $\mathrm{N}(t) = 1$, in fact $t^{q+1} = (x^{q-1})^{q+1} = 1$. Then we have

$$z^{q+1} = \mathrm{N}(z) = \mathrm{N}(a^q) = a^{q^2+q} = a^{q+1} = \mathrm{N}(a)$$

and so the equation becomes

$$z^2 + z + z^{q+1} = 0.$$

Since $t \neq 0, z \neq 0$, then we must have

$$z^q + z = 1.$$

We can note that, since $a^{q+1} \in \mathbb{F}_q$, then it is possible to compute its trace from $\mathbb{F}_q$ to $\mathbb{F}_2$, and we obtain

$$\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(z^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(z^2+z) = z+z^2+z^2+z^4+\ldots+z^{q/2}+z^q = z+z^q.$$

If it is equal to 0, we have a contradiction, then there is not any solution $x \in \mathbb{F}_{q^2}$. On the other hand if it is equal to 1, then we have solutions.

When the solutions exist, since $z^{q+1} = a^{q+1}$, a solution z is $a\alpha^{j(q-1)}$, for some j, and the other is $z+1$, which we can write as $a\alpha^{j'(q-1)}$. From each of these we have the corresponding $t = (\frac{\alpha^j}{a})^{q-1}$ and so the x's are $\frac{\alpha^{j+i(q+1)}}{a} = \frac{\alpha^j\beta^i}{a}$ and $\frac{\alpha^{j'+i(q+1)}}{a} = \frac{\alpha^{j'}\beta^i}{a}$, with $i = 0, \ldots, q-2$.

We can summarize:

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 0$, there is only *one* solution. This happens when $a = 0$, which it is not acceptable, and for $\frac{q}{2}-1$ other values of a^{q+1}, so the possible values of a are $(\frac{q}{2}-1)(q+1)$.
- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 1$, there are $2q-1$ solutions. This happens for $\frac{q}{2}$ values of a^{q+1}, so the possible values of a are $\frac{q}{2}(q+1)$.

As in the odd case, we apply the automorphism (3.3) to the parabolas of type $y = ax^2$ and we can see that distinct automorphisms generate distinct parabolas. We omit the easy adaption of our earlier proof.
So we have proved the following theorem:

Theorem 6.2.2. *The Hermitian curve $\mathcal{H}$ and the parabola $y = ax^2$ intersect in either one point or $2q-1$ points.*
Moreover, from the application of (3.3) to these parabolas, we obtain:

$q^3(\frac{q}{2}-1)(q+1)$ *parabolas with one point of intersection with $\mathcal{H}$.*

$q^3\frac{q}{2}(q+1)$ *parabolas with $2q-1$ points of intersection with $\mathcal{H}$.*

* Case $y = ax^2 + c$ with $\mathrm{Tr}(c) \neq 0$. We consider the equation (6.1). We divide the problem into two parts:

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 0$, we know that $F_a(x)$ is equal to zero only for $x = 0$. If $x \neq 0$, then by Lemma 6.2.1 if we fix j we have that $F_a(x) = F_a(\alpha^j\beta^i) = \beta^{2i}F_a(\alpha^j)$ are all the elements of $\mathbb{F}_q^*$. But j can assume $q+1$ distinct values, so any value of $\mathbb{F}_q^*$ can be obtained $q+1$ times. So, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q+1$ solutions.

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 1$, $F_a(x) = 0$ has $2q-1$ solutions. So, if we fix an index j, the values of $F_a(\alpha^j\beta^i) = \beta^{2i}F_a(\alpha^j)$ are all equal to zero or are all the elements of $\mathbb{F}_q^*$. There are exactly two distinct values of j that give zero, so any non-zero value of $\mathbb{F}_q$ can be obtained $q-1$ times. So, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q-1$ solutions.

We apply the automorphism (3.3) to the parabola $y = ax^2 + c$ and we obtain (6.3). These are all distinct and different from those of Theorem 6.2.2, because the planar intersection of $\mathcal{H}$ and the previous parabolas are different. The number of values of c such that $\mathrm{Tr}(c) \neq 0$ are exactly $q^2 - q$, but we must be careful and not count twice the same parabola. In particular, if two parabolas share a and b, then they are in the same orbit if $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c})$. So we must consider only one of these for any non-zero value of $\mathrm{Tr}(c)$. These are $q-1$ of these values.
Summarizing, we have proved the following theorem:

Theorem 6.2.3. *The Hermitian curve $\mathcal{H}$ and the parabola $y = ax^2 + c$ with $\mathrm{Tr}(c) \neq 0$ intersect in either $q+1$ or $q-1$ points.*
Moreover, from the application of (3.3) to these parabolas, we obtain:

- $q^3(\frac{q}{2} - 1)(q+1)(q-1)$ *parabolas (with $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 0$) with $q+1$ points of intersection with $\mathcal{H}$.*
- $q^3\frac{q}{2}(q+1)(q-1)$ *parabolas (with $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 1$) with $q-1$ points of intersection with $\mathcal{H}$.*

By summing all parabolas that we have found in Theorem 6.2.2 and Theorem 6.2.3, we obtain

$$q^3(q+1)\left(\frac{q}{2} - 1 + \frac{q}{2} + (q-1)(\frac{q}{2} - 1 + \frac{q}{2})\right) =$$

$$= q^3(q+1)(q-1)(1+q-1) = q^4(q^2-1).$$

Since this is exactly the total number of the parabolas, this means that we actually considered all parabolas, and so we obtain the second half of Theorem 6.0.1.

Small-weight codewords of Hermitian codes

In this chapter we analyse the small-weight codewords of Hermitian codes of the first phase, that is, of all codes $C(m,q)$, with $m \leq q^2-2$. In particular we are able to obtain geometric characterizations for small-weight codewords for those Hermitian codes. From these geometric characterizations, we obtain explicit formulae which permits us to determine the number of minimum-weight codewords for all Hermitian codes with $d \leq q$ (see Section 7.3). In Section 7.4 we find the number of words having weight $d+1$ for some special cases and in Section 7.5 we compute all second-weight codewords for codes with distance $d = 3, 4$.

This work can be found in our article [MPS12].

In the last section, we use a geometrical approach reporting our results in [FM11].

7.1 Corner codes and edge codes

The first phase Hermitian codes can be either *edge codes* or *corner codes*.

Definition 7.1.1. *Let $2 \leq d \leq q$ and let $1 \leq j \leq d-1$.*
Let $L_0^d = \{1, x, \ldots, x^{d-2}\}, L_1^d = \{y, xy, \ldots, x^{d-3}y\}, \ldots, L_{d-2}^d = \{y^{d-2}\}$.
Let $l_1^d = x^{d-1}, \ldots, l_j^d = x^{d-j}y^{j-1}$.

- *If $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d$, then we say that $C(m,q)$ is a **corner code** and we denote it by H_d^0.*
- *If $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d \sqcup \{l_1^d, \ldots, l_j^d\}$, then we say that $C(m,q)$ is an **edge code** and we denote it by H_d^j.*

From previous results (see Chapter 4.2), that we report also in Table 5.1, we have the following theorem.

Theorem 7.1.2. *Let $2 \leq d \leq q$, $1 \leq j \leq d-1$. Then*

$$d(H_d^0) = d(H_d^j) = d, \quad \dim_{\mathbb{F}_{q^2}}(H_d^0) = n - \frac{d(d-1)}{2}, \ \dim_{\mathbb{F}_{q^2}}(H_d^j) = n - \frac{d(d-1)}{2} - j.$$

In other words all $ev_{\mathcal{P}}(x^r y^s)$, where $\mathcal{P}$ is the set of the $\mathbb{F}_{q^2}$-rational affine points of $\mathcal{H}$, are linearly independent (i.e. H has maximal rank). Moreover for any distance d there are exactly d Hermitian codes (one corner code and $d-1$ edge codes). We can represent the above codes as in the following picture, where we consider the five smallest non-trivial codes (for any $q \geq 3$).

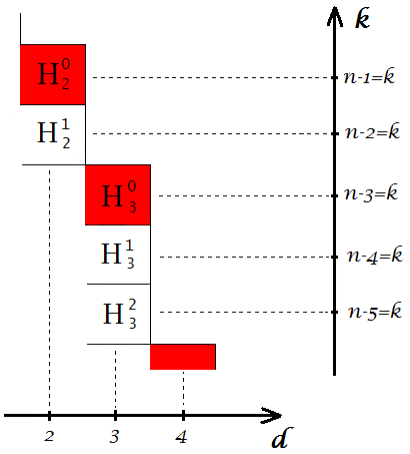
H_2^0 is a $[n, n-1, 2]$ code.
$\mathcal{B}_{m,q} = L_0^2 = \{1\}$, so the parity-check matrix of H_2^0 is $(1, \ldots, 1)$.

H_2^1 is a $[n, n-2, 2]$ code.
$\mathcal{B}_{m,q} = L_0^2 \sqcup l_1^2 = \{1, x\}$

H_3^0 is a $[n, n-3, 3]$ code.
$\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 = \{1, x, y\}$

H_3^1 is a $[n, n-4, 3]$ code.
$\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup l_1^3 = \{1, x, y, x^2\}$

H_3^2 is a $[n, n-5, 3]$ code.
$\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup \{l_1^3, l_2^3\} = \{1, x, y, x^2, xy\}$



7.2 First results for the first phase

Ideal J_w of Proposition 4.2.1 for $C(m,q)$ is

$$J_w = \Big\langle \begin{array}{l} \left\{ \sum_{i=1}^{w} z_i x_i^r y_i^s \right\}_{x^r y^s \in \mathcal{B}_{m,q}}, \left\{ x_i^{q+1} - y_i^q - y_i \right\}_{i=1,\ldots,w}, \\ \left\{ z_i^{q^2-1} - 1 \right\}_{i=1,\ldots,w}, \left\{ x_i^{q^2} - x_i \right\}_{i=1,\ldots,w}, \left\{ y_i^{q^2} - y_i \right\}_{i=1,\ldots,w}, \\ \left\{ \prod_{1 \leq i < j \leq w} ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) \right\} \Big\rangle. \end{array} \tag{7.1}$$

Let $w \geq v \geq 1$. Let $Q = (\overline{x}_1, \ldots, \overline{x}_w, \overline{y}_1, \ldots, \overline{y}_w, \overline{z}_1, \ldots, \overline{z}_w) \in \mathcal{V}(J_w)$. We say that Q is in **v-block position** if we can partition $\{1, \ldots, n\}$ in v blocks $I_1, \ldots, I_v$ such that

$$\overline{x}_i = \overline{x}_j \iff \exists\, 1 \leq h \leq v \text{ such that } i, j \in I_h.$$

W.l.o.g. we can assume $|I_1| \leq \cdots \leq |I_v|$ and $I_1 = \{1, \ldots, u\}$. It is simple to prove the following numerical lemma.

Lemma 7.2.1. *We always have $u + v \leq w + 1$. If $u \geq 2$ and $v \geq 2$, then $v \leq \lfloor \frac{w}{2} \rfloor$ and $u + v \leq \lfloor \frac{w}{2} \rfloor + 2$.*

We need the following technical lemma.

Lemma 7.2.2. *Let us consider the edge code H_d^j with $1 \leq j \leq d-1$ and $3 \leq d \leq w \leq 2d-3$. Let $Q = (\overline{x}_1, \ldots, \overline{x}_w, \overline{y}_1, \ldots, \overline{y}_w, \overline{z}_1, \ldots, \overline{z}_w)$ be a solution of J_w in v-block position, with $v \leq w$, then exactly one of the following cases holds:*

(a) $u = 1$, $v > d$ and $w \geq d+1$

or

(b) $v = 1$, that is, $\bar{x}_1 = \cdots = \bar{x}_w$.

If $d = 2$ and $w = 2$, then (a) holds for H_2^1.

Proof. We denote for all $1 \leq h \leq v$

$$X_h = \bar{x}_i \text{ if } i \in I_h, \quad Z_h = \sum_{i \in I_h} \bar{z}_i, \quad Y_{h,\delta} = \sum_{i \in I_h} \bar{y}_i^{\delta} \bar{z}_i \text{ with } 1 \leq \delta \leq u-1$$

(a) $u = 1$. We have to prove, by contradiction, that $v > d$.
Let $v \leq d$. Since $Q \in \mathcal{V}(J_w)$, then $L_0^w(Q) = l_1^w(Q) = 0$, that is

$$0 = \sum_{i=1}^{w} \bar{x}_i^r \bar{z}_i = \sum_{i \in I_h} X_h^r \bar{z}_i = \sum_{h=1}^{v} X_h^r Z_h \quad 0 \leq r \leq d-1. \tag{7.2}$$

We only need to consider only the first v equations of (7.2), because $v \leq d$, so

$$\sum_{h=1}^{v} X_h^r Z_h = 0 \quad 0 \leq r \leq v-1 \iff \begin{pmatrix} 1 & \ldots & 1 \\ X_1 & \ldots & X_v \\ \vdots & \ldots & \vdots \\ X_1^{v-1} & \ldots & X_v^{v-1} \end{pmatrix} \begin{pmatrix} Z_1 \\ \vdots \\ Z_v \end{pmatrix} = 0 \tag{7.3}$$

The above matrix is a Vandermonde matrix, so it has maximal rank v. Therefore, the solution of (7.3) is $(Z_1, \ldots, Z_v) = (0, \ldots, 0)$. Since $u = 1$, then $Z_1 = \overline{z}_1 = 0$, which contradicts $\overline{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. So if $v > d$ then $w \geq d+1$.

(b) $u \geq 2$. We suppose by contradiction that $v \geq 2$.
We consider Proposition 4.2.1. A subset of equations of condition (4.4) is the following system, where $0 \leq r \leq v$

$$\begin{cases} \sum_{i=1}^{w} \bar{x}_i^r \bar{z}_i = 0 \\ \sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i \bar{z}_i = 0 \\ \quad \vdots \\ \sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i^{u-1} \bar{z}_i = 0 \end{cases} \iff \begin{cases} \sum_{h=1}^{v} X_h^r Z_h = 0 \\ \sum_{h=1}^{v} X_h^r Y_{h,1} = 0 \\ \quad \vdots \\ \sum_{h=1}^{v} X_h^r Y_{h,u-1} = 0 \end{cases} \tag{7.4}$$

In fact system (7.4) is a subset of (4.4) if and only if $\deg(\bar{x}_i^v \bar{y}_i^{u-1}) \leq d-1$ for any $i = 1, \ldots, w$. That is, $v + (u-1) \leq d-1 \iff v + u \leq d$.
To verify it, since $v \geq 2$, it is sufficient to apply Lemma 7.2.1 and we obtain $u + v \leq \lfloor \frac{w}{2} \rfloor + 2 \leq \lfloor \frac{2d-3}{2} \rfloor + 2 = d$.
By system (7.4) we obtain u Vandermonde matrices (all having rank v). Therefore, the solutions of these systems are zero-solutions. So, in the particular case $h = 1$, we have $Z_1 = Y_{1,1} = \ldots = Y_{1,u-1} = 0$, that is

$$\begin{cases} \sum_{i=0}^{u} \bar{z}_i = 0 \\ \sum_{i=0}^{u} \bar{y}_i \bar{z}_i = 0 \\ \quad \vdots \\ \sum_{i=0}^{u} \bar{y}_i^{u-1} \bar{z}_i = 0 \end{cases} \iff \begin{pmatrix} 1 & \ldots & 1 \\ \bar{y}_1 & \ldots & \bar{y}_u \\ \vdots & \ldots & \vdots \\ \bar{y}_1^{u-1} & \ldots & \bar{y}_u^{u-1} \end{pmatrix} \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_u \end{pmatrix} = 0$$

Since the $\bar{y}_i$'s are all distinct (because the $\bar{x}_i$'s are all equal), we obtain a Vandermonde matrix, and so $\bar{z}_1 = \cdots = \bar{z}_u = 0$, but this is impossible because $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. Therefore $v = 1$.

The case H_2^1 is trivial. □

7.3 Minimum-weight codewords

Corollary 7.3.1. *Let us consider the edge code H_d^j with $1 \leq j \leq d-1$.*
If $Q = (\overline{x}_1, \ldots, \overline{x}_d, \overline{y}_1, \ldots, \overline{y}_d, \overline{z}_1, \ldots, \overline{z}_d) \in \mathcal{V}(J_d)$, then $\bar{x}_1 = \cdots = \bar{x}_d$. In other words, the points that correspond to a minimum-weight word lie in the intersection of the Hermitian curve $\mathcal{H}$ and a vertical line.
Whereas if $d \geq 4$ and $Q = (\overline{x}_1, \ldots, \overline{x}_{d+1}, \overline{y}_1, \ldots, \overline{y}_{d+1}, \overline{z}_1, \ldots, \overline{z}_{d+1}) \in \mathcal{V}(J_{d+1})$, then one of the following cases holds

(a) $\bar{x}_i \neq \bar{x}_j$ with $i \neq j$ for $1 \leq i, j \leq d+1$.

or

(b) $\bar{x}_1 = \cdots = \bar{x}_{d+1}$.

Proof. We are in the hypotheses of Lemma 7.2.2. So if $w = d$ then $u \neq 1$. So $v = 1$. Whereas, if $w = d+1$ then there are two possibilities. In case (a) of Lemma 7.2.2, all the $\bar{x}_i$'s are different, since $v = d+1$, or, case (b), $\bar{x}_1 = \cdots = \bar{x}_{d+1}$. □

Now we can prove the following theorem for edge codes.

Theorem 7.3.2. *The number of minimum weight words of an edge code H_d^j is*

$$A_d = q^2(q^2-1)\binom{q}{d}.$$

Proof. By Proposition 4.2.1 we know that J_d represents all words of minimum weight. The first set of ideal basis (7.1) has exactly $\frac{d(d-1)}{2}+j$ equations, where $1 \leq j \leq d-1$. So, if $j=1$, this set implies the following system:

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \\ \bar{x}_1^{d-1}\bar{z}_1 + \cdots + \bar{x}_d^{d-1}\bar{z}_d = 0 \end{cases} \tag{7.5}$$

Whereas, if $j > 1$ then we have to add the first $j-1$ of following equations:

$$\begin{cases} \bar{x}_1^{d-2}\bar{y}_1\bar{z}_1 + \cdots + \bar{x}_d^{d-2}\bar{y}_d\bar{z}_d = 0 \\ \quad \vdots \\ \bar{x}_1\bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{x}_d\bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{7.6}$$

But $\bar{x}_1 = \ldots = \bar{x}_d$, since we are in the hypotheses of Corollary 7.3.1. So the system becomes

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{7.7}$$

We have q^2 choices for the $\bar{x}_i$'s and, by Lemma 3.2.1, we have $\binom{q}{d}d!$ different $\bar{y}_i$'s, since for any choice of the $\bar{x}_i$'s there are exactly q possible values for the $\bar{y}_i$'s, but we need just d of them and any permutation of these will be again a solution. Now we have to compute the solutions for the $\bar{z}_i$'s.
We write the system (7.7) as a matrix, which is a Vandermonde matrix with rank $d-1$. This means that the solution space has linear dimension 1 because $1 = d-(d-1) =$ number of variables $-$ rank of matrix. So the solutions are $(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha)$ with $\alpha \in \mathbb{F}_{q^2}^*$, where a_j are fixed since they depend on $\bar{y}_i$. So the number of the z's is $|\mathbb{F}_{q^2}^*| = q^2-1$, then $A_d = \frac{1}{d!}\left(q^2(q^2-1)\binom{q}{d}d!\right)$. □

We consider now corner codes. We have the following geometric characterisation.

Proposition 7.3.3. *Let us consider the corner code H_d^0. Then the points $(\bar{x}_1, \bar{y}_1), \ldots, (\bar{x}_d, \bar{y}_d)$ corresponding to minimum-weight words lie on the same line.*

Proof. The minimum-weight words of a corner code have to verify the first condition set of J_w, which has $\frac{d(d-1)}{2}$ equations. That is,

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{7.8}$$

This system is the same as (7.5), but with a missing equation. This means that (7.8) has all solutions of system (7.5) and other solutions.
If we consider a subset of (7.8):

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad \vdots \\ \bar{x}_1^{d-2}\bar{z}_1 + \cdots + \bar{x}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{7.9}$$

we note that the $\bar{z}_i$'s are all non-zero if all $\bar{x}_i$'s are distinct (or all are equal). Therefore, we have only two possibilities for the $\bar{x}_i$'s: either are all different or they coincide. The same consideration is true for the $\bar{y}_i$'s, in fact when we consider (7.8) and we exchange x with y, we obtain again (7.8).
So we have two alternatives:

- The $\bar{x}_i$'s are all equal or the $\bar{y}_i$'s are all equal, so our proposition is true.
- The $\bar{x}_i$'s and the $\bar{y}_i$'s are all distinct. We will prove that they lie on a non-horizontal line that intersects the Hermitian curve.
  Let $y = \beta x + \lambda$ be a non-vertical line passing through two points in a minimum weight configuration. We can do an affine transformation of this type:

$$\begin{cases} x = x' \\ y = y' + ax', \quad a \in \mathbb{F}_{q^2} \end{cases}$$

  such that at least two of the y''s are equal and not all y's are coincident. Substituting the above transformation in (7.8) and applying some operations between

the equations, we obtain a system that is equivalent to (7.8). But this new system has all y''s equal (or all distinct), so the y''s have to be all equal. Hence we can conclude that the points lie on the same line.

□

We finally prove the following theorem:

Theorem 7.3.4. *The number of words having weight d of a corner code H_d^0 is*

$$A_d = q^2(q^2-1)\binom{q}{d-1}\frac{q^3-d+1}{d}.$$

Proof. Again, the points corresponding to minimum-weight words of a corner code have to verify (7.8). By above proposition, we know that these points lie in the intersections of any line and the Hermitian curve $\mathcal{H}$.
Let $Q = (\overline{x}_1, \ldots, \overline{x}_d, \overline{y}_1, \ldots, \overline{y}_d, \overline{z}_1, \ldots, \overline{z}_d) \in \mathcal{V}(J_d)$ such that $\overline{x}_1 = \ldots = \overline{x}_d$, that is, the points $(\bar{x}_i, \bar{y}_i)$ lie on a vertical line. We know that the number of such Q's is

$$q^2(q^2-1)\binom{q}{d}d!\,.$$

Now we have to compute the number of solutions $Q \in \mathcal{V}(J_d)$ such that $(\bar{x}_i, \bar{y}_i)$ lie on a non-vertical line.
By Lemma 3.2.2 we know that the number of the $\bar{y}_i$'s and $\bar{x}_i$'s is

$$(q^4-q^3)\binom{q+1}{d}d!,$$

since for any choice of the $\bar{y}_i$'s there are exactly $q+1$ possible values for the $\bar{x}_i$'s, but we need just d of these (and the system is invariant). As regards the number of the $\bar{z}_i$'s, we have to compute the number of solutions of system (7.8).
We apply an affine transformation to the system (7.8) to obtain a horizontal line, that is, to have all the $\bar{x}_i$'s different and all the $\bar{y}_i$'s equal, so we obtain a system equivalent to system (7.7). Therefore we have a Vandermonde matrix, hence the number of the $\bar{z}_i$'s is q^2-1. So

$$\begin{aligned} A_d = &\ \tfrac{1}{d!}\left(q^2(q^2-1)\tbinom{q}{d}d! + (q^4-q^3)(q^2-1)\tbinom{q+1}{d}d!\right) \\ = &\ q^2(q^2-1)\tbinom{q}{d-1}\tfrac{q^3-d+1}{d}. \end{aligned}$$

□

7.4 Second-weight codewords

In this section we study the case when the x_i's and the y_i's lie either on a vertical line or a non-vertical line.

Theorem 7.4.1. *The number of words of weight $d+1$ with $y_1 = \ldots = y_{d+1}$ of a corner code H_d^0 is:*

$$(q^2-q)(q^4-(d+1)q^2+d)\binom{q+1}{d+1}.$$

Whereas for an edge code H_d^j with $1 \leq j \leq d-1$ the numbers is:

$$(q^2-q)\binom{q+1}{d+1}.$$

Proof. We have q^2 choice for the $\bar{y}_i$'s and, by Corollary 3.2.3, we have $\binom{q+1}{d+1}(d+1)!$ different $\bar{x}_i$'s, since for any choice of the $\bar{y}_i$'s there are exactly $q+1$ possible values for the $\bar{x}_i$'s, but we need just $(d+1)$ of them and any permutation of these will be again a solution.
Now we have to compute the solutions for the $\bar{z}_i$'s, in the two distinct cases.

* **Case H_d^0.** By Proposition 4.2.1 we know that J_d represents all words of minimum weight. The first set of ideal basis (7.1) has exactly $\frac{d(d-1)}{2}$ equations, which is system (7.8) with more variables, that is, instead of $\bar{x}_d$, $\bar{y}_d$ and $\bar{z}_d$, we have, respectively, $\bar{x}_{d+1}$, $\bar{y}_{d+1}$ and $\bar{z}_{d+1}$. Since $\bar{y}_1 = \ldots = \bar{y}_{d+1}$, the said variation of system (7.8) is

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_{d+1} = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_{d+1}\bar{z}_{d+1} = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_{d+1}^2\bar{z}_{d+1} = 0 \\ \quad \vdots \\ \bar{x}_1^{d-2}\bar{z}_1 + \cdots + \bar{x}_{d+1}^{d-2}\bar{z}_{d+1} = 0 \end{cases} \tag{7.10}$$

We can note that, if we write the system (7.10) as a matrix adding these two equations $x_1^{d-1}+\ldots+x_{d+1}^{d-1} = 0$ and $x_1^d+\ldots+x_{d+1}^d = 0$ we obtain a Vandermonde matrix. So all rows of (7.10) are linearly independent. This means that the solution space has linear dimension 2 because $2 = (d+1)-(d-1)$. So the number of the z's is $q^4 - |\{z_i = \ 0 \text{ for at least an } i\}|$, since we have q^2 for each z_{d+1} and z_d. We want to compute the number of $z_i = 0$ for at least one i.
Since the matrix H has maximum rank, we can apply the Gauss elimination to

the system (7.10)

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_{d+1} = 0 \\ h_{2,2}\bar{z}_2 + \ldots + h_{2,d}\bar{z}_d + h_{2,d+1} + \bar{z}_{d+1} = 0 \\ \vdots \\ h_{d-1,d-2}\bar{z}_{d-2} + h_{d-1,d-1}\bar{z}_{d-1} + h_{d-1,d}\bar{z}_d + h_{d-1,d+1}\bar{z}_{d+1} = 0 \\ h_{d-1,d-1}\bar{z}_{d-1} + h_{d-1,d}\bar{z}_d + h_{d-1,d+1}\bar{z}_{d+1} = 0 \end{cases} \tag{7.11}$$

If we solve the system (7.11) we obtain

$$h_{d-1,d-1}\bar{z}_{d-1} + h_{d-1,d}\bar{z}_d + h_{d-1,d+1}\bar{z}_{d+1} = 0 \tag{7.12}$$

First of all we consider the case $\bar{z}_{d-1} = 0$, that is

$$h_{d-1,d}\bar{z}_d + h_{d-1,d+1}\bar{z}_{d+1} = 0 \iff \bar{z}_d = -\frac{h_{d-1,d+1}}{h_{d-1,d}}\bar{z}_{d+1} \tag{7.13}$$

The equation (7.13) in the variable $\bar{z}_{d+1} \in \mathbb{F}_{q^2}$ has exactly q^2 solutions. In particular, we have the pair $(\bar{z}_d, \bar{z}_{d+1}) = (0,0)$ and other $q^2 - 1$ ways to choose the variable $\bar{z}_{d+1}$.
We have similar conditions when $\bar{z}_d = 0$ and $\bar{z}_{d+1} = 0$. As before we have the pairs $(\bar{z}_{d-1}, \bar{z}_{d+1}) = (0,0)$ and $(\bar{z}_{d-1}, \bar{z}_d) = (0,0)$ and other $q^2 - 1$ ways to choose $\bar{z}_{d-1}$ and $q^2 - 1$ ways to choose $\bar{z}_d$.
So the equation (7.12) has exactly $3(q^2-1) + |\{(\bar{z}_{d-1}, \bar{z}_d, \bar{z}_{d+1}) = (0,0,0)\}| = 3q^2 - 2$ solutions.
Now we consider the second last line of the system (7.11): $h_{d-1,d-2}\bar{z}_{d-2} + h_{d-1,d-1}\bar{z}_{d-1} + h_{d-1,d}\bar{z}_d + h_{d-1,d+1}\bar{z}_{d+1} = 0$, that is,

$$\bar{z}_{d-2} = -(k_{d-1}\bar{z}_{d-1} + k_d\bar{z}_d + k_{d+1}\bar{z}_{d+1}) \tag{7.14}$$

First of all we have to study the case $\bar{z}_{d-2} = 0$. We just studied the case in which all variables $\bar{z}_{d-1} = \bar{z}_d = \bar{z}_{d+1} = 0$, so we have to study the case when all variables are different from zero, that is, $\frac{k_{d-1}}{k_{d+1}}\bar{z}_{d-1} + \frac{k_d}{k_{d+1}}\bar{z}_d = -\bar{z}_{d+1} = k \in \mathbb{F}_{q^2}^*$.
So the equation (7.14) has exactly (q^2-1) solutions.
We repeat the argument for each of system's equations (7.11), there are $(d-2)$ of them, if we do not count the last equation. Therefore

$$\#(\bar{z}_i = 0 \text{ for at least one } i) = 3q^2 - 2 + (d-2)(q^2-1) = (d+1)q - d$$

So the system (7.11) has exactly $q^4 - (d+1)q + d$ solutions. Then the number of words of weight $d+1$ with $y_1 = \ldots = y_{d+1}$ of H_d^0 is:

$$(q^2-q)(q^4 - (d+1)q^2 + d)\binom{q+1}{d+1}.$$

∗ **Case** H_d^j. In this case the first set of ideal basis (7.1) contains exactly $\frac{d(d-1)}{2}+j$ equations, where $1 \leq j \leq d-1$. So, if $j=1$, this set implies the system (7.5) with more variables, that is, instead of $\bar{x}_d$, $\bar{y}_d$ and $\bar{z}_d$, we have, respectively, $\bar{x}_{d+1}$, $\bar{y}_{d+1}$ and $\bar{z}_{d+1}$. Whereas, if $j>1$ then we have to add the first $j-1$ of equations (7.6) with more variables.
Since $\bar{y}_1 = \ldots = \bar{y}_{d+1}$, the system becomes

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_{d+1} = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_{d+1}\bar{z}_{d+1} = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_{d+1}^2\bar{z}_{d+1} = 0 \\ \quad \vdots \\ \bar{x}_1^{d-1}\bar{z}_1 + \cdots + \bar{x}_{d+1}^{d-1}\bar{z}_{d+1} = 0 \end{cases} \tag{7.15}$$

This means that the solution space has linear dimension $d-(d-1)=1$. So the number of the z's is $|\mathbb{F}_{q^2}^*| = q^2-1$, then the number of words of weight $d+1$ with $y_1 = \ldots = y_{d+1}$ of H_d^j is:

$$(q^2-1)(q^2-q)\binom{q+1}{d+1}.$$

□

Theorem 7.4.2. *The number of words of weight $d+1$ with $x_1 = \ldots = x_{d+1}$ of a corner code H_d^0 and of an edge code H_d^j is:*

$$q^2(q^4-(d+1)q^2+d)\binom{q}{d+1}.$$

Proof. By Proposition 4.2.1 we know that J_d represents all words of minimum weight. For an edge code the first set of ideal basis (7.1) implies, if $j=1$ the system (7.5) with more variables[1] and if $j>1$ we have to add the first $j-1$ of equations (7.6) with more variables. Whereas, for a corner code, the first set of ideal basis (7.1) implies the system (7.8) with more variables. But $\bar{x}_1 = \ldots = \bar{x}_{d+1}$, so the systems becomes

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_{d+1} = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_{d+1}\bar{z}_{d+1} = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_{d+1}^{d-2}\bar{z}_{d+1} = 0 \end{cases} \tag{7.16}$$

[1] instead of $\bar{x}_d$, $\bar{y}_d$ and $\bar{z}_d$, we have, respectively, $\bar{x}_{d+1}$, $\bar{y}_{d+1}$ and $\bar{z}_{d+1}$. This is true every time that we write with more variables

We have q^2 choice for the $\bar{x}_i$'s and, by Lemma 3.2.1, we have $\binom{q}{d+1}(d+1)!$ different $\bar{y}_i$'s, since for any choice of the $\bar{x}_i$'s there are exactly q possible values for the $\bar{y}_i$'s, but we need just $d+1$ of them and any permutation of these will be again a solution. And we have $(q^4-(d+1)q^2+d)$ possible $\bar{z}_i$'s which is exactly the situation met in Theorem 7.4.1.

□

Theorem 7.4.3. *The number of words of weight $d+1$ of a corner code H_d^0 with (x_i, y_i) lying on a non-vertical line is:*

$$(q^4-q^3)(q^4-(d+1)q^2+d)\binom{q+1}{d+1}.$$

Theorem 7.4.4. *The number of words of weight $d+1$ of an edge code H_d^j with (x_i, y_i) lying on a non-vertical line is:*

$$(q^4-q^3)(q^2-1)\binom{q+1}{d+1}.$$

The proofs are similar to those of the statements as in Section 7.2 and the previous theorems and so are omitted.
In other cases, we have to consider the intersection of the curve with higher degree curves and the formulae get more complicated. For example the cubic found in [Cou11, BR12a].

Now we are going to study some special cases of Hermitian codes, that is, we count the number of words having weight $d+1$ for any Hermitian code having distance $d=3$ or $d=4$. In the following section we are going to prove these theorems:

Theorem 7.4.5. *The number of words of weight 4 of a corner code H_3^0 is:*

$$A_4 = \frac{1}{4}\left(\binom{q^3}{3}(q+1) - q^2\binom{q+1}{3}(3q^3+2q^2-8)\right)(q-1)(q^3-3).$$

The number of words of weight 4 of an edge code H_3^1 is:

$$A_4 = q^2\binom{q}{4}(q^4-4q^2+3) + \frac{q^4(q^2-1)^2(q-1)^2}{8} + (q^2-1)\sum_{k=4}^{2q} N_k\binom{k}{4}.$$

Where N_k is the number of parabolas and non-vertical lines that intersect $\mathcal{H}$ in exactly k points.
The number of words of weight 4 of an edge code H_3^2 is:

$$A_4 = q^2(q-1)\binom{q+1}{4}(2q^3-3q^2-4q+9).$$

Theorem 7.4.6. *The number of words of weight* 5 *of a corner code* H_4^0 *is:*

$$A_5 = \frac{1}{5}q^2\binom{q}{4}(q^3-4)(q^2-1)(q^2-4).$$

The number of words of weight 5 *of all edge codes* H_4^j *for* $1 \leq j \leq 3$ *is:*

$$A_5 = q^2(q-1)\binom{q+1}{5}(2q^3-4q^2-5q+16).$$

The formula for A_4 of H_3^1 in Theorem 7.4.5 contains some implicit values N_k's. To derive explicit values it is enough to consider Theorem 6.0.1.

7.5 The complete investigation for $d = 3, 4$.

In this section we will study separately the corner and edge codes of distance 3 and 4, that is, H_3^0, H_3^1, H_3^2, H_4^0, $\{\mathrm{H}_4^j\}_{1\leq j\leq 3}$.

Study of H_3^0.
Now we count the number of words with weight $w = 4$. In this case, the first condition set of J_w becomes:

$$\begin{cases} z_1 + z_2 + z_3 + z_4 = 0 \\ x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 = 0 \\ y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4 = 0 \end{cases}$$

We notice that this is a linear system in z_i. We first choose 4 points $P_i = (x_i, y_i)$ on $\mathcal{H}$ and then we compute the number of solutions in z_i's. The coefficient matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{pmatrix}$$

This matrix cannot have rank 1. If the rank is 2, this means that all P_i's lie on a same line. The vector space of solutions has dimension 2, so that we have $q^4 - 4(q^2-1) - 1$ solutions in z_i's (we have to exclude the zero solution and solutions with one $z_i = 0$).

Otherwise, the rank is 3. In this case, we have 3 points on a same line, say P_1, P_2, P_3, if and only if we have a square submatrix of order 3 whose determinant is 0, but this implies that $z_4 = 0$, which is not admissible. If we choose 4 points such that no 3 of them lie on a same line, all z_i's will be non-zero and we get a codeword. The vector space of solutions has dimension 1, so that we have $q^2 - 1$ solutions in z_i's (we have to exclude the zero solution).

If the rank is 2, the total number of solutions (in x_i, y_i, z_i) is

$$\left(q^2\binom{q}{4} + (q^4 - q^3)\binom{q+1}{4}\right)(q^4 - 4q^2 + 3).$$

If the rank is 3, the total number of solutions (in x_i, y_i, z_i) is

$$\left(\binom{q^3}{4} - q^2\binom{q}{3}(q^3 - q) - (q^4 - q^3)\binom{q+1}{3}(q^3 - q - 1) + \right.$$

$$\left. -q^2\binom{q}{4} - (q^4 - q^3)\binom{q+1}{4}\right)(q^2 - 1).$$

Putting together, we get the total number of codewords of weight 4 of H_3^0:

$$A_4 = \left(\binom{q^3}{4} - q^2\binom{q}{3}(q^3 - q) - (q^4 - q^3)\binom{q+1}{3}(q^3 - q - 1)\right)(q^2 - 1) +$$

$$+ \left(q^2\binom{q}{4} + (q^4 - q^3)\binom{q+1}{4}\right)(q^4 - 5q^2 + 4).$$

Doing the computations we obtain the first part of Theorem 7.4.5.

Study of H_3^1.
We count the number of words with weight $w = 4$. In this case, the first condition set of J_w becomes:

$$\begin{cases} z_1 + z_2 + z_3 + z_4 = 0 \\ x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 = 0 \\ y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4 = 0 \\ x_1^2z_1 + x_2^2z_2 + x_3^2z_3 + x_4^2z_4 = 0 \end{cases}$$

As above, we first choose 4 points $P_i = (x_i, y_i)$ on $\mathcal{H}$ and then we compute the number of solutions in z_i's. The coefficient matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \end{pmatrix} \tag{7.17}$$

Now we study the rank of the matrix according to "v-blocks".

If all x_i's are equal, we have 4 points on a vertical line; the rank is 2 (see below) and the number of codewords is (see case H_3^0)

$$q^2\binom{q}{4}(q^4 - 4q^2 + 3).$$

If only three x_i's are equal, we have 3 points on a vertical line and another one outside, but this configuration is impossible for H_3^0 (that is, we do not have codewords associated to it), and it is also impossible for H_3^1, since $\mathrm{H}_3^1 \subset \mathrm{H}_3^0$.

If we have two pairs of equal x_i's (for instance, $x_1 = x_2 \neq x_3 = x_4$), we can have codewords. In this case, we deduce

$$z_1 + z_2 = 0, z_3 + z_4 = 0,$$

$$z_1(y_1 - y_2) + z_3(y_3 - y_4) = 0,$$

so that we have $\binom{q^2}{2}$ ways to choose $\{x_1, x_3\}$, $\binom{q}{2}$ ways to choose $\{y_1, y_2\}$, $\binom{q}{2}$ ways to choose $\{y_3, y_4\}$, $q^2 - 1$ ways to choose z_1, this determines all z_i. The number of codewords in this case is

$$\frac{q^4(q^2-1)^2(q-1)^2}{8}.$$

If only two x_i's are equal, say $x_1 = x_2$, we can show that we have $z_1 + z_2 = 0$, $z_3 = 0, z_4 = 0$, which is not admissible.

If we have all x_i's distinct, the submatrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \end{pmatrix}$$

has rank 3, but if the whole matrix (7.17) has rank 4 we can only have the zero solution, which is not admissible. Thus, (7.17) must have rank 3, that is, the y_i's row must be linearly dependent on the other rows. This means that

$$\exists\, a, b, c \in \mathbb{F}_{q^2} \text{ such that } y_i = ax_i^2 + bx_i + c \;\forall\, i = 1, \ldots, 4.$$

That is, all P_i's lie on the same parabola (or on the same non-vertical line, when $a = 0$). In this case, the number of codewords is

$$(q^2 - 1) \sum_{k=4}^{2q} N_k \binom{k}{4},$$

where N_k is the number of parabolas and non-vertical lines that intersect $\mathcal{H}$ in exactly k points.

Putting all together we get A_4, that is, the second part of Theorem 7.4.5.

Study of H_3^2.

We count the number of words with weight $w = 4$. In this case, the first condition set of J_w becomes:

$$\begin{cases} z_1 + z_2 + z_3 + z_4 = 0 \\ x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 = 0 \\ y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4 = 0 \\ x_1^2z_1 + x_2^2z_2 + x_3^2z_3 + x_4^2z_4 = 0 \\ x_1y_1z_1 + x_2y_2z_2 + x_3y_3z_3 + x_4y_4z_4 = 0 \end{cases}$$

As above, we first choose 4 points $P_i = (x_i, y_i)$ on $\mathcal{H}$ and then we compute the number of solutions in z_i's. The coefficient matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ x_1y_1 & x_2y_2 & x_3y_3 & x_4y_4 \end{pmatrix} \tag{7.18}$$

Now we study the rank of the matrix according to "v-blocks".

If all x_i's are equal, we have 4 points on a vertical line; the rank is 2 (see below) and the number of codewords is (see case H_3^1)

$$q^2\binom{q}{4}(q^4 - 4q^2 + 3).$$

If only three x_i's are equal, we have 3 points on a vertical line and another one outside, but this configuration is impossible (as above).

If we have two pairs of equal x_i's (for instance, $x_1 = x_2 \neq x_3 = x_4$), we can deduce

$$z_1 + z_2 = 0, z_3 + z_4 = 0,$$

and then

$$\begin{cases} z_1(y_1 - y_2) + z_3(y_3 - y_4) & = & 0 \\ x_1z_1(y_1 - y_2) + x_3z_3(y_3 - y_4) & = & 0 \end{cases}$$

but this system in the unknowns $y_1 - y_2, y_3 - y_4$ has determinant $z_1z_3(x_3 - x_1) \neq 0$, so that $y_1 = y_2$, which is impossible.

If only two x_i's are equal, say $x_1 = x_2$, we can show that we have $z_1 + z_2 = 0$, $z_3 = 0, z_4 = 0$, which is not admissible.

If we have all x_i's distinct, the submatrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \end{pmatrix}$$

has rank 3, but if the whole matrix (7.18) has rank 4 we can only have the zero solution, which is not admissible. Thus, (7.18) must have rank 3, that is, the y_i's and x_iy_i's rows must be linearly dependent on the other rows. This means that $y = ax^2 + bx + c$ and $xy = dx^2 + ex + f$, then $ax^3 + (b-d)x^2 + (c-e)x - f = 0$. But this equation can have at most 3 distinct solutions, and we need 4. Thus we must have $a = 0, b = d, c = e, f = 0$, that is, $y = bx + c$: all P_i's lie on a same non-vertical line, and the number of codewords is

$$(q^4 - q^3)\binom{q+1}{4}(q^2 - 1).$$

Putting all together we get A_4, that is, the last part of Theorem 7.4.5.

Study of H_4^0.
We count the number of words with weight $w = 5$. We have a linear system in z_i with a (6×5) matrix. If its rank is 5, we can only have the zero solution, which is not admissible. Thus, its rank must be at most 4; this means that we have at least 2 relationships of linear dependency, say

$$\begin{cases} xy = a + bx + cy + dx^2 \\ y^2 = e + fx + gy + hx^2. \end{cases}$$

We need to find 5 points on the intersection of 2 different conics, but this means that the 2 conics must be degenerate, they must have a common line, and all 5 points belong to this line. We could distinguish between vertical lines and non-vertical lines, but in both cases the rank of the matrix is exactly 3. So, the number of codewords is

$$A_5 = \left((q^4 - q^3)\binom{q+1}{5} + q^2\binom{q}{5}\right)(q^4 - 5q^2 + 4).$$

Doing the computations we obtain the first part of Theorem 7.4.6.

Study of H_4^1, H_4^2, H_4^3.
To count the number of words with weight $w = 5$, we remember that

$$\mathrm{H}_4^0 \supseteq \mathrm{H}_4^1 \supseteq \mathrm{H}_4^2 \supseteq \mathrm{H}_4^3 \supseteq \mathrm{H}_5^0$$

and the first and the last code have all words with weight 5 corresponding to 5 points on a line. We notice that for a vertical line the rank of the matrix is 3, while for a non-vertical line the rank of the matrix is 4. So, the number of codewords is

$$A_5 = q^2\binom{q}{5}(q^4 - 5q^2 + 4) + (q^4 - q^3)\binom{q+1}{5}(q^2 - 1).$$

Doing the computations we obtain the last part of Theorem 7.4.6.

7.6 On the geometry of small weight codewords of AG codes

In the previous sections, the number of small weight codewords for some families of Hermitian codes was determined. Besides explicit computation, the main ingredient in Section 7.3 is a geometric characterization of the points in the support of a minimum weight codeword, which turn out to be collinear (see Corollary 7.3.1 and Proposition 7.3.3).

In this section, we report our results in [FM11].

Here we show that such a property is not peculiar to Hermitian codes, but it holds in full generality for dual algebraic geometric codes on any smooth complete intersection projective variety of arbitrary dimension. We start recalling some geometrical base notions in regard to AG codes. To do these we consider Chapter Two of [HvLP98], the first two chapters of [Sti93] and Chapter Thirteen of [HKT08].

In the following section, we denote by $\mathbb{F}$ the algebraic closure of $\mathbb{F}_q$.

Let $\mathbb{A}^r$ be the r-dimensional affine space with coordinates $x_1 \ldots, x_r$ and let $\mathbb{P}^r$ be the r-dimensional projective space with homogenous coordinates $x_0, x_1 \ldots, x_r$. In $\mathbb{A}^r$, the algebraic set of zeros of ideal I of $\mathbb{F}[x_1, \ldots, x_r]$ are the variety $V(I)$.

Let I be a prime ideal in the ring $\mathbb{F}[x_1, \ldots, x_r]$. The set $\mathcal{X}$ of zeros of I is called an *affine variety*. We denote with $\mathbb{F}[\mathcal{X}]$ the coordinate ring $\mathbb{F}[x_1, \ldots, x_m]/I$ of the variety $\mathcal{X}$ and the quotient field of $\mathbb{F}[\mathcal{X}]$ is denoted by $\mathbb{F}(\mathcal{X})$, that is a *rational function field* on $\mathcal{X}$

$$\mathbb{F}(\mathcal{X}) = \Big\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in \mathbb{F}[\mathcal{X}], g \neq 0 + I \Big\}.$$

Let $\mathcal{X}$ be an algebraic curve defined over $\mathbb{F}_q$, that is, an affine variety of dimension one, where the dimension of $\mathcal{X}$ is the transcendence degree of $\mathbb{F}(\mathcal{X})$ over $\mathbb{F}$.

In projective space $\mathbb{P}^r$, the situation is similar but we have to use the homogenous coordinates. So a projective variety $\mathcal{X}$ is the zero set in $\mathbb{P}^r$ of a homogeneous prime ideal $I \in \mathbb{F}[X_0, X_1, \ldots, X_r]$. Consider the subring $R(\mathcal{X})$ of $\mathbb{F}(X_0, X_1, \ldots, X_r)$ consisting of the fractions f/g, where f and g are homogeneous polynomials of the same degree and $g \notin I$. Then $R(\mathcal{X})$ has a unique maximal ideal $M(\mathcal{X})$ consisting of all those f/g with $f \in I$. The function field $F(\mathcal{X})$ is by definition $R(X)/M(X)$.

Let $\mathcal{X}$ be an affine variety and let P be a point on $\mathcal{X}$. Then a rational function φ is called *regular* in the point P if we can find polynomials f and g such that $g(P) \neq 0$

and φ is the coset of f/g.
If $\mathcal{X}$ is a projective variety, we have the same definition. In this case, f and g are two homogeneous polynomials of the same degree.

The *local ring* $\mathcal{O}_P$ of the point P on the variety $\mathcal{X}$ is the set of rational functions that are regular in P. Let $\mathcal{M}_P$ be the set of functions in $\mathcal{O}_P$ that are zero at P.
We consider t the generating element of $\mathcal{M}_P$. It is possible to write every element z of $\mathcal{O}_P$ as $z = ut^m$, where u is a unit and m is a natural number. If $m > 0$, then P is a *zero* of multiplicity m of z, otherwise P is a *pole*. We denote this by $v_P(z) = m$ and the function t is called *local parameter.*

Finally we recall a smooth curve and its related notations.

Consider a curve $\mathcal{X}$ in $\mathbb{A}^2$, defined by the equation $f = 0$. Let P be a point on this curve. If at least one of the partial derivatives f_X or f_Y is not zero in P, then P is called a *simple* or *nonsingular* point of the curve and a curve is called *nonsingular*, *regular* or *smooth* if all the points are nonsingular.

Let $\mathcal{X}$ be an absolutely irreducible (i.e. irreducible in the algebraic closure) nonsingular projective curve over $\mathbb{F}_q$. We recall that a *divisor* on $\mathcal{X}$ is a formal sum

$$D = \sum_{P \in \mathcal{X}} n_P P \text{ with } n_P \in \mathbb{Z} \text{ and almost all } n_P = 0.$$

The *support* of a divisor is the set of points with nonzero coefficient, that is

$$supp(D) = \{P \in \mathcal{X} \mid n_P \neq 0\}.$$

A divisor D is called *effective* if all coefficients n_P are non-negative. The *degree* $\deg(D)$ of the divisor D is $\sum n_P$.

If f is a rational function on $\mathcal{X}$, not identically 0, we define the divisors of f as

$$(f) = \sum_{P \in \mathcal{X}} v_P(f)P = (f)_0 - (f)_\infty,$$

where, if we denote with Z and N, respectively, the set of zeros and the set of poles of f, we have the *zero* and the *pole divisor*

$$(f)_0 = \sum_{P \in Z} v_P(f)P \text{ and } (f)_\infty = \sum_{P \in N} -|v_P(f)|P.$$

Let $P \in \mathbb{P}^r$. An integer $n > 0$ is called a *pole number* of P if there is an element $f \in \mathbb{F}$ with $(f)_\infty = nP$. Otherwise n is called a *gap* number of P.

Now, we are already to define a Riemann-Roch space.

Definition 7.6.1. *Let D be a divisor on a curve $\mathcal{X}$. The* ***Riemann-Roch space*** *associated to D is a vector space $\mathcal{L}(D)$ over $\mathbb{F}$ definited as*

$$\mathcal{L}(D) = \{f \in \mathbb{F}(\mathcal{X}) \mid (f) + D \geq 0\} \cup \{0\}.$$

The dimension of $\mathcal{L}(D)$ over $\mathbb{F}$ is denoted by $l(D)$, which is called also the dimension of the divisor D.

The genus g of $\mathbb{F}(\mathcal{X})$ is defined by

$$g = \max\{\deg D - l(D) + 1 \mid D \in \mathrm{Div}(\mathcal{X})\}.$$

Theorem 7.6.2. *If D is a divisor of $\mathbb{F}(\mathcal{X})$ of degree $\deg D \geq 2g - 1$ then*

$$l(D) = \deg D + 1 - g.$$

Proof. See proof of Theorem 1.5.17. of [Sti93]. □

Now we have all the geometrical notions needed to define an AG code.
Assume that $P_1, \ldots, P_n$ are rational points on $\mathcal{X}$ and D is a divisor such that $D = P_1 + \ldots + P_n$. Let G be some other divisor such that $supp(D) \cap supp(G) \neq \emptyset$ and we denote with m the degree of G, that is, $m = \deg(G)$. Then we can define

Definition 7.6.3. *The algebraic-geometric code (or AG code) $C(D, G)$ associated with the divisors D and G is defined as*

$$C(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subset \mathbb{F}_q^n.$$

In other words an algebraic-geometric code is the image of the evaluation map, i.e. $\mathrm{Im}(ev_D) = C(D, G)$, where the evaluation map is $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ given by

$$ev_D(f) = (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n.$$

Theorem 7.6.4. *Let $C(D, G)$ be a $[n, k, d]$ algebraic-geometric code. Then*

- $k = l(G) - l(G - D)$.
- $d \geq n - m$.

Furthermore if $2g - 2 < m < n$ then $k = m - g + 1$.

Corollary 7.6.5 (Goppa's Bound)**.** *Let $C(D, G)$ be a $[n, k, d]$ algebraic-geometric code and let $2g - 2 < m < n$. Then*

$$d \geq n - k + 1 - g.$$

Let $C(D,G)^{\perp}$ be a dual of $C(D,G)$. Then it is also an algebraic-geometric code.

Corollary 7.6.6. *Let $C^{\perp}(D,G)$ be a $[n,k_{\perp},d_{\perp}]$ algebraic-geometric code. Then*

- $k_{\perp} = n - m + g - 1$.
- $d_{\perp} \geq m - 2g + 2$.
- $n - k_{\perp} + 1 - g \leq d_{\perp} \leq n - k_{\perp} + 1$.

Note that in Chapter 5 we saw this corollary for the special case of Hermitian codes. In particular we have the distance in Lemma 5.2.5 and the dimension is a consequence of Theorem 5.2.3.

We are ready to report some notation and results (without demonstration) from the paper *The dual minimum distance of arbitrary-dimensional algebraic-geometric codes* of A. Couvreur [Cou11].

We denote with $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u))$ the space of homogeneous forms of degree u in $r+1$ variables.

Definition 7.6.7. *Let $P_1, \ldots, P_s$ be rational points of $\mathbb{P}^r$. They are in* ***u-general position*** *if the evaluation maps $ev_{P_1}, \ldots, ev_{P_s}$ are linearly independent in the dual of $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u))$. If they are not in u-general position, we can say that they are* ***u-linked****. Moreover they are said to be* ***minimally u-linked*** *if they are u-linked and if each proper subset of $\{P_1, \ldots, P_s\}$ is in u-general position.*

Lemma 7.6.8. *Let $P_1, \ldots, P_s$ be a minimally u-linked configuration of points in $\mathbb{P}^r$. Let d and l be two integers satisfying respectively $1 < d < u$ and $1 < l < s$. Let H be a hypersurface of degree d containing exactly l of the P_i's. Then, the $s - l$ remaining points are $(u-d)$-linked.*

Proposition 7.6.9. *A set of $s \leq u + 1$ distinct points $P_1, \ldots, P_s \in \mathbb{P}^r$ is u-general.*

Proposition 7.6.10. *Let $P_1, \ldots, P_{u+2}$ be a family of u-linked points. Then they are collinear.*

Proposition 7.6.11. *A configuration of $s \leq 2u + 1$ distinct points $P_1, \ldots, P_s \in \mathbb{P}^r$ such that no $m + 2$ of them are collinear is u-general.*

Proposition 7.6.12. *For all $u \geq 1$, any minimally u-linked configuration of $n \leq 3u$ points is a set of coplanar points.*

Proposition 7.6.13. *A configuration of $s \leq 3u-1$ distinct points such that no $m+2$ of them are collinear and no $2m+2$ of them lie on a plane conic, are u-general.*

Proposition 7.6.14. *An u-linked configuration of $3u$ points such that no $u+2$ of them are collinear and no $2u+2$ of them lie on a plane conic is a family of coplanar points lying at the intersection of a cubic and a curve of degree u having no common component.*

Now we can start with our results.

Theorem 7.6.15. *Let $\mathcal{X} \subset \mathbb{P}^r$, $r \geq 2$, be a smooth connected complete intersection defined over $\mathbb{F}_q$. Let D and G be two divisors on $\mathcal{X}$ as previous and let G be such that $\mathcal{L}(G) \supseteq H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u))$. Let d be the minimum distance of the code $C(D,G)^\perp$ and let $\{P_{i_1}, \ldots, P_{i_d}\}$ be the points in the support of a minimum weight codeword.*

(i) If $d \leq u+2$, then $d = u+2$ and all the $u+2$ points P_{i_j} are collinear in $\mathbb{P}^r$.

(ii) If $d \leq 2u+2$ and no $u+2$ of the P_{i_j}'s are collinear, then $d = 2u+2$ and all the $2u+2$ points P_{i_j} lie on a plane conic.

(iii) If $d \leq 3u$, no $u+2$ of the P_{i_j}'s are collinear and no $2u+2$ of them lie on a plane conic, then $d = 3u$ and all the $3u$ points P_{i_j} lie at the intersection of two coplanar plane curves of respective degrees 3 and u.

Proof. Let $c \in C(D,G)^\perp$ be a minimum weight codeword having support $\{P_{i_1}, \ldots, P_{i_s}\}$ with $s = d$. By the definition of a dual code, we have

$$\sum_{j=1}^{s} c_j f(P_{i_j}) = 0 \text{ for every } f \in \mathcal{L}(G) \supseteq H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u)).$$

In particular, we have

$$\sum_{j=1}^{s} c_j ev_{P_{i_j}}(f) = 0 \text{ for every } f \in H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u)).$$

Hence $ev_{P_{i_j}}$ turn out to be linearly dependent in $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(u))^\perp$ and by Definition 7.6.7, $P_{i_1}, \ldots, P_{i_s}$ are u-linked. Now we have, in case

(i) by Proposition 7.6.9, $d = s = u+2$ and so we can apply Proposition 7.6.10.

(ii) by Proposition 7.6.11, $d = s = 2u+2$ and so we apply Proposition 7.6.12.

(iii) by Proposition 7.6.13, $d = s = 3u$ and by Proposition 7.6.14 we prove this case.

□

We focus on the Hermitian codes (Chapter Eight of [Sti93] and Chapter Five of [HvLP98]).

As we know, a special case of algebraic-geometric code is a Hermitian codes. We consider the Hermitian curve $\mathcal{H}$ of affine equation $x^{q+1} = y^q + y$ defined over $\mathbb{F}_{q^2}$. We recall that the genus of $\mathcal{H}$ is $g = q(q-1)/2$ and $\mathcal{H}$ has $q^3 + 1$ points of degree one, namely a pole Q_∞ and q^3 distinct points $P_{\alpha,\beta} = (\alpha, \beta)$ such that $\alpha^{q+1} = \beta^q + \beta$.

Definition 7.6.16. *For $m \in \mathbb{Z}$ we define the code $C(m,q) = C(D, mQ_\infty)$ where*

$$D = \sum_{\alpha^{q+1}=\beta^q+\beta} P_{\alpha,\beta}$$

is the sum of all places of degree one (except Q_∞, that is a point at infinity) of the Hermitian function field $\mathbb{F}(\mathcal{H})$. The codes $C(m,q)$ are called ***Hermitian codes****.*

We can note that if $m < 0$, then $\mathcal{L}(mQ_\infty) = 0$ and so $C(m,q) = 0$.
For $m > q^3 + (2g-2) = q^3 + q^2 - q - 2$, by Theorem 7.6.4 and Theorem 7.6.2 we have that

$$\dim C(m,q) = l(mQ_\infty) + l(mQ_\infty - D) = (m + 1 - g) - (m - q^3 + 1 - g) = q^3,$$

therefore $C(m,q) = \mathbb{F}_{q^2}^n$.
So we study the Hermitian codes with $0 \leq m \leq q^3 + (2g-2) = q^3 + q^2 - q - 2$.

We can note that if $m < 0$, then $\mathcal{L}(mQ_\infty) = 0$ and so $C(m,q) = 0$.
For $m > q^3 + (2g-2) = q^3 + q^2 - q - 2$, by Theorem 7.6.4 and Theorem 7.6.2 we have that

$$\dim C(m,q) = l(mQ_\infty) + l(mQ_\infty - D) = (m + 1 - g) - (m - q^3 + 1 - g) = q^3,$$

therefore $C(m,q) = \mathbb{F}_{q^2}^n$.
So we study the Hermitian codes with $0 \leq m \leq q^3 + (2g-2) = q^3 + q^2 - q - 2$.

Now we report a result (see Lemma 6.4.4. of [Sti93]), that we need for the our following propositions and the four phases of Hermitian code, that are in Chapter 5.

Let $m, i, j \geq 0$, $j \leq q-1$ and $iq + j(q+1) \leq m$. Then the elements $x^i y^j$ form a basis of $\mathcal{L}(mQ_\infty)$.

So our general result specializes as follows:

Corollary 7.6.17. *Let $\mathcal{H} \subset \mathbb{P}^2$ be the Hermitian curve defined over $\mathbb{F}_{q^2}$. Let $C(D,G)^\perp$ be the Hermitian code. Let d be the minimum distance and let $\{P_{i_1}, \dots, P_{i_d}\}$ be the points in the support of a minimum weight codeword.*

- *If $0 \leq m \leq q^2 - 2$, then all the points P_{i_j} are collinear.*
- *If $m \geq q^2 - 1$, then the following holds.*
  - *(i) If $d \leq q+1$, then all the points P_{i_j} are collinear.*
  - *(ii) If $d \leq 2q$, then either $q+1$ of the points P_{i_j} are collinear, or all the points P_{i_j} lie on a plane conic.*
  - *(iii) If $d \leq 3q-3$, then either $q+1$ of the points P_{i_j} are collinear, or $2q$ of the points P_{i_j} lie on a plane conic, or all the points P_{i_j} lie at the intersection of two coplanar plane curves of respective degrees 3 and $q-1$.*

Proof. $\mathcal{L}(G) = \langle \{x^i y^j : i \geq 0, 0 \leq j \leq q-1, iq + j(q+1) \leq m\} \rangle$ and $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(k))$ can be identified with the set of polynomials in r variables of degree at most k. We want to prove that $\mathcal{L}(G) \supseteq H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(k))$ for every $k \geq 0$ such that $k \leq q-1$ and $k(q+1) \leq m$.

- Let $0 \leq m \leq q^2-2$ and let $d = u+2$. So $u = d-2 < q-1$. We have $m = aq+b$ with $1 \leq b \leq a \leq q-1$ and $b \neq q-1$. So we know that $d = a+1$ if $a > b$ and $d = a+2$ if $a = b$. Hence $d = u+2$ implies:

  for $a > b$, $u = a-1$ and so $u(q+1) = (a-1)(q+1) \leq m$ since $a \leq q-1$.

  for $a = b$, $u = a$ and so $u(q+1) = a(q+1) = m \leq m$.

- Let $m \geq q^2 - 1$ and let $u = q-1$. Then $u(q+1) = q^2 - 1 \leq m$.

We proved that $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(u)) \subseteq \mathcal{L}(G)$. Now our claim follows from Theorem 7.6.15. □

Note that the first point of Corollary 7.6.17 we have proved in Section 7.3, specifically in Corollary 7.3.1 and in Proposition 7.3.3 and the second point is significant just for the second phase. In fact the corresponding minimum distance satisfies our assumption $d \leq 3q-3$ only for $q \leq 3$ in the third phase and never in the fourth phase.

In the case of Hermitian codes we may even describe the geometry of small, even if not minimum, weight codewords (notice that our technical assumption $\mathcal{L}(G) = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d-2))$ is satisfied by Definition 7.1.1 of corner code).

Proposition 7.6.18. *Let $\mathcal{H} \subset \mathbb{P}^2$ be the Hermitian curve defined over $\mathbb{F}_{q^2}$. Let $C(D,G)^\perp$ be the Hermitian code. If $0 \leq m \leq q^2-2$ and $\mathcal{L}(G) = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d-2))$, then at least $d-1$ of the points $\{P_{i_1}, \ldots, P_{i_{d+\delta}}\}$ in the support of a codeword of weight $d+\delta$, where $0 \leq \delta \leq d-3$, are collinear.*

Proof. If c_j are the non-zero components of the corresponding codeword, then

$$\sum_{j=1}^{d+\delta} c_j f(P_{i_j}) = 0$$

for every $f \in \mathcal{L}(G) \supseteq H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d-2))$, in particular $\{P_{i_1}, \ldots, P_{i_{d+\delta}}\}$ are $(d-2)$-linked.

If they are not minimally $(d-2)$-linked, then (up to reordering) we have

$$\sum_{j=1}^{d+\delta-1} b_j f(P_{i_j}) = 0$$

for every $f \in H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d-2))$. Our assumption $\mathcal{L}(G) = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d-2))$ implies that the b_j's are the components of a codeword of weight strictly less than $d+\delta$. By induction on δ starting from Corollary 7.6.17 we conclude that at least $d-1$ of them are collinear.

Assume now that the points $\{P_{i_1}, \ldots, P_{i_{d+\delta}}\}$ are minimally $(d-2)$-linked. If they are not collinear, there exists a hyperplane H containing exactly l of them, with $2 \leq l \leq d+\delta-1$. By Lemma 7.6.8, the remaining $d+\delta-l$ points are (minimally) $(d-3)$-linked and from Proposition 7.6.11, it follows that at least $(d-1)$ of them are collinear since by our numerical assumption on δ we have $d+\delta-l \leq 2(d-3)+1$. □

Decoding of affine-variety codes

In this chapter we report our article [MOS12].

The approach presented in Section 4.3 shares the same problem with other similar approaches ([CRHT94b],[LY97],[CM02a]). In the portion of the Gröbner basis corresponding to the elimination ideal $I_{S,x_{t,1}}$ (see Section 2.3), one should choose a polynomial g in $\mathbb{F}_q[S, x_{t,1}] \setminus \mathbb{F}_q[S]$, specialize it to the received syndrome, and then find its $x_{t,1}$-roots. The problem is that it is not possible to know in advance which polynomial has to be chosen, and there might be hundreds of "candidate" polynomials. Let us call ideal $J^{C,t}_{\mathcal{FL}}$ the "Cooper ideal for affine-variety codes" (the convenience for this historically inaccurate name will be clear in a moment) and the "Cooper variety" its variety.

The same problem is present in the ideal for decoding cyclic codes presented in [CRHT94b], which we will call the "Cooper ideal for cyclic codes" (although again its formal definition was first presented in [CRHT94b]), where a huge number of polynomials can be found as soon as the code parameters are not trivial. In this case an improvement was proposed in [CM02a]. Instead of specializing the whole polynomial, one can specialize only its leading polynomial, since it does not vanish identically if and only if the whole polynomial does not vanish (by the Gianni-Kalkbrener theorem, that is, Theorem 2.3.3). We could adopt exactly the same strategy for the "Cooper ideal for affine-variety codes" and thus get a significant improvement on the algorithm proposed in [FL98]. This improvement would reduce the cost of the specialization, but would still require an evaluation (in the worst case) for any candidate polynomial. In Section 7 of [CM02a] a more refined strategy has been investigated, that is, the vanishing conditions coming from the leading polynomials were grouped and a decision tree was formed. In the example proposed there, this resulted in a drastic reduction of the computations required to identify the right candidate. Unfortunately, this strategy has not been deeply investigated in the general case, but we believe that it is obvious how this could be done also for the Cooper ideal for affine-variety codes, obtaining thus another improvement.

In [LY97] it was noted that the Cooper variety for cyclic codes contains also points that do not correspond to valid syndrome-error location pairs and thus are

useless. In [OS05] the authors enlarge the Cooper ideal in order to remove exactly the non-valid pairs, which we call "spurious solutions". The new ideal turns out to be stratified (although the notion of stratified ideal is established later in [GS09]) and hence to contain the general error locator polynomial, thanks to deep properties of some Gröbner bases of stratified ideals, which is the *only* polynomial that needs to be specialized. We are now going to explain how this improvement can be obtained also for the Cooper variety for affine-variety codes.
We define several modified versions of the Cooper ideal for decoding affine-variety codes. We summarize what we are going to do:

- In Section 8.1 we define a decoding ideal $J_*^{C,t}$ (8.6) that is able to correct any correctable error, even not knowing in advance the number of errors.

- However, in Section 8.2 we show why this decoding ideal does not necessarily contain locator polynomials that play the same role of generator error locator polynomials for cyclic codes. Still, these weak forms of locators (Definition 8.2.5) can be used to decode.

- In Section 8.3 we develop the commutative algebra necessary to show the existence of weak locators, with Section 8.4 devoted to the long proof of the main result, and then in Section 8.5 we will finally be able to define a set of multidimensional general error locator polynomials (see Definition 8.5.2). We define a suitable ideal containing this set as we show in Theorem 8.6.6.

We note that other authors try to link the lexicographic Gröbner basis of an ideal with the points of its variety, using interpolation at the univariate level, see, for example, [Led08].

8.1 Decoding with ghost points

Note that Fitzgerald and Lax consider the possible error locations as t points in $\mathcal{V}(I)$, that we call $P_{\sigma_1}, \ldots, P_{\sigma_t}$, but they denote their components dropping the reference to σ, that is, $P_{\sigma_l} = (x_{l,1}, \ldots, x_{l,m})$ for $1 \leq l \leq t$. We adhere to this notation from now on.

We observe that in the Cooper ideal (4.8) there is not any constraint on point pairs. But we want that all error locations are distinct. We have to force this, i.e. any two locations $P_{\sigma_j} = (x_{j,1}, \ldots, x_{j,m})$ and $P_{\sigma_k} = (x_{k,1}, \ldots, x_{k,m})$ must differ in at least one component. So we add this condition:

$$\prod_{1 \leq \iota \leq m} ((x_{j,\iota} - x_{k,\iota})^{q-1} - 1) = 0 \qquad \text{for } 1 \leq j < k \leq t.$$

In fact, if $\alpha \in \mathbb{F}_q$, then $\alpha \neq 0 \iff \alpha^{q-1} = 1$. Therefore, the product $\prod_{1\leq\iota\leq m}((x_{j,\iota} - x_{k,\iota})^{q-1} - 1)$ is zero if and only if at least for one ι we have $(x_{j,\iota} - x_{k,\iota})^{q-1} = 1$, i.e. $x_{j,\iota} \neq x_{k,\iota}$ and thus $P_{\sigma_j} \neq P_{\sigma_k}$. Our ideal becomes

$$\begin{aligned} \widehat{J}_{\mathcal{FL}}^{C,t} = \Big\langle \quad & \Big\{\textstyle\sum_{j=1}^{t} e_j b_\rho(x_{j,1},\ldots,x_{j,m}) - s_\rho\Big\}_{1\leq\rho\leq r}, \{e_j^{q-1} - 1\}_{1\leq j\leq t}, \\ & \{g_h(x_{j,1},\ldots,x_{j,m})\}_{\substack{1\leq h\leq\gamma,,\\ 1\leq j\leq t}} \\ & \big\{\textstyle\prod_{1\leq\iota\leq m}((x_{j,\iota} - x_{k,\iota})^{q-1} - 1)\big\}_{1\leq j<k\leq t} \Big\rangle \quad . \end{aligned} \tag{8.1}$$

Remark 8.1.1. Ideal $\widehat{J}_{\mathcal{FL}}^{C,t}$ can be used to correct and it will work better than $J_{\mathcal{FL}}^{C,t}$, since its variety does not contain spurious solutions. However, we cannot expect that $\widehat{J}_{\mathcal{FL}}^{C,t}$ contains polynomials with a role similar to that of the generic error locator in the cyclic case, because $\widehat{J}_{\mathcal{FL}}^{C,t}$ still depends on the knowledge of the error number.

In the following we modify (8.1) to allow for different-weight syndromes.

(a) First, we note that in $\widehat{J}_{\mathcal{FL}}^{C,t}$ the following condition is verified

$$e_j^{q-1} = 1 \text{ with } j = 1,\ldots,t.$$

This is equivalent to saying that exactly t errors occurred, which are $e_1,\ldots,e_t \in \mathbb{F}_q^*$. We must allow for some e_j with $j = 1,\ldots,t$ to be equal to zero. We would obtain a new ideal where the conditions $e_j^{q-1} = 1$ are replaced with $e_j^q = e_j$ for every $j = 1,\ldots,t$.

(b) We recall the changes made to the Cooper ideal in [OS05] for cyclic codes. We consider the error vector

$$e = (\underbrace{0,\ldots,0}_{k_1-1}, \underset{\uparrow}{e_1}_{k_1}, 0,\ldots,0, \underset{\uparrow}{e_l}_{k_l}, 0,\ldots,0, \underset{\uparrow}{e_\mu}_{k_\mu}, \underbrace{0,\ldots,0}_{n-1-k_\mu}) \quad \text{with } \mu \leq t,$$

where $k_1,\ldots,k_\mu$ are the error positions and $e_1\ldots,e_\mu$ are the error values. We consider the j-th syndrome and we obtain the following equation

$$\sum_{l=1}^{\mu} e_l(\alpha^{i_j})^{k_l} = s_j. \tag{8.2}$$

(For the n-th root codes in [GS06, GS09] the formulas are slightly more complicated). To arrive at the desired equation

$$\sum_{l=1}^{t} e_l(\alpha^{i_j})^{k_l} = s_j \tag{8.3}$$

we have to add the "virtual error position" k defined as $\alpha^{\mathsf{k}} = 0 \ \forall \alpha \in \mathbb{F}$. Using the location $z_l = \alpha^{k_l}$ (and so the "virtual error location" is $\alpha^{\mathsf{k}} = 0$), equation (8.3) becomes

$$s_j = \sum_{l=1}^{\mu} e_l (z_l)^{i_j} + \sum_{l=\mu+1}^{t} e_l (\alpha^{\mathsf{k}})^{k_l} = \sum_{l=1}^{\mu} e_l (z_l)^{i_j} + \sum_{l=\mu+1}^{t} e_l (0)^{k_l} = \sum_{l=1}^{t} e_l (z_l)^{i_j}.$$

We can rephrase what we did by saying that we are using 0 as a *ghost error location*, meaning that if we find ν zero roots in the error location polynomial, then $\mu = t - \nu$ (ν error locations are ghost locations and so they do not correspond to actual errors).

(c) Let us come back to the affine-variety case. The error vector is

$$e = (\underbrace{0, \ldots, 0}_{\sigma_1 - 1}, \underset{\uparrow}{e_1}, \underset{P_{\sigma_1}}{}, 0, \ldots, 0, \underset{\uparrow}{e_l}, \underset{P_{\sigma_l}}{}, 0, \ldots, 0, \underset{\uparrow}{e_\mu}, \underset{P_{\sigma_\mu}}{}, \underbrace{0, \ldots, 0}_{n-1-\sigma_\mu}).$$

The valid error locations are the points $P_{\sigma_l} = (x_{l,1}, \ldots, x_{l,m})$, $1 \leq l \leq \mu$. The equation corresponding to (8.2) is

$$s_\rho = \sum_{l=1}^{\mu} e_l b_\rho (P_{\sigma_l}) = \sum_{l=1}^{\mu} e_l b_\rho (x_{l,1}, \ldots, x_{l,m}). \tag{8.4}$$

We want a sum like (8.3), something like $s_\rho = \sum_{l=1}^{t} e_l b_\rho (P_{\sigma_l})$. In order to do that, we would need $\sum_{l=\mu+1}^{t} e_l b_\rho (P_{\sigma_l}) = 0$, for some convenient *ghost points* $\{P_{\sigma_l}\}_{\mu+1 \leq l \leq t}$. Actually, we can use just one ghost point, that we call P_0. But it must *not* lie on the variety, otherwise it could be confused with valid locations. In particular, we cannot hope to use always the ghost point $P_0 = (x_{0,1}, \ldots, x_{0,m}) = (0 \ldots, 0)$, since $(0 \ldots, 0)$ could be a point on the variety. For example, the Hermitian curve $\mathcal{H} : x^{q+1} = y^q + y$ contains $(0, 0)$ for any q.
Let P_0 be a ghost point. Not only do we need to choose P_0 outside the variety, but we must also force $e_j = 0$ for the error values in P_0, since we cannot hope that $b_\rho(P_0) = 0$ for each ρ. With these assumptions, we obtain

$$\begin{array}{rcl} s_\rho & = & \sum_{l=1}^{\mu} e_l b_\rho (x_{l,1}, \ldots, x_{l,m}) + \sum_{l=\mu+1}^{t} e_l b_\rho (P_0) \\ & = & \sum_{l=1}^{\mu} e_l b_\rho (x_{l,1}, \ldots, x_{l,m}) + \sum_{l=\mu+1}^{t} 0 \, b_\rho (P_0) \\ & = & \sum_{l=1}^{\mu} e_l b_\rho (x_{l,1}, \ldots, x_{l,m}) \, . \end{array} \tag{8.5}$$

(d) For us a ghost point is any point $P_0 \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$. Depending on the variety, there can be clever ways to choose P_0.

Definition 8.1.2. *Let $P_0 = (\overline{x}_{0,1}, \ldots, \overline{x}_{0,m}) \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$. We say that P_0 is an **optimal ghost point** if there is a $1 \leq j \leq m$ such that the hyperplane $x_j = \overline{x}_{0,j}$ does not intersect the variety. We call j the **ghost component**.*

In other words, for any optimal ghost point there is at least a component not shared with any variety point. See Figure 8.1 for an example.

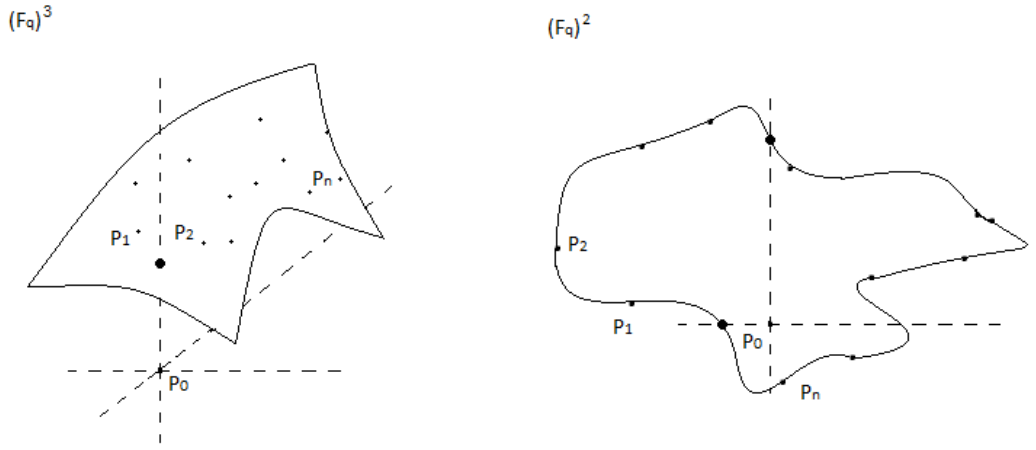


Figure 8.1: In the first picture we have a optimal ghost point with two ghost components. In the second, a non-optimal ghost point.

Remark 8.1.3. The advantage of using optimal ghost points is that it is enough to look at any ghost component in order to discard non-valid locations.

If a curve is smooth and maximal (e.g., an Hermitian curve), it will probably intersect any hyperplane and so no optimal ghost point will exist in this case.

(e) We are ready to define a new ideal, summarising the above argument.
We start from equations (8.5):

$$\left\{ \sum_{j=1}^{t} e_j b_\rho(x_{j,1}, \ldots, x_{j,m}) - s_\rho \right\}_{1 \leq \rho \leq r}$$

We choose a ghost point $P_0 = (x_{0,1}, \ldots, x_{0,m}) \notin \mathcal{V}(I)$. We need to find a generator set for the radical ideal I' vanishing on $\mathcal{V}(I) \sqcup \{P_0\}$. The easiest way of doing this is to start from any Gröbner basis G of I and to use the Buchberger-Möller algorithm (see Theorem 2.2.17) to compute the Gröbner basis G' of

I'. We restate Buchberger-Möller algorithm in Theorem 8.4.1 (with respect to Theorem 2.2.17) using a slightly different notation. Let $G' = \{g'_h\}_{1\leq h\leq \gamma'}$. We can insert in our new ideal the following polynomials

$$\{g'_h(x_{j,1},\ldots,x_{j,m})\}_{\substack{1\leq h\leq \gamma',\\ 1\leq j\leq t}}$$

In our new system we put $\{e_j^q = e_j\}$, because there can be zero values (corresponding to ghost locations). We enforce $(x_{j,1},\ldots,x_{j,m}) \neq P_0$ for all j corresponding to actual error locations. In order to do that, when $e_j \neq 0$ we must have at least one component of P_{σ_j} different from that of P_0, that is, $e_j \prod_{1\leq\iota\leq m}((x_{j,\iota}-x_{0,\iota})^{q-1}-1) = 0$. So we can add

$$\left\{ e_j \prod_{1\leq\iota\leq m}((x_{j,\iota}-x_{0,\iota})^{q-1}-1) \right\}_{1\leq j\leq t}.$$

On the other hand, when $e_j = 0$ we want $(x_{j,1},\ldots,x_{j,m}) = P_0$. To enforce it, we add

$$\left\{(e_j^{q-1}-1)(x_{j,\iota}-x_{0,\iota})\right\}_{\substack{1\leq j\leq t,\\ 1\leq\iota\leq m}}.$$

Finally, if two points correspond to valid locations then they must be distinct. However, if at least one is a ghost point, then the following requirement does not hold:

$$\left\{ e_j e_k \prod_{1\leq\iota\leq m}((x_{j,\iota}-x_{k,\iota})^{q-1}-1) \right\}_{1\leq j<k\leq t}.$$

We denote by $J_*^{C,t}$ the ideal in $\mathbb{F}_q[s_1,\ldots,s_r,X_t,\ldots,X_1,e_1,\ldots,e_t]$, with $X_1 = \{x_{1,1},\ldots,x_{1,m}\},\ldots,X_t = \{x_{t,1},\ldots,x_{t,m}\}$ s.t.

$$\begin{aligned} J_*^{C,t} = \Big\langle \quad & \left\{\textstyle\sum_{j=1}^t e_j b_\rho(x_{j,1},\ldots,x_{j,m}) - s_\rho\right\}_{1\leq\rho\leq r}, \{e_j^q - e_j\}_{1\leq j\leq t}, \\ & \{g'_h(x_{j,1},\ldots,x_{j,m})\}_{\substack{1\leq h\leq\gamma',\\ 1\leq j\leq t}}, \left\{(e_j^{q-1}-1)(x_{j,\iota}-x_{0,\iota})\right\}_{\substack{1\leq j\leq t,\\ 1\leq\iota\leq m}}, \\ & \left\{e_j \textstyle\prod_{1\leq\iota\leq m}((x_{j,\iota}-x_{0,\iota})^{q-1}-1)\right\}_{1\leq j\leq t}, \\ & \left\{e_j e_k \textstyle\prod_{1\leq\iota\leq m}((x_{j,\iota}-x_{k,\iota})^{q-1}-1)\right\}_{1\leq j<k\leq t}\Big\rangle. \end{aligned} \tag{8.6}$$

Since $I' = \langle\{g'_h\}_{1\leq h\leq H}\rangle$ contains the field equations, we may add them to reduce the computation of the Gröbner basis of $J_*^{C,t}$.

8.2 Weak locator polynomials

We would like to define some locator polynomials for affine-variety codes that play the same role as those in Definition 4.4.7. We would expect to find them in our ideal (8.6). These locators might look like

$$\mathcal{L}_i(S, x_1, \ldots, x_i) = x_i^t + a_{t-1}x_i^{t-1} + \cdots + a_0, \tag{8.7}$$

with $a_j \in \mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$, $0 \leq j \leq t-1$, that is, $\mathcal{L}_i$ is a monic polynomial with degree t with respect to the variable x_i and its coefficients are in $\mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$. We would also want the following property.
Given a syndrome $\mathbf{s} = (\bar{s}_1, \ldots \bar{s}_r) \in (\mathbb{F}_q)^r$, corresponding to an error vector of weight $\mu \leq t$ and μ error locations $(\bar{x}_{1,1}, \ldots, \bar{x}_{1,m})$, $\ldots$, $(\bar{x}_{\mu,1}, \ldots, \bar{x}_{\mu,m})$, if we evaluate the S variables at $\mathbf{s}$ and the variables $x_1, \ldots, x_{i-1}$ at $\bar{x}_{j,1}, \ldots, \bar{x}_{j,i-1}$ for any $1 \leq j \leq \mu$, then the roots of $\mathcal{L}_i(\mathbf{s}, \bar{x}_{j,1}, \ldots, \bar{x}_{j,i-1}, x_i)$ are either $\{\bar{x}_{1,i}, \ldots, \bar{x}_{t,i}\}$, when $\mu = t$, or $\{\bar{x}_{1,i}, \ldots, \bar{x}_{\mu,i}, \bar{x}_{0,i}\}$, when $\mu \leq t-1$. Apart from the actual location components and possibly the ghost component, polynomial $\mathcal{L}_i$ should not have other solutions.

To show that a polynomial of this kind does not necessarily exist in $J_*^{C,t}$, we consider the following examples.

Example 8.2.1. Let us consider an MDS code $C = C^{\perp}(I, L)$ $[5, 1, 5]$ from the plane curve $\{y^5 - y^4 + y^3 - y^2 + y - x = 0\} \cap \{x - 1 = 0\}$ over $\mathbb{F}_7$ and with

$$L = \{y - 3, y^2 - 1, y^3 + 3, y^4 - 1\},$$
$$\mathcal{V}(I) = \{(1,1), (1,2), (1,3), (1,4), (1,5)\}.$$

It is easy to see that C can correct up to $t = 2$ errors. Let us consider the lex term-ordering with $s_1 < s_2 < s_3 < s_4 < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ in $\mathbb{F}_7[s_1, s_2, s_3, s_4, s_5, x_2, y_2, x_1, y_1, e_1, e_2]$. Ideal $J_*^{C,t}$ is generated by

$$\begin{aligned}
&\langle e_1^7 - e_1, e_2^7 - e_2, x_1 - 1, x_2 - 1, y_1^6 - y_1^5 + y_1^4 - y_1^3 + y_1^2 - y_1, y_2^6 - y_2^5 + y_2^4 - y_2^3 + y_2^2 - y_2,\\
&e_1(-y_1^4 + y_1^3 + y_1^2 - 2y_1 + 2) + e_2(-y_2^4 + y_2^3 + y_2^2 - 2y_2 + 2) - s_1, e_2((x_2 - 1)^6 - 1)(y_2^6 - 1),\\
&e_1(3y_1^4 - 2y_1^3 + 3y_1^2 + 3y_1) + e_2(3y_2^4 - 2y_2^3 + 3y_2^2 + 3y_2) - s_2, e_1(3y_1^4 - y_1^2 - 2) + e_2(3y_2^4 - y_2^2 - 2) - s_3,\\
&e_1(-y_1^4 + 2y_1^3 - y_1^2 - 3y_1 + 3) + e_2(-y_2^4 + 2y_2^3 - y_2^2 - 3y_2 + 3) - s_4, e_1((x_1 - 1)^6 - 1)(y_1^6 - 1),\\
&e_1e_2((x_1 - x_2)^6 - 1)((y_1 - y_2)^6 - 1), (e_2^6 - 1)(x_2 - 1), (e_2^6 - 1)y_2, (e_1^6 - 1)(x_1 - 1), (e_1^6 - 1)y_1\rangle,
\end{aligned}$$

where the ghost point is $P_0 = (1, 0)$. The reduced Gröbner basis G with respect to $s_1 < s_2 < s_3 < s_4 < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ has 27 elements and the *new locators* are $\mathcal{L}_1(s_1, \ldots, s_5, x_2) = \mathcal{L}_x$ and $\mathcal{L}_2(s_1, \ldots, s_5, x_2, y_2) = \mathcal{L}_{xy}$ (see Appendix for polynomials a and b):

$$\mathcal{L}_x = \mathbf{x} - 1 \text{ and } \mathcal{L}_{xy} = \mathbf{y}^2 + \mathbf{y}a + b.$$

Note that $\mathcal{L}_x$ does not play any role, because all x's are equal to 1. So to apply the decoding we evaluate only $\mathcal{L}_{xy}$ at $\overline{\mathbf{s}}$ and we expect to obtain the (second) components of error locations. We show it in two cases:

- We suppose that two errors occur at the points $P_1 = (1,1)$ and $P_2 = (1,2)$, both with error values 1, so the syndrome vector corresponding to the error vector $(1,1,0,0,0)$ is $\overline{\mathbf{s}} = (2,1,0,0)$.
  In order to find the error positions we evaluate $\mathcal{L}_{xy}$ in $\overline{\mathbf{s}}$. We obtain two different solutions $\mathcal{L}_{xy}(\overline{\mathbf{s}}, y) = y^2 - 3y + 2 = (y-2)(y-1)$, that identify the two error locations.

- We consider $\overline{\mathbf{s}} = (0,4,4,0,1)$ corresponding to $(0,0,0,4,0)$, so only one error occurs in the point $(1,3)$. Evaluating $\mathcal{L}_{xy}$ at $\overline{\mathbf{s}}$ we obtain $\mathcal{L}_{xy}(\overline{\mathbf{s}}, y) = y^2 - 3y = y(y-3)$. Also in this case we obtain a correct solutions (0 is the ghost component). So the above choice of $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ seems correct.

Now we consider the above code but with a different ghost point. Also in the following example, we take an optimal ghost point.

Example 8.2.2. Let us consider the same MDS code $C = C^{\perp}(I, L)$ as in Example 8.2.1. In this example we choose the (optimal) ghost point $P_0 = (0,0)$. The ideal $J_*^{C,t}$ is generated by

$$\begin{aligned}
&\langle e_1^7 - e_1, e_2^7 - e_2, x_1y_1 - y_1, x_2y_2 - y_2, x_1^2 - x_1, x_2^2 - x_2, y_1^6 - y_1^5 + y_1^4 - y_1^3 + y_1^2 - y_1,\\
&y_2^6 - y_2^5 + y_2^4 - y_2^3 + y_2^2 - y_2, e_1(-y_1^4 + y_1^3 + y_1^2 - 2y_1 + 2) + e_2(-y_2^4 + y_2^3 + y_2^2 - 2y_2 + 2) - s_1,\\
&e_1(3y_1^4 - 2y_1^3 + 3y_1^2 + 3y_1) + e_2(3y_2^4 - 2y_2^3 + 3y_2^2 + 3y_2) - s_2, e_1(3y_1^4 - y_1^2 - 2) + e_2(3y_2^4 - y_2^2 - 2) - s_3,\\
&e_1(-y_1^4 + 2y_1^3 - y_1^2 - 3y_1 + 3) + e_2(-y_2^4 + 2y_2^3 - y_2^2 - 3y_2 + 3) - s_4, e_1(x_1^6 - 1)(y_1^6 - 1),\\
&e_2(x_2^6 - 1)(y_2^6 - 1), e_1e_2((x_1 - x_2)^6 - 1)((y_1 - y_2)^6 - 1), (e_2^6 - 1)x_2, (e_2^6 - 1)y_2, (e_1^6 - 1)x_1, (e_1^6 - 1)y_1.\rangle,
\end{aligned}$$

The reduced Gröbner basis G with respect to $s_1 < s_2 < s_3 < s_4 < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ has 27 elements and the *new locators* are $\mathcal{L}_1(\mathcal{S}, x_2) = \mathcal{L}_x$ and $\mathcal{L}_2(\mathcal{S}, x_2, y_2) = \mathcal{L}_{xy}$, where $\mathcal{S} = \{s_1, \ldots, s_5\}$ (see Appendix for c and d):

$$\mathcal{L}_x = \mathbf{x}^2 - \mathbf{x} \text{ and } \mathcal{L}_{xy} = \mathbf{y}^2 + \mathbf{y}c + d. \tag{8.8}$$

Also in this case $\mathcal{L}_x$ does not depend on any syndrome, so to apply the decoding we just specialize $\mathcal{L}_{xy}(\overline{\mathbf{s}}, \overline{\mathbf{x}}, y)$. We would like that the solutions of $\mathcal{L}_{xy}(\overline{\mathbf{s}}, \overline{\mathbf{x}}, y) = 0$ are exactly the second components of error locations, but this is not always the case. Let us consider the same errors as in Example 8.2.1:

- We suppose that two errors occur at the points $P_1 = (1,1)$ and $P_2 = (1,2)$, with both error values 1, so the syndrome vector corresponding to the error vector

$(1,1,0,0,0)$ is $\overline{\mathbf{s}} = (2,1,0,0)$. In order to find the error positions we evaluate $\mathcal{L}_{xy}$ in $\overline{\mathbf{s}}$. We obtain three different solutions

$$\mathcal{L}_{xy}(\overline{\mathbf{s}},1,y) = y^2 - 3y + 2 = (y-1)(y-2),$$
$$\mathcal{L}_{xy}(\overline{\mathbf{s}},0,y) = y^2 - 3y - 3 = (y+2)^2.$$

In this case, we are lucky, because $(0,5)$ is not a point coordinate and so we can discard $y = 5$ finding the two error locations.

- We consider $\overline{\mathbf{s}} = (0,4,4,0,1)$ corresponding to $(0,0,0,4,0)$, so only one error occurs in the point $(1,3)$. Evaluating $\mathcal{L}_{xy}$ in $(\overline{\mathbf{s}})$ we obtain

$$\mathcal{L}_{xy}(\overline{\mathbf{s}},1,y) = y^2 - y + 1 = (y-3)(y+2),$$
$$\mathcal{L}_{xy}(\overline{\mathbf{s}},0,y) = y^2 - y = y(y-1).$$

In this case we have four possible solutions $(1,3)$, $(1,5)$,$(0,0)$ and $(0,1)$, but only three are acceptable, which are $(1,3)$, $(1,5)$ and $(0,0)$. To individuate those corresponding to the syndrome vector $\overline{\mathbf{s}}$, we must compute the two syndromes and we will see that $(1,3)$ and $(0,0)$ are correct. In this case, the above choice of $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ is unfortunate.

One might think that the unpleasant behaviour of (8.8) is due to the degenerate geometric situation. Unfortunately, this is not entirely true, as next the example shows (we end this long example with a horizontal line).

Example 8.2.3. Let us consider, as in Example 4.3.1, the Hermitian code $C = C^{\perp}(I,L)$ from the curve $y^2+y = x^3$ over $\mathbb{F}_4$ and with defining monomials $\{1,x,y,x^2,xy\}$. It is well-known that C can correct up to $t = 2$ errors. Let us consider the lexicographic term-ordering with $s_1 < \ldots < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ in $\mathbb{F}_4[s_1,s_2,s_3,s_4,s_5,x_2,y_2,x_1,y_1,e_1,e_2]$. Ideal $J^{C,t}_{\mathcal{FL}}$ is

$$\langle x_1^4 - x_1, y_1^4 - y_1, x_2^4 - x_2, y_2^4 - y_2, e_1^3 - 1, e_2^3 - 1, y_1^2 + y_1 - x_1^3, y_2^2 + y_2 - x_2^3,$$
$$e_1 + e_2 - s_1,\ \ e_1x_1 + e_2x_2 - s_2,\ \ e_1y_1 + e_2y_2 - s_3,\ \ e_1x_1^2 + e_2x_2^2 - s_4,$$
$$e_1x_1y_1 + e_2x_2y_2 - s_5\rangle,$$

and the reduced Gröbner basis G (with respect to $<$) has 53 elements.
The authors of [FL98] report 119 polynomials because they do not use lex but a block order, which is faster to compute but which usually possesses larger Gröbner bases. In $G \cap (\mathbb{F}_4[S,x_2] \setminus \mathbb{F}_4[S])$ there are 5 polynomials of degree 2 in x_2 and these are our candidate polynomials:

$$\begin{aligned} g_5 = \ & \mathbf{x_2}^2 s_5 + \mathbf{x_2}(s_5s_4s_2^2 + s_4^2s_3^2s_2s_1^2 + s_4^2s_2s_1 + s_4s_3^2s_1 + s_4s_3^3s_2^2s_1^2 + s_4s_3s_1^2 + s_4s_1^3 + s_3^2s_2^2s_1^3 + s_2^2s_1^2) + \\ & s_5^3s_3 + s_5s_4^2s_3^3s_2 + s_5s_4^2s_2 + s_4^3s_3^3s_2^3s_1 + s_4^3s_3^3s_1 + s_4^3s_3^2s_2^3s_1^2 + s_4^3s_3s_2^3 + s_4^3s_1 + s_4^2s_3^3s_2^2 + s_4^2s_3^2s_2^2s_1 + \\ & s_4s_3^2s_2 + s_4s_2s_1^2 + s_3^3s_2^3s_1 + s_3s_2^3s_1^3 + s_3s_2^3 + s_2^3s_1 \end{aligned}$$

$$g_4 = \mathbf{x_2}^2 s_4 + \mathbf{x_2}(s_4^2 s_2^2 + s_2^3 s_1 + s_1 + s_4^2 s_3^2 s_1^3) + s_4^2 s_3^2 + s_4^2 s_2^3 s_1^2 + s_4^2 s_1^2 + s_4 s_3 s_2^2 s_1^3 + s_4 s_3 s_2^2 + s_2 s_1^3 + s_2$$

$$g_3 = \mathbf{x_2}^2 s_3 + \mathbf{x_2}(s_4^2 s_3 s_1 + s_4 s_3 s_2^2 s_1^3 + s_4 s_3 s_2^2 + s_3 s_2 s_1^2) + s_5^2 s_3^2 + s_5 s_3^2 s_2 + s_4^2 s_3^3 s_2 s_1 + s_4^2 s_3^2 s_2 s_1^2 + s_4 s_3^3 s_1^3 + s_4 s_3^2 s_1 + s_3^3 s_2^2 s_1^2 + s_3^2 s_2^2 s_1^3 + s_3^2 s_2^2$$

$$g_2 = \mathbf{x_2}^2 s_2 + \mathbf{x_2}(s_4^2 s_2 s_1 + s_4 s_1^3 + s_4 + s_2^2 s_1^2) + s_4^2 s_2^2 + s_4 s_3^2 s_2 s_1^3 + s_4 s_3^2 s_2 + s_4 s_2 s_1^2 + s_3 s_2^3 s_1^3 + s_3 s_2^3 + s_2^3 s_1$$

$$g_1 = \mathbf{x_2}^2 (s_1) + \mathbf{x_2}(s_4^2 s_1^2 + s_2 s_1^3) + s_4^2 s_2 s_1 + s_4 s_1^3 + s_2^2 s_1^2$$

Of course, there are other similar polynomials in $J_{\mathcal{FL}}^{C,t} \cap (\mathbb{F}_4[S, x_2] \setminus \mathbb{F}_4[S])$ and they may be found for example by computing Gröbner bases with respect to other orderings. It is immediate that the leading polynomials are just $\{s_1, \ldots, s_5\}$. Suppose that we receive a syndrome $\mathbf{s} = (\bar{s}_1, \ldots, \bar{s}_5)$. If it is zero, then no errors occurred. Otherwise, we might follow the most obvious way to correct, that is, we might substitute $\mathbf{s}$ in all g_i's, until we find one which does not vanish identically. The improvement introduced by Caboara and Mora translates here in checking only the leading polynomials, i.e. checking which of the syndrome components $\bar{s}_i$ is non-zero. Since clearly at least one is non-zero, with a negligible computational effort we are able to determine the right candidate.

Let us now follow our proposal. Ideal $J_*^{C,t}$ is generated by

$$\begin{aligned}
&\{x_1^4 - x_1,\ y_1^4 - y_1,\ x_2^4 - x_2,\ y_2^4 - y_2,\ e_1^4 - e_1,\ e_2^4 - e_2,\ y_1^2 x_1 + y_1^2 + y_1 x_1 + y_1 + x_1^3 + x_1,\\
&y_2^2 x_2 + y_2^2 + y_2 x_2 + y_2 + x_2^3 + x_2, y_1^3 + y_1 x_1^3 + y_1 + x_1^3, y_2^3 + y_2 x_2^3 + y_2 + x_2^3, e_1 + e_2 - s_1,\\
&e_1 x_1 + e_2 x_2 - s_2,\ e_1 y_1 + e_2 y_2 - s_3,\ e_1 x_1^2 + e_2 x_2^2 - s_4, e_1 x_1 y_1 + e_2 x_2 y_2 - s_5,\\
&e_1((x_1-1)^3 - 1)((y_1-1)^3 - 1), e_2((x_2-1)^3 - 1)((y_2-1)^3 - 1), (e_1^3 - 1)(x_1 - 1),\\
&(e_1^3 - 1)(y_1 - 1), (e_2^3 - 1)(x_2 - 1), (e_2^3 - 1)(y_2 - 1), e_1 e_2((x_1 - x_2)^3 - 1)((y_1 - y_2)^3 - 1)\}.
\end{aligned}$$

where the ghost point is $(1, 1)$ (note that $1^3 \neq 1^2 + 1$).

The reduced Gröbner basis G with respect to $s_1 < s_2 < s_3 < s_4 < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ has 32 elements and the *new locators* are $\mathcal{L}_1(s_1, \ldots, s_5, x_2) = \mathcal{L}_x$ and $\mathcal{L}_2(s_1, \ldots, s_5, x_2, y_2) = \mathcal{L}_{xy}$, that are the polynomials of degree two in, respectively, x_2 and y_2:

$$\begin{aligned}
\mathcal{L}_x = \ & \mathbf{x}^2 + \mathbf{x}(s_1^2 s_2 s_4^3 + s_4^3 + s_1 s_2^3 s_4^2 + s_1^2 s_2^2 s_4^2 + s_1 s_4^2 + s_2^2 s_4 + s_1 s_2 s_4 + s_2^3 + s_1^2 s_2 + s_1^3) +\\
& s_3 s_5^2 + s_2 s_3 s_5 + s_1 s_2^2 s_4^3 + s_1^2 s_2 s_4^3 + s_2 s_3^3 s_4^2 + s_1 s_2 s_3^2 s_4^2 + s_1^2 s_2 s_3 s_4^2 + s_1 s_3^2 s_4^2 + s_1^3 s_2 s_4^2 +\\
& s_2 s_4^2 + s_1^2 s_3^3 s_4 + s_1^3 s_3^2 s_4 + s_1 s_3 s_4 + s_1^2 s_2^3 s_4 + s_1^3 s_2^2 s_4 + s_1^2 s_4 + s_1^3 s_2^3 s_3^3 + s_2^3 s_3^3 + s_1 s_2^2 s_3^3 +\\
& s_1^3 s_3^3 + s_3^3 + s_1^2 s_2^2 s_3^2 + s_1^3 s_2^2 s_3 + s_2^2 s_3 + s_1^3 s_2^3 + s_2^3 + s_1 s_2^2 + s_1^3 + 1
\end{aligned}$$

$$\begin{aligned}
\mathcal{L}_{xy} = \ & \mathbf{y}^2 + \mathbf{y}(s_3^3 + s_1 s_3^2 + s_1^2 s_2^3 s_3 + s_1^2 s_3 + s_1^3) + \mathbf{x}(s_2^2 s_3 s_4^3 + s_1 s_2^2 s_4^3 + s_1^2 s_2 s_3 s_4^2 + s_1^2 s_3^3 s_4 + s_3^2 s_4 +\\
& s_1 s_3 s_4 + s_1^2 s_2^3 s_4) + s_5^3 + s_2 s_3^2 s_4^2 s_5 + s_3 s_4 s_5 + s_2^2 s_5 + s_3^3 s_4^3 + s_1 s_2^3 s_3^2 s_4^3 + s_2^3 s_4^3 + s_1^2 s_2^2 s_3^3 s_4^2 +\\
& s_1^2 s_2 s_3^2 s_4 + s_1^3 s_2 s_3 s_4 + s_1 s_2 s_4 + s_2^3 s_3^3 + s_3^3 + s_1 s_2^3 s_3^2 + s_1 s_3^2 + s_1^2 s_2^3 s_3 + s_1^2 s_3 + s_1^3 s_2^3 + s_1^3 + 1
\end{aligned}$$

We can apply the decoding in this way: we specialize $\mathcal{L}_x(s, x)$ to $\bar{\mathbf{s}}$ for any received syndrome. If the syndrome corresponds to two errors, then we expect that the roots

of $\mathcal{L}_x(\overline{\mathbf{s}}, x)$ are the first components of error locations and the roots of $\mathcal{L}_{xy}(\overline{\mathbf{s}}, \overline{\mathbf{x}}, y)$ are exactly the second components of error locations. But it is not always true, we show it in three cases:

- We suppose that two errors occur at the points $P_6 = (\alpha, \alpha+1)$ and $P_7 = (\alpha+1, \alpha)$, with both error values 1, so the syndrome vector corresponding to the error vector $(0,0,0,0,0,1,1,0)$ is $\overline{\mathbf{s}} = (0,1,1,1,0)$.
  In order to find the error positions we evaluate $\mathcal{L}_x$ in $\overline{\mathbf{s}}$ and we obtain the correct values of x, in fact:

$$\mathcal{L}_x(\overline{\mathbf{s}}, x) = x^2 + x + 1 = (x-\alpha)(x-(\alpha+1)).$$

  Now we have to evaluate $\mathcal{L}_{xy}$ in $(\overline{\mathbf{s}}, \overline{\mathbf{x}})$. We obtain four different solutions

$$\mathcal{L}_{xy}(\overline{\mathbf{s}}, \alpha, y) = y^2 + y + 1 = (y-\alpha)(y-(\alpha+1))$$
$$\mathcal{L}_{xy}(\overline{\mathbf{s}}, \alpha+1, y) = y^2 + y + 1 = (y-\alpha)(y-(\alpha+1)).$$

  But this is a *problem* for us, because all these solutions are curve points: (α,α),$(\alpha,\alpha+1)$,$(\alpha+1,\alpha)$,$(\alpha+1,\alpha+1)$. Only two are the correct locations. To individuate those corresponding to the syndrome vector $\overline{\mathbf{s}}$, we must compute the two syndromes and we will see that $(\alpha+1,\alpha), (\alpha,\alpha+1)$ are correct. Another methods to find the correct locations are combinatorial algorithms as [FRR06, Lun10, GRS03]. All of these methods of try-and-see works nice because the code is small, but soon it becomes unfeasible. So the above choice of $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ is unfortunate.

- We suppose that the syndrome is $(\alpha+1, 0, \alpha, 0, 0)$, corresponding to the error vector $(1, \alpha, 0, 0, 0, 0, 0, 0)$. So two errors have occurred and their values are 1 and α in the point, respectively, $P_1 = (0,0)$ and $P_2 = (0,1)$. In order to find the error locations we evaluate $\mathcal{L}_x$ in $\overline{\mathbf{s}}$ and we obtain $\mathcal{L}_x(\overline{\mathbf{s}}, x) = x^2 + x = x(x-1)$, then we evaluate $\mathcal{L}_{xy}$ in $(\overline{\mathbf{s}}, 0)$ and $(\overline{\mathbf{s}}, 1)$ and we get $\mathcal{L}_{xy}(\overline{\mathbf{s}}, 0, y) = \mathcal{L}_{xy}(\overline{\mathbf{s}}, 1, y) = y^2 + y = y(y-1)$. The equations

$$\mathcal{L}_x(\overline{\mathbf{s}}, x) = \mathcal{L}_{xy}(\overline{\mathbf{s}}, 1, y) = \mathcal{L}_{xy}(\overline{\mathbf{s}}, 0, y) = 0 \tag{8.9}$$

  have four possible solutions: $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$. Since the points $(1,0)$ and $(1,1)$ do not lie on the Hermitian curve, then only one solution couple is admissible: $\{(0,0),(0,1)\}$. This situation is better than the above case, because we can immediately understand what the correct solutions of system (8.9) are. This happens by chance and in any case the solutions of equation $\mathcal{L}_x(\overline{\mathbf{s}}) = 0$ are not what we want.

- Finally we consider $\overline{\mathbf{s}} = (\alpha+1, \alpha+1, 1, \alpha+1, 1)$ corresponding to $(0, 0, \alpha+1, 0, 0, 0, 0, 0)$, so only one error occurs. Evaluating $\mathcal{L}_x$ and $\mathcal{L}_{xy}$, respectively, in $\overline{\mathbf{s}}$ and $(\overline{\mathbf{s}}, \overline{\mathbf{x}})$, we obtain

$$\begin{cases} \mathcal{L}_x(\overline{\mathbf{s}}, x) = x^2 + 1 \\ \mathcal{L}_{xy}(\overline{\mathbf{s}}, 1, y) = y^2 + (\alpha+1)y + \alpha = (y-1)(y-\alpha). \end{cases} \tag{8.10}$$

  In this case we are extremely lucky because the two polynomials $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ answer correctly: the solutions of system (8.10) are $(1, 1)$, which is the ghost point, and $(1, \alpha)$, which is the error location.

Remark 8.2.4. Since, in Example 8.2.3, the curve equation has all coefficients in $\mathbb{F}_2$, the ideal $J_{\mathcal{FL}}^{C,t}$ actually lies in $\mathbb{F}_2[s_1, s_2, s_3, s_4, s_5, x_2, y_2, x_1, y_1, e_1, e_2]$. This is a special case of a more general fact: for any affine variety-code and any decoding ideal that we are considering in the whole paper, all polynomials defining these ideals have no coefficient different from $\{1, -1\}$, except possibly for the polynomials defining I. Therefore, if it is possible to have a basis for the ideal I with all coefficients in a smaller field, then any of its Gröbner bases will have elements with the same coefficient field, which means that the basis computation will be much faster.

Since polynomials like $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ in Example 8.2.3 contain the right solutions (together with unwelcome parasite solutions), they deserve a definition. See Section 4.1 for our notation.

Definition 8.2.5. *Let $C = C^{\perp}(I, L)$ be an affine-variety code. Let $1 \leq i \leq m$. Let $P_0 = (\bar{x}_{0,1}, \ldots, \bar{x}_{0,m}) \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$ be a ghost point. Let*

$$t_i = \min\left\{t\,,\, |\{\hat{\pi}_i(P) \mid P \in \mathcal{V}(I) \cup P_0\}|\right\},$$

and let $\mathcal{P}_i$ be a polynomial in $\mathbb{F}_q[S, x_1, \ldots, x_i]$, where $S = \{s_1, \ldots, s_r\}$. Then $\{\mathcal{P}_i\}_{1 \leq i \leq m}$ is a set of **weak multi-dimensional general error locator polynomials** *of C if for any i*

- *$\mathcal{P}_i(S, x_1, \ldots, x_i) = x_i^{t_i} + a_{t_i-1}x_i^{t_i-1} + \cdots + a_0$, with $a_j \in \mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$, $0 \leq j \leq t_i - 1$, that is, $\mathcal{P}_i$ is a monic polynomial with degree t_i with respect to the variable x_i and its coefficients are in $\mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$;*
- *given a syndrome $\overline{\mathbf{s}} = (\bar{s}_1, \ldots \bar{s}_r) \in (\mathbb{F}_q)^r$, corresponding to an error vector of weight $\mu \leq t$, and μ error locations $(\bar{x}_{1,1}, \ldots, \bar{x}_{1,m})$, $\ldots$, $(\bar{x}_{\mu,1}, \ldots, \bar{x}_{\mu,m})$, if we evaluate the S variables at $\overline{\mathbf{s}}$ and the variables $(x_1, \ldots, x_{i-1})$ at the truncated vectors $\overline{\mathbf{x}}^j = (\bar{x}_{j,1}, \ldots, \bar{x}_{j,i-1})$ for $0 \leq j \leq \mu$, then the roots of $\mathcal{P}_i(\overline{\mathbf{s}}, \overline{\mathbf{x}}^j, x_i)$ contain:*

- *either* $\{\bar{x}_{h,i} \mid \overline{\mathbf{x}}^h = \overline{\mathbf{x}}^j,\ 0 \leq h \leq \mu\}$ *(when* $\mu < t$*),*
- *or* $\{\bar{x}_{h,i} \mid \overline{\mathbf{x}}^h = \overline{\mathbf{x}}^j,\ 1 \leq h \leq \mu\}$ *(when* $\mu = t$*),*

plus possibly some parasite solutions.

Note that the difference between $\{\bar{x}_{h,i} \mid \overline{\mathbf{x}}^h = \overline{\mathbf{x}}^j,\ 0 \leq h \leq \mu\}$ and $\{\bar{x}_{h,i} \mid \overline{\mathbf{x}}^h = \overline{\mathbf{x}}^j,\ 1 \leq h \leq \mu\}$ is that the latter set does not consider the ghost point.

Now we consider an alternative strategy to compute the error locations, using the weak multi-dimensional general error locator polynomials and some other polynomials in ideal $J_*^{C,t}$.

Since it is convenient to know in advance the error number and the error values, we provide the following definition for a general correctable linear code. Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with correction capability $t \geq 1$. Choose any parity-check matrix with entries in an appropriate extension field $\mathbb{F}_{q^M}$ of $\mathbb{F}_q$, $M \geq 1$. Its syndromes lie in $(\mathbb{F}_{q^M})^{n-k}$ and form a vector space of dimension $r = n - k$ over $\mathbb{F}_q$.

Definition 8.2.6. *Let* $\mathcal{E} \in \mathbb{F}_q[S, e]$*, where* $S = \{s_1, \ldots, s_r\}$*. Then* $\mathcal{E}$ *is a* **general error evaluator polynomial** *of* C *if*

- $\mathcal{E}(S, e) = a_t e^t + a_{t-1} e^{t-1} + \cdots + a_0$*, with* $a_j \in \mathbb{F}_q[S]$*,* $0 \leq j \leq t$*, that is,* $\mathcal{E}$ *is a polynomial with degree* t *with respect to the variable* e *and its coefficients are in* $\mathbb{F}_q[S]$*;*
- *Given a syndrome* $\overline{\mathbf{s}} = (\bar{s}_1, \ldots \bar{s}_r) \in (\mathbb{F}_{q^M})^r$ *corresponding to an error vector of weight* $\mu \leq t$ *and with* $\bar{e}_1, \ldots, \bar{e}_\mu$ *as error values, we evaluate the* S *variables at* $\overline{\mathbf{s}}$*, then the roots of* $\mathcal{E}$ *are the error values* $\bar{e}_1, \ldots, \bar{e}_\mu$ *plus* 0 *with multiplicity* $t - \mu$*.*

The importance of $\mathcal{E}$ lies in fact that the error number is μ if and only if

$$e^{t-\mu} | \mathcal{E}(\overline{\mathbf{s}}) \quad \text{and} \quad e^{(t-\mu+1)} \not| \mathcal{E}(\overline{\mathbf{s}}).$$

The ideal $J_*^{C,t} \cap \mathbb{K}[S, e_1, \ldots, e_t]$ is easily seen to be stratified, as follows. There is a bijective correspondence between correctable syndromes and correctable errors (i.e., errors of weight $\tau \leq t$) and so if we fix $1 \leq l \leq t$ and $1 \leq s \leq t - l$ we can always find l error values $e_1, \ldots, e_l$ that have s extensions at level e_{l+1}. So we can apply Proposition 4.4.3 and obtain the existence of $\mathcal{E}$.

Theorem 8.2.7. *For any affine-variety code* $C = C^\perp(I, L)$*, the general error evaluator polynomial exists.*

Proof. We apply Proposition 4.4.3 to the stratified ideal $J_*^{C,t} \cap \mathbb{K}[S, e_1, \ldots, e_t]$. It is enough to take g with $\mathbf{T}(g) = \mathsf{a}_L^L$ with $\mathcal{A} = \{e_1, \ldots, e_t\}$ and $\mathcal{S} = S$. □

Using $\mathcal{E}$, we know not only τ, but also the τ error values. In order to exploit this information, we can consider a straightforward generalisation of weak multi-dimensional general error locator polynomials (see Definition 8.2.5) where the locators are actually $\mathcal{P}_i^e \in \mathbb{F}_q[S, e, x_1, \ldots, x_{i-1}]$. We do not give a long definition for these, since we think it is obvious.
We consider again Example 8.2.3 to show two alternative strategies.

Example 8.2.8. Let us consider the Hermitian code $C = C^{\perp}(I, L)$ from the curve $y^2 + y = x^3$ over $\mathbb{F}_4$ and with defining monomials $\{1, x, y, x^2, xy\}$, as in the Example 8.2.3. The reduced Gröbner basis G of $J_*^{C,t}$ with respect to lex with $s_1 < s_2 < s_3 < s_4 < s_5 < e_2 < e_1 < x_2 < y_2 < x_1 < y_1$ has 33 elements and the general error evaluator polynomial $\mathcal{E}$ is

$$\begin{aligned}\mathcal{E} =& \mathbf{e}^2 + \mathbf{e}s_1 + s_4^3 s_3^2 + s_4^3 s_3 s_1 + s_4^3 s_2^3 s_1^2 + s_4^3 s_1^2 + s_4^2 s_3^2 s_2^2 s_1^2 + s_4^2 s_3 s_2^2 s_1^3 + s_4 s_3^2 s_2 s_1 + \\ & s_4 s_3 s_2 s_1^2 + s_4 s_2 s_1^3 + s_4 s_2 + s_3^2 s_2^3 s_1^3 + s_3^2 + s_3 s_2^3 s_1 + s_3 s_1 + s_2^3 s_1^2.\end{aligned}$$

In G there are also these polynomials:

$$\mathcal{P}_x^e = \mathbf{x}^2 + \mathbf{x} s_4 s_2^2 + \mathbf{e}\, a_x + b_x \text{ and } g_x = \mathbf{x}_1 + \mathbf{x}_2 + c_x,$$

where $a_x, b_x, c_x \in \mathbb{F}_4[s_1, s_2, s_3, s_4, s_5]$ (see Appendix for the full polynomials). Now we change the lex ordering to $s_1 < \cdots < s_5 < e_2 < e_1 < y_2 < x_2 < y_1 < x_1$. In the new Gröbner basis we have other two polynomials $\mathcal{P}_y^e$ and g_y.

$$\mathcal{P}_y^e = \mathbf{y}^2 + \mathbf{y}(s_4 s_3 s_2 + s_2^3 + 1) + \mathbf{e}\, a_y + b_y \text{ and } g_y = \mathbf{y_1} + \mathbf{y_2} + c_y,$$

where $a_y, b_y, c_y \in \mathbb{F}_4[s_1, s_2, s_3, s_4, s_5]$ (see Appendix for the full polynomials). We can decode as follows. First we evaluate $\mathcal{E}(\bar{\mathbf{s}})$ and we find two error values $\mathbf{e_1}, \mathbf{e_2}$ (when $\tau = 1$, one is zero).

- If the syndrome corresponds to two errors, then the roots of $\mathcal{P}_x^e(\mathbf{s}, \mathbf{e_2}, x)$ are the first components of error locations,
- else if $\bar{\mathbf{s}}$ corresponds to one error, we specialize $g_x(s, e, x_1, x_2)$ in $(\mathbf{s}, \mathbf{e_2}, 1)$, where 1 is the ghost component, and again the root of $g_x(\mathbf{s}, \mathbf{e_2}, \mathbf{1}, x_2)$ is the first component of the error location.

Similarly we use $\mathcal{P}_y^e$ and g_y to find the second location components. Let us explain in detail the above-mentioned decoding with the help of the three cases of Example 8.2.3.

- $\overline{\mathbf{s}} = (0,1,1,1,0)$ is the syndrome vector corresponding to the error vector $(0,0,0,0,0,1,1,0)$. Evaluating $\mathcal{E}$ in $\overline{\mathbf{s}}$ we obtain: $\mathcal{E}(\overline{\mathbf{s}}) = e^2+1$, so two errors have occurred and their values is 1. In order to find the error positions we evaluate $\mathcal{P}_x^e$ and $\mathcal{P}_y^e$ in $(\mathbf{s},1)$ and we obtain

$$\mathcal{P}_x^e(\overline{\mathbf{s}},1) = x^2+x+1 = (x-\alpha)(x-(\alpha+1))$$
$$\mathcal{P}_y^e(\overline{\mathbf{s}},1) = y^2+y+1 = (y-\alpha)(y-(\alpha+1)).$$

  The system $\mathcal{P}_x^e(\overline{\mathbf{s}},1) = \mathcal{P}_y^e(\overline{\mathbf{s}},1) = 0$ have four possible solutions: $(\alpha,\alpha),(\alpha+1,\alpha+1)$, $(\alpha+1,\alpha)$ and $(\alpha,\alpha+1)$. But only two solution pairs are admissible: $\{(\alpha+1,\alpha),(\alpha,\alpha+1)\}$ and $\{(\alpha,\alpha),(\alpha+1,\alpha+1)\}$, since both α and $\alpha+1$ must appear as first components (and as second components). We are in the same ambiguous situation as in Example 8.2.3.

- Now we consider the syndrome $\overline{\mathbf{s}} = (\alpha+1,0,\alpha,0,0)$, corresponding to a vector $(1,\alpha,0,0,0,0,0,0)$. Evaluating $\mathcal{E}$ in $\overline{\mathbf{s}}$ we obtain $\mathcal{E}(\overline{\mathbf{s}}) = (e-1)(e-\alpha)$, so two errors have occurred and their values are 1 and α. In order to find the error positions we evaluate $\mathcal{P}_x^e$ and $\mathcal{P}_y^e$ in $(\mathbf{s},1)$ (or in $(\mathbf{s},\alpha)$)

$$\mathcal{P}_x^e(\overline{\mathbf{s}},1) = f_x(\overline{\mathbf{s}},\alpha) = x^2 \text{ and } \mathcal{P}_y^e(\overline{\mathbf{s}},1) = f_y(\overline{\mathbf{s}},\alpha) = y^2+y = y(y-1).$$

  The solutions of the system $f_x(\overline{\mathbf{s}},1) = f_y(\overline{\mathbf{s}},1) = 0$ are $\{(0,0),(1,\alpha)\}$, in this case we find the correct error positions. Note that this case is an ambiguous situation in Example 8.2.3, while here it is not.

- Vector $\overline{\mathbf{s}} = (\alpha+1,\alpha+1,1,\alpha+1,1)$ is the syndrome corresponding to $(0,0,\alpha+1,0,0,0,0,0)$. We evaluate $\mathcal{E}$ and we get $\mathcal{E}(\overline{\mathbf{s}}) = e^2+(\alpha+1)e$. So only one error occurred and its value is $\alpha+1$. We evaluate g_x and g_y in $(\overline{\mathbf{s}},\alpha+1,1)$, where 1 is the first ghost component, and we have

$$g_x(\overline{\mathbf{s}},\alpha+1,1) = x_2+1 \text{ and } g_y(\overline{\mathbf{s}},\alpha+1,1) = y_2+\alpha.$$

  Therefore the error location is $(1,\alpha)$.

Now we consider another type of decoding, using $\mathcal{E}$ and taking polynomials from $\widehat{J}_{\mathcal{FL}}^{C,t}$ as in (8.1). First, we evaluate $\mathcal{E}(\overline{\mathbf{s}})$ to know the number of errors. We do not need their values. Instead, we compute the Gröbner basis of ideal $\widehat{J}_{\mathcal{FL}}^{C,\tau}$, with $1 \leq \tau \leq t$ and we collect polynomials in $\mathbb{F}_q[S,x]$ and $\mathbb{F}_q[S,y]$. For example,if two errors occur we use $s_1 < s_2 < s_3 < s_4 < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ and $\ldots s_5 < y_2 < \ldots$ to get, for $\tau = 2$,

$$\begin{aligned} f_{2,x} = \; & \mathbf{x}^2 + \mathbf{x}(s_4^2 s_1 + s_4 s_2^2 s_1^3 + s_4 s_2^2 + s_2 s_1^2) + s_5^2 s_3 + s_5 s_3 s_2 + s_4^2 s_3^3 s_2 + s_4^2 s_3^2 s_2 s_1 + s_4^2 s_3 s_2 s_1^2 \\ & + s_4^2 s_2 + s_4 s_3^3 s_1^2 + s_4 s_3^2 s_1^3 + s_4 s_3 s_1 + s_4 s_1^2 + s_3^3 s_2^2 s_1 + s_3^2 s_2^2 s_1^2 + s_3 s_2^2 s_1^3 + s_3 s_2^2 + s_2^2 s_1 \end{aligned}$$

$$\begin{aligned} f_{2,y} = \; & \mathbf{y}^2 + \mathbf{y}(s_4^3 + s_4 s_3 s_2 s_1^3 + s_4 s_3 s_2 + s_4 s_2 s_1 + s_3^2 s_1 + s_3 s_1^2 + s_2^3 s_1^3 + s_1^3 + 1) + s_5^3 + s_5 s_4^2 s_3^2 s_2 + \\ & s_5 s_3^3 s_2^2 + s_5 s_2^2 + s_4^3 s_3 s_2^3 s_1^2 + s_4^3 s_3 s_1^2 + s_4^3 s_2^2 + s_4^3 + s_4^2 s_3^3 s_2^2 s_1^2 + s_4^2 s_3^2 s_2^2 + s_4^2 s_3 s_2^2 s_1 + \\ & s_4 s_3^3 s_2 s_1 + s_4 s_3 s_2 s_1^3 + s_4 s_3 s_2 + s_3^3 + s_3 s_2^3 s_1^2 + s_2^3 s_1^3 + s_2^3 + 1 \end{aligned}$$

and for $\tau = 1$

$$f_{1,x} = \mathbf{x} + s_2 s_1^2 \quad \text{and} \quad f_{1,y} = \mathbf{y} + s_3 s_1^2.$$

The decoding with $\{f_{2,x}, f_{2,y}, f_{1,x}, f_{1,y}\}$ is obvious.
These polynomials are not the ideal polynomials yet, because again we may find parasite solutions (except with $\tau = 1$).

In the previous examples we have used some polynomials as weak multi-dimensional general error locator polynomials, as for example $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ in Example 8.2.3. It is not obvious that such polynomials exist for any (affine-variety) code. To prove this, we need to analyse in depth the structure of the zero-dimensional ideal $J_*^{C,t}$. This ideal turns out to belong to several interesting classes of zero-dimensional ideals, defined as generalizations of stratified ideals. These ideal classes are rigorously studied in Section 8.3, where it is claimed in full generality that the sought-after polynomials can be found in a suitable Gröbner basis. Section 8.4 is devoted to the proof of this claim. In Section 8.5 we will come back to the coding setting.

8.3 Results on some zero–dimensional ideals

Our aim in this section is to describe the structure of the reduced Gröbner basis for some special classes of zero-dimensional ideals which are generalizations of stratified ideals.

First we provide a generalization of the material in Section 4.4. In this section $J \subset \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1, \mathcal{T}]$ is a zero–dimensional ideal, with $\mathcal{S} = \{\mathsf{s}_1, \ldots, \mathsf{s}_N\}$, $\mathcal{A}_j = \{\mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,m}\}$, $j = 1, \ldots, L$, $\mathcal{T} = \{\mathsf{t}_1, \ldots, \mathsf{t}_K\}$. We fix a block order $<$ on $\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1, \mathcal{T}]$, with $\mathcal{S} < \mathcal{A}_L < \cdots < \mathcal{A}_1 < \mathcal{T}$, such that within $\mathbb{A}_j$ we use lex with $\mathsf{a}_{j,1} < \mathsf{a}_{j,2} < \cdots < \mathsf{a}_{j,m}$ (for any j). Let $\mathbb{A}$ and $\mathbb{A}_{j,i}$ denote the affine spaces $\mathbb{A} = \mathbb{K}^{N+mL+K}$ and $\mathbb{A}_{j,i} = \mathbb{K}^{N+m(L-j)+i}$.

With the usual notation for the elimination ideals, we want to partition $\mathcal{V}(J_{\mathcal{S}})$ according to the number of extensions in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{L,1}})$, similarly to what was done in Subsection 4.4.1 in the one-variable case, that is, when $m = 1$. The additional complication here is that the a variables are not L any more, but rather they are collected

into L blocks, each block having m variables. Since we order the a variables first according to their block (block $\mathcal{A}_L$ is the least) and then within the block from the least to the greatest, their first index denotes the block and their second index denotes their position within the block itself. So, the least a variable is $\mathsf{a}_{L,1}$ and the greatest is $\mathsf{a}_{1,m}$.
The members of the partition of $\mathcal{V}(J_{\mathcal{S}})$ will be called $\{\Sigma_l^{L,1}\}$ (similarly to the previously defined Σ_l^L). The maximum number of extensions will be called $\eta(L,1)$ (compare with $\lambda(L)$).

Remark 8.3.1. It is essential to count the number of extensions in $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{L,1}})$ discarding their multiplicities. In the definition of a stratified ideal we required radicality, so in that case multiplicities did not arise. However, in our following multi-dimensional generalisations of results and definitions from Subsection 4.4.1-4.4.3, we must drop radicality and so we have to be very careful when handling multiplicities.

In the general case, if we consider block j and variable $\mathsf{a}_{j,i}$, we partition the variety $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i}})$ into subsets $\{\Sigma_l^{j,i+1}\}$ according to the number of extensions to $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i},\mathsf{a}_{j,i+1}})$, that is, adding the next variable $\mathsf{a}_{j,i+1}$. The maximum number of extensions will be called $\eta(j,i+1)$. We meet a special case when we consider the last variable in a block (i.e., $i=m$), since in that case we extend from $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,m}})$ to $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j-1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,m},\mathsf{a}_{j-1,1}})$. However, no confusion will arise if we follow our convention of naming the partition members according to the *added* variable, so they are called $\{\Sigma_l^{j-1,1}\}$ in this case, even if their union is V$=\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j-1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,m}})$. Coherently, $\eta(j-1,1)$ denotes the maximum number of extensions for points in V.

A formal description of the above discussion goes as follows, where l,j and m are integers such that $l\geq 1$, $1\leq j\leq L$ and $1\leq i\leq m$:

$$
\begin{aligned}
\Sigma_l^{L,1} =&\{(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N)\in\mathcal{V}(J_{\mathcal{S}}) \mid \exists \text{ exactly } l \text{ distinct values } \bar{\mathsf{a}}_{L,1}^{(1)},\ldots,\bar{\mathsf{a}}_{L,1}^{(l)}\\
&\text{s.t. } (\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_{L,1}^{(\ell)})\in\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{L,1}}) \text{ with } 1\leq\ell\leq l\},\\
\Sigma_l^{j,1} =&\big\{(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_{L,1},\ldots,\bar{\mathsf{a}}_{L,m},\ldots,\bar{\mathsf{a}}_{j+1,1},\ldots,\bar{\mathsf{a}}_{j+1,m})\in\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}}) \mid\\
&\exists \text{ exactly } l \text{ distinct values } \bar{\mathsf{a}}_{j,1}^{(1)},\ldots,\bar{\mathsf{a}}_{j,1}^{(l)} \text{ s.t. for any } \ 1\leq\ell\leq l\\
&(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_{L,1},\ldots,\bar{\mathsf{a}}_{L,m},\ldots,\bar{\mathsf{a}}_{j+1,1},\ldots,\bar{\mathsf{a}}_{j+1,m},\bar{\mathsf{a}}_{j,1}^{(\ell)})\in\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1}})\big\}\\
&j=1,\ldots,L-2,\\
\Sigma_l^{j,i} =&\big\{(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_{L,1},\ldots,\bar{\mathsf{a}}_{L,m},\ldots,\bar{\mathsf{a}}_{j+1,1},\ldots,\bar{\mathsf{a}}_{j+1,m},\bar{\mathsf{a}}_{j,1},\ldots,\bar{\mathsf{a}}_{j,i-1}) \text{ in}\\
&\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1}}) \mid \exists \text{ exactly } l \text{ distinct values } \bar{\mathsf{a}}_{j,i}^{(1)},\ldots,\bar{\mathsf{a}}_{j,i}^{(l)} \text{ s.t.}\\
&(\bar{\mathsf{s}}_1,\ldots,\bar{\mathsf{s}}_N,\bar{\mathsf{a}}_{L,1},\ldots,\bar{\mathsf{a}}_{L,m},\ldots,\bar{\mathsf{a}}_{j+1,1},\ldots,\bar{\mathsf{a}}_{j+1,m},\bar{\mathsf{a}}_{j,1},\ldots,\bar{\mathsf{a}}_{j,i-1},\bar{\mathsf{a}}_{j,i}^{(\ell)}) \text{ is in}\\
&\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i}})\, 1\leq\ell\leq l\big\},\quad i=2,\ldots,m,\ j=1,\ldots,L-1.
\end{aligned}
$$

The maximum number of extensions at any level, which is $\eta(j,i)$, plays an important role for our approach and therefore deserves a precise definition. Before defining it, we need an elementary result.

Fact 8.3.2. *Given J, there is a set of natural numbers $\{\eta(j,i)\}_{\substack{1\leq j\leq L,\\ 1\leq i\leq m}}$ such that*

i) $\mathcal{V}(J_{\mathcal{S}}) = \sqcup_{l=1}^{\eta(L,1)}\Sigma_l^{L,1}$;

ii) $\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{L,1},\ldots,\mathsf{a}_{L,i}}) = \sqcup_{l=1}^{\eta(L,i+1)}\Sigma_l^{L,i+1}$, $i = 1,\ldots,m-1$;

iii) $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L}) = \sqcup_{l=1}^{\eta(L-1,1)}\Sigma_l^{L-1,1}$;

iv) $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}}) = \sqcup_{l=1}^{\eta(j,1)}\Sigma_l^{j,1}$, $j = 1,\ldots,L-2$;

v) $\mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i}}) = \sqcup_{l=1}^{\eta(j,i+1)}\Sigma_l^{j,i+1}$, $i = 1,\ldots,m-1, j = 1,\ldots,L-1$;

vi) $\Sigma_{\eta(j,i)}^{j,i} \neq \emptyset$, $\forall i = 1,\ldots,m$, $\forall j = 1,\ldots,L$.

Proof. Since I is a zero-dimensional ideal, $\mathcal{V}(I)$ is finite and so any variety projection $V = \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1}})$ has a finite number of points. Obviously V is the union of the corresponding $\Sigma_l^{j,i}$, which means that there can be only a finite number of non-empty $\Sigma_l^{j,i}$ and so we use the notation $\eta(j,i)$ to denote the largest l such that $\Sigma_l^{j,i}$ is non-empty. □

Definition 8.3.3. *The* **level function** *of J (with respect to the $\mathcal{A}_L,\ldots,\mathcal{A}_1$ variables) is the function $\eta : \{1\ldots L\}\times\{1\ldots m\}\to\mathbb{N}$ satisfying Fact 8.3.2.*

We want now to generalize our previous definition of stratified ideals (Definition 4.4.1) to the multivariate case, but dropping radicality (see Remark 8.3.1). It turns out that there are two ways of doing it: we have a weaker notion in the next definition and two stronger notions in the subsequent definition.

Definition 8.3.4. *Let J be a zero-dimensional ideal with the above notation. We say that J is a* **weakly stratified ideal** *if*

$$\Sigma_l^{j,i} \neq \emptyset \qquad \text{for } 1 \leq l \leq \eta(j,i),\ 1 \leq i \leq m,\ 1 \leq j \leq L.$$

Being weakly stratified means that when considering the elimination ideal at level (j,i) (block j and variable $\mathsf{a}_{j,i}$) if there is a variety point with $l \geq 2$ extensions then there is another point with $l-1$ extensions.

The following definition of multi-stratified ideal is given at variable-block level, rather than at a single-variable level. It contains two conditions: there is at least one point with exactly j extensions and there are no "gaps" in the number of extensions

(for any integer $1 \leq l \leq j$ there is at least one point with l extensions). So it is exactly the multi-dimensional analogue of the definition of stratified ideals, except that we drop the radicality. Unfortunately, this straightforward generalization does not guarantee the existence of polynomials playing the role of "ideal" locators, and so in the same definition we provide an even stronger notion "strongly multi-stratified ideal".

Definition 8.3.5. *Let J be a zero-dimensional ideal with the above notation. Let us consider the natural projections*

$$\begin{aligned}
&\pi_L : \quad \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L}) \quad \longrightarrow \mathcal{V}(J_{\mathcal{S}}) \\
&\pi_j : \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathcal{A}_j}) \longrightarrow \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}}),\ j = 1,\ldots,L-1 \\
&\rho_j : \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathcal{A}_j}) \longrightarrow \mathcal{V}(J_{\mathcal{A}_j}),\ j = 1,\ldots,L
\end{aligned}$$

Ideal J is a **multi-stratified ideal** *(in the $\mathcal{A}_L,\ldots,\mathcal{A}_1$ variables) if*

1) *for any $1 \leq j \leq L-1$ and for any $P \in \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}})$ we have that $|\pi_j^{-1}(\{P\})| \leq j$. Moreover, for any $\bar{s} \in \mathcal{V}(J_{\mathcal{S}})$ we have that $|\pi_L^{-1}(\{\bar{s}\})| \leq L$;*

2) *for any $1 \leq j \leq L-1$ there is $Q \in \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}})$ s.t. $|\pi_j^{-1}(\{Q\})| = j$. Moreover, there is $\bar{s} \in \mathcal{V}(J_{\mathcal{S}})$ s.t. $|\pi_L^{-1}(\{\bar{s}\})| = L$.*

For any $1 \leq j \leq L$, let $Z_j = \rho_j(\mathcal{V}(J))$. We say that ideal J is a **strongly multi-stratified ideal** *(in the $\mathcal{A}_L,\ldots,\mathcal{A}_1$ variables) if 1) holds and*

3) *for any $1 \leq j \leq L-1$, for any $T \subset Z_j$ s.t. $1 \leq |T| \leq j$ there is a $Q \in \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}})$ s.t. $\rho_j(\pi_j^{-1}(\{Q\})) = T$. Moreover, for any $T \subset Z_L$ s.t. $1 \leq |T| \leq L$ there is an $\bar{s} \in \mathcal{V}(J_{\mathcal{S}})$ s.t. $\rho_L(\pi_L^{-1}(\{\bar{s}\})) = T$.*

Again, in the previous definition, we do not count multiplicities.

Remark 8.3.6. For any zero-dimensional ideal J with the above notation, let $Z = Z_1$. Once $\rho_{j'}(\mathcal{V}(J)) = \rho_j(\mathcal{V}(J))$ for any $1 \leq j, j' \leq L$, we obviously have $\rho_j(\pi_L^{-1}(\{\bar{s}\})) \subset Z$. Assuming this, 1) and 3) could be replaced by saying that there is a bijection between the sets of $\rho_j(\pi_L^{-1}(\{Q\}))$ and all (non-empty) subsets of Z with up to j elements (and a similar condition at level L).

We note the following obvious fact.

Fact 8.3.7. *Let $m \geq 1$. If J is a strongly multi-stratified ideal then J is a multi-stratified ideal.*

Let $m = 1$. If J is a multi-stratified ideal then J is a weakly stratified ideal. If J is radical, then J is a multi-stratified ideal if and only if J is a stratified ideal.

The next two examples clarify (in the case $m = 1$) the notions of multi-stratified ideals and of weakly stratified ideals.

Example 8.3.8. Let $\mathcal{S} = \{\mathsf{s}_1\}$, $\mathcal{A}_1 = \{\mathsf{a}_{1,1}\}$, $\mathcal{A}_2 = \{\mathsf{a}_{2,1}\}$, so that $m = 1$, and $\mathcal{T} = \{\mathsf{t}_1\}$. Let $J = \mathcal{I}(Z) \subset \mathbb{C}[\mathsf{s}_1, \mathsf{a}_{2,1}, \mathsf{a}_{1,1}, \mathsf{t}_1]$ with $Z = \{(0,0,0,0),\ (0,1,1,0),\ (0,2,2,0)\}$. The order $<$ is $s_1 < a_{2,1} < a_{1,1} < t_1$ and the varieties are

$$\mathcal{V}(J_{\mathcal{S}}) = \{0\}, \quad \mathcal{V}(J_{\mathcal{S},\mathsf{a}_{2,1}}) = \{(0,0),(0,1),(0,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{2,1},\mathsf{a}_{1,1}}) = \{(0,0,0),(0,1,1),(0,2,2)\}.$$

Let us consider the projection $\pi_2 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathsf{a}_{2,1}}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}})$. Then $|\pi_2^{-1}(\{0\})| = 3$. We have $\sum_3^{2,1} = \{0\}$ and $\sum_1^{2,1} = \emptyset$, $\sum_2^{2,1} = \emptyset$. So $\eta(2,1) = 3$ and J is not a weakly stratified ideal (neither a stratified ideal).

Example 8.3.9. Let $\mathcal{S} = \{\mathsf{s}_1\}$, $\mathcal{A}_1 = \{\mathsf{a}_{1,1}\}$, $\mathcal{A}_2 = \{\mathsf{a}_{2,1}\}$, $\mathcal{A}_3 = \{\mathsf{a}_{3,1}\}$, $\mathcal{T} = \{\mathsf{t}_1\}$ so that $m = 1$. Let $J = \mathcal{I}(Z) \subset \mathbb{C}[\mathsf{s}_1, \mathsf{a}_{3,1}, \mathsf{a}_{2,1}, \mathsf{a}_{1,1}, \mathsf{t}_1]$ with $Z = \{(0,1,0,0,0,0),\ (0,2,1,1,2),\ (2,2,2,0,0)\}$. The order $<$ is $s_1 < a_{3,1} < a_{2,1} < a_{1,1} < t_1$ and the varieties are

$$\mathcal{V}(J_{\mathcal{S}}) = \{0,2\}, \quad \mathcal{V}(J_{\mathcal{S},\mathsf{a}_{3,1}}) = \{(0,1),(0,2),(2,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{3,1},\mathsf{a}_{2,1}}) = \{(0,1,0),(0,2,1),(2,2,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},\mathsf{a}_{3,1},\mathsf{a}_{2,1},\mathsf{a}_{1,1}}) = \{(0,1,0,0),(0,2,1,1),(2,2,2,0)\}.$$

Let us consider the projection $\pi_3 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathsf{a}_{3,1}}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}})$. Then $|\pi_3^{-1}(\{0\})| = 2$ and $|\pi_3^{-1}(\{2\})| = 1$, so $\sum_2^{3,1} = \{0\}$, $\sum_1^{3,1} = \{2\}$ and $\eta(3,1) = 2$, but $\sum_3^{3,1} = \emptyset$. Similarly, $\eta(2,1) = \eta(1,1) = 1$. So J is a weakly stratified ideal that is not multi-stratified (and not stratified).

However, if $m \geq 2$, a weakly stratified ideal is not necessarily a multi-stratified ideal and, viceversa, a multi-stratified ideal is not necessarily a weakly stratified ideal, as shown in the following example.

Example 8.3.10. Let $\mathcal{S} = \{\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3\}$, $\mathcal{A}_1 = \{\mathsf{a}_{1,1}, \mathsf{a}_{1,2}\}$, $\mathcal{A}_2 = \{\mathsf{a}_{2,1}, \mathsf{a}_{2,2}\}$, $\mathcal{A}_3 = \{\mathsf{a}_{3,1}, \mathsf{a}_{3,2}\}$, $\mathcal{T} = \{\mathsf{t}_1\}$ so that $m = 2$. Let $J = \mathcal{I}(Z) \subset \mathbb{C}[\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, \mathsf{a}_{3,1}, \mathsf{a}_{3,2}, \mathsf{a}_{2,1}, \mathsf{a}_{2,2}, \mathsf{a}_{1,1}, \mathsf{a}_{1,2}, \mathsf{t}_1, \mathsf{t}_2]$, with $Z = \{(0,0,1,1,\ 1,1,1,3,1,1,1),\ (0,0,1,1,2,1,3,1,2,1,1),\ (0,0,1,1,3,0,0,2,1,1,2),$ $(1,1,2,2,1,2,1,0,0,0,1),(1,1,2,0,1,1,1,0,1,2,1),(1,1,2,0,1,1,0,1,0,0,1),(2,3,0,3,3,1,$ $0,1,1,1,2)\}$. The order $<$ is $s_1 < s_2 < s_3 < a_{3,1} < a_{3,2} < a_{2,1} < a_{2,2} < a_{1,1} < a_{1,2} < t_1$ and the varieties are

$$\begin{aligned}
\mathcal{V}(J_{\mathcal{S}}) = &\ \{(0,0,1),(1,1,2),(2,3,0)\},\\
\mathcal{V}(J_{\mathcal{S},\mathcal{A}_3}) = &\ \{(0,0,1,1,1),(0,0,1,1,2),(0,0,1,1,3),(1,1,2,2,1),(1,1,2,0,1),(2,3,0,3,3)\},\\
\mathcal{V}(J_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2}) = &\ \{(0,0,1,1,1,1,1),(0,0,1,1,2,1,2),(0,0,1,1,3,0,0),(1,1,2,2,1,2,1),(1,1,2,0,1,1,1),\\
&\ (1,1,2,0,1,1,0),(2,3,0,3,3,1,0)\},\\
\mathcal{V}(J_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2,\mathcal{A}_1}) = &\ \{(0,0,1,1,1,1,1,3,1),(0,0,1,1,2,1,2,1,2),(0,0,1,1,3,0,0,2,1),(1,1,2,2,1,2,1,0,0),\\
&\ (1,1,2,0,1,1,1,0,1),(1,1,2,0,1,1,0,1,0),(2,3,0,3,3,1,0,1,1)\}.
\end{aligned}$$

Let us consider the projection $\pi_3 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}})$. Then $|\pi_3^{-1}(\{(0,0,1)\})| = 3$, $|\pi_3^{-1}(\{(1,1,2)\})| = 2$ and $|\pi_3^{-1}(\{(2,3,0)\})| = 1$.
Similarly, if we consider $\pi_2 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3})$, then $|\pi_2^{-1}(\{(1,1,2,0,1)\})|$ is equal to 2 and for other $P \in \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3})$ we have that $|\pi_2^{-1}(\{P\})| = 1$.
Finally, if we consider $\pi_1 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2,\mathcal{A}_1}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2})$, then for any $P \in \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathcal{A}_3,\mathcal{A}_2})$ we have that $|\pi_1^{-1}(\{P\})| = 1$ and so J is multi-stratified. It is easy to see that J is not weakly stratified. In fact, if we consider the projection $\pi_{3,1} : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathsf{a}_{3,1},\mathsf{a}_{3,2}}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathsf{a}_{3,1}})$ then

$$\pi_{3,2}^{-1}(\{(0,0,1,1)\}) = \{(0,0,1,1,1),(0,0,1,1,2),(0,0,1,1,3)\},$$
$$\pi_{3,2}^{-1}(\{(1,1,2,2)\}) = \{(1,1,2,2,1)\}, \quad \pi_{3,2}^{-1}(\{(1,1,2,0)\}) = \{(1,1,2,0,1)\}$$
$$\pi_{3,2}^{-1}(\{(2,3,0,3)\}) = \{(2,3,0,3,3)\}.$$

So $\sum_3^{3,2} = \{(0,0,1,1)\}$, but $\sum_2^{3,2} = \emptyset$.

Proposition 8.3.11. *Let J be a strongly multi-stratified ideal then J is a weakly stratified ideal.*

Proof. For any $1 \leq i \leq m$ and for any $j = 1, \ldots, L-1$, let us consider the natural projection

$$\pi_{j,i} : \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\bar{\mathsf{a}}_{j,1},\ldots,\bar{\mathsf{a}}_{j,i}}) \longrightarrow \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\bar{\mathsf{a}}_{j,1},\ldots,\bar{\mathsf{a}}_{j,i-1}})$$

We will also use ρ_j and π_j as in Definition 8.3.5.
To avoid complications, we consider only the case $2 \leq i \leq m-1$, being the modifications in the $i = 1$ and $i = m$ obvious.
The first fact that we note is that $\eta(j,i) \leq j$, because if the pre-images at block level contain at most j elements, then at variable level they cannot contain more. Let $2 \leq l \leq \eta(j,i)$ such that $\Sigma_l^{j,i} \neq \emptyset$. It is enough to show that $\Sigma_{l-1}^{j,i} \neq \emptyset$.
Let $\bar{R}, \bar{P}$ and Q such that $Q \in \Sigma_l^{j,i}$, $Q = (\bar{\mathcal{S}}, \bar{\mathcal{A}}_L, \ldots, \bar{\mathcal{A}}_{j+1}, \bar{\mathsf{a}}_{j,1}, \ldots, \bar{\mathsf{a}}_{j,i-1})$,
$\bar{P} = (\bar{\mathcal{S}}, \bar{\mathcal{A}}_L, \ldots, \bar{\mathcal{A}}_{j+1})$, $\bar{R} = (\bar{\mathsf{a}}_{j,1}, \ldots, \bar{\mathsf{a}}_{j,i-1})$, so $Q = (\bar{P}, \bar{R})$.
Then $\pi_{j,i}^{-1}(\{Q\}) = \{(Q,\lambda_1), \ldots, (Q,\lambda_l)\}$ and all λ_ℓ's are distinct.
Let $\Gamma_1, \ldots, \Gamma_l \in \mathcal{V}(J_{\mathsf{a}_{j,i+1},\ldots,\mathsf{a}_{j,m}})$ such that $(Q,\lambda_\ell,\Gamma_\ell) \in \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_j})$. The Γ_ℓ's do not have to be distinct. For any $1 \leq \ell \leq l$ at least one such Γ_ℓ must exist. We choose one Γ_ℓ for any ℓ. So $\{(Q,\lambda_1,\Gamma_1), \ldots, (Q,\lambda_l,\Gamma_l)\} \subset \pi_j^{-1}(\bar{P})$ and $\{(\bar{R},\lambda_\ell,\Gamma_\ell)\}_{1\leq\ell\leq l}$ is a subset of $\rho_j(V(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathcal{A}_j}))$. Let

$$T = \{(\bar{R},\lambda_1,\Gamma_1), \ldots, (\bar{R},\lambda_{l-1},\Gamma_{l-1})\}.$$

Then $T \subset \rho_j(V(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathcal{A}_j}))$ and $|T| = l-1 \leq \eta(j,i)-1 \leq j-1$.
Since J is strongly multi-stratified, there is $\widetilde{P} \in \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1}})$ such that

$$T = \rho_j(\pi_j^{-1}(\{\widetilde{P}\})), \text{ so } \pi_j^{-1}(\{\widetilde{P}\}) = \{(\widetilde{P},\bar{R},\lambda_1,\Gamma_1), \ldots, (\widetilde{P},\bar{R},\lambda_{l-1},\Gamma_{l-1})\}.$$

This implies that $\{(\widetilde{P},\bar{R},\lambda_1), \ldots, (\widetilde{P},\bar{R},\lambda_{l-1})\} = \pi_{j,i}^{-1}(\{(\widetilde{P},\bar{R})\})$, and so $\Sigma_{l-1}^{j,i} \neq \emptyset$, as all λ_ℓ's are distinct. □

Let $\prec_{\text{lex}}$ be the lexicographic term order such that $\mathcal{A}_L \prec_{\text{lex}} \ldots \prec_{\text{lex}} \mathcal{A}_1$ and for any $1 \leq j \leq L$ we have $a_{j,1} \prec_{\text{lex}} \ldots \prec_{\text{lex}} a_{j,m}$. Let $<_S$ be a term order on $\mathcal{S}$ and $<_{\mathcal{T}}$ a term order on $\mathcal{T}$. Let $<$ be the block order $<= (<_S, \prec_{\text{lex}}, <_{\mathcal{T}})$ (for definitions see Section 2.1). We are now assuming that J is any zero-dimensional ideal is $\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1, \mathcal{T}]$. Let $G = \text{GB}(J)$. We consider a Gröbner basis of elimination ideal $\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1] \setminus \mathbb{K}[\mathcal{S}]$ (see Section 2.3). It is well–known that the elements of $G \cap (\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1] \setminus \mathbb{K}[\mathcal{S}])$ can be collected into non-empty blocks $\{G^j\}_{1 \leq j \leq L}$, where

$$G^L = G \cap (\mathbb{K}[\mathcal{S}, \mathcal{A}_L] \setminus \mathbb{K}[\mathcal{S}])$$

and, for $1 \leq j \leq L-1$,

$$G^j = G \cap (\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathcal{A}_j] \setminus \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}]).$$

Then we denote by $G^{L,1}$, $G^{L,i}$, $G^{j,1}$ and $G^{j,i}$, $1 < j \leq L$, $1 < i \leq m$, respectively, the sets:

$$\begin{aligned}
G^{L,1} &= G \cap (\mathbb{K}[\mathcal{S}, \mathsf{a}_{L,1}] \setminus \mathbb{K}[\mathcal{S}]) \\
G^{L,i} &= G \cap (\mathbb{K}[\mathcal{S}, \mathsf{a}_{L,1}, \ldots, \mathsf{a}_{L,i}] \setminus \mathbb{K}[\mathcal{S}, \mathsf{a}_{L,1}, \ldots, \mathsf{a}_{L,i-1}]) \\
G^{j,1} &= G \cap (\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}] \setminus \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}]) \\
G^{j,i} &= G \cap (\mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}] \setminus \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}]).
\end{aligned}$$

In other words, let g be any polynomial in $G^{j,i}$. Then:

- g contains the variable $\mathsf{a}_{j,i}$,
- g does not contain any greater variable (i.e. no variables in blocks $\mathcal{A}_{j+1} \ldots \mathcal{A}_1$ and none of the remaining variables in the j-th block $\mathsf{a}_{j,i+1}, \ldots, \mathsf{a}_{j,m}$),
- g may contain lesser variables (the $\mathcal{S}$ variables, the a variables contained in blocks $L, \ldots, j-1$ and the lesser a variables in the same block: $\mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}$).

As the ideal under consideration is assumed zero-dimensional, the sets $G^{j,i}$ are non-empty. The polynomials in any $G^{j,i}$ can be grouped according to their degree δ with respect to $\mathsf{a}_{j,i}$.
For us it is essential to know the *maximum value* of δ in $G^{j,i}$, that we call

$$\zeta(j,i) \tag{8.11}$$

So we can write:

$$G^{j,i} = \sqcup_{\delta=1}^{\zeta(j,i)} G_\delta^{j,i}, \quad j = 1, \ldots, L, \ i = 1, \ldots, m, \text{ with } G_{\zeta(j,i)}^{j,i} \neq \emptyset,$$

but some $G_\delta^{j,i}$ could be empty. In this way, if $g \in G_\delta^{j,i}$ we have:

- $g \in \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}][\mathsf{a}_{j,i}] \setminus \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}]$
- $\deg_{\mathsf{a}_{j,i}}(g) = \delta$.

Note that we can view ζ as a function $\zeta : \{1 \ldots L\} \times \{1 \ldots m\} \to \mathbb{N}$, that is, as a function with exactly the same range of η.

If $g \in G_\delta^{j,i}$, then we can write uniquely g as

$$g = a_\delta \mathsf{a}_{j,i}^\delta + a_{\delta-1}\mathsf{a}_{j,i}^{\delta-1} + \cdots + a_0,$$

with $a_j \in \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}]$. and a_δ is the leading polynomial of g. We name the elements of $G_\delta^{j,i}$ according to the term order of their leading terms, *i.e.* $G_\delta^{j,i} = \{g_{j,\delta,1}^{(i)}, \ldots, g_{j,\delta,|G_\delta^{j,i}|}^{(i)}\}$, with $\mathbf{T}(g_{j,\delta,h}^{(i)}) < \mathbf{T}(g_{j,\delta,h+1}^{(i)})$ for any h.
We note the following lemma.

Lemma 8.3.12. *For any $j = 1, \ldots, L$ and $i = 1, \ldots, m$, $G_{\zeta(j,i)}^{j,i} = \{g_{j,\zeta(j,i),1}^{(i)}\}$, i.e. there exists only one polynomial in $G_{\zeta(j,i)}^{j,i}$ such that $\deg_{\mathsf{a}_{j,i}} = \zeta(j,i)$.*

Proof. From elementary properties of Gröbner bases of zero-dimensional ideals, for any variable $\mathsf{a}_{j,i}$, G must contain a polynomial g with leading term $\mathsf{a}_{j,i}^k$, for some $k \geq 1$. Note that $g \in G^{j,i}$, because variable $\mathsf{a}_{j,i}^k$ is present in g and any greater variable cannot be present. If there is a $\overline{g} \in G^{j,i}$ with $\deg_{\mathsf{a}_{j,i}} \overline{g} \geq k$, then $\mathsf{a}_{j,i} | \mathbf{T}(\overline{g})$ and so $\overline{g}$ can be removed (recall that G is reduced). As a consequence, g has the highest possible degree in $\mathsf{a}_{j,i}$, i.e. $k = \zeta(j,i)$, and so $g = g_{j,\zeta(j,i),1}^{(i)}$. □

We are ready for the main result of this section. Compare with Theorem 32 in [GS09].

Proposition 8.3.13. *Let G be a reduced Gröbner basis of a radical weakly stratified ideal J with respect to $<$ as previously described. Let $\mathcal{V}(J) \subset \mathbb{A}$. Then for any $j = 1, \ldots, L$ and $i = 1, \ldots, m$,*

$$G^{j,i} = \sqcup_{\delta=1}^{\zeta(j,i)} G_\delta^{j,i}, \text{ with}$$

1. *$\zeta(j,i) = \eta(j,i)$, i.e. ζ is the level function of J;*
2. *$G_\delta^{j,i} \neq \emptyset$ for any $1 \leq \delta \leq \zeta(j,i)$;*
3. *$G_{\zeta(j,i)}^{j,i} = \{g_{j,\zeta(j,i),1}^{(i)}\}$, i.e. there exists only one polynomial in $G_{\zeta(j,i)}^{j,i}$ such that $\deg_{\mathsf{a}_{j,i}} = \zeta(j,i)$;*
4. *we have that*
$$\mathbf{T}(g_{j,\zeta(j,i),1}^{(i)}) = \mathsf{a}_{j,i}^{\zeta(j,i)}.$$

Note that it is the radicality that ensures 1., but in later situations we will have 1. also without radicality.

In Section 8.4 we are going to prove the previous proposition using the Buchberger-Möller theorem. Note that it may be proved also using other two approaches that are [CM90, CM95, CM02b] and [FRR06, Lun10, GRS03].

8.4 Proof of Proposition 8.3.13

8.4.1 Preliminaries of proof

To prove Proposition 8.3.13 we use the Buchberger-Möller theorem:

Theorem 8.4.1 (Buchberger-Möller). *Let $H' \subset H$ be ideals in $\mathbb{K}[V_1, \ldots, V_{\mathcal{N}}]$ such that:*

(i) there is a $\mathbb{K}$-linear map $\theta : H \longmapsto \mathbb{K}$ s.t. $\ker(\theta) = H'$,

(ii) there are $\mathcal{N}$ field elements $\{\beta_k\}_{1 \leq k \leq \mathcal{N}} \subset \mathbb{K}$ s.t. $(V_k - \beta_k)H \subset H'$ for $1 \leq k \leq \mathcal{N}$, that is, $\theta((V_k - \beta_k)f) = 0$ for all $f \in H$.

Let W be a strictly ordered Gröbner basis of H relative to a term order $<$, then a Gröbner basis W' of H' w.r.t $<$ can be constructed as follows:

1. *compute $\alpha_g = \theta(g)$ for all $g \in W$.*
2. *if $\alpha_g = 0$ for all g, then $W = W'$, which happens if and only if $H = H'$ and $\theta = 0$ in $Hom_{\mathbb{K}}(H, \mathbb{K})$.*
3. *otherwise, let g^* be the least g such that $\alpha_g \neq 0$.*

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

- $W_1 = \{g \mid g < g^*\}$,
- $W_2 = \{(V_k - \beta_k)g^* \mid 1 \leq k \leq \mathcal{N}\}$,
- $W_3 = \{g - \frac{\alpha_g}{\alpha_{g^*}} g^* \mid g > g^*\}$.

Remark 8.4.2. In the proof of Theorem 8.4.1, the hypothesis (ii) is used only to prove that $W_2 \subset H'$. Therefore, Theorem 8.4.1 still holds if we replace (ii) with a much weaker hypothesis, that is,

(iii) there are $\mathcal{N}$ field elements $\{\beta_k\}_{1 \leq k \leq N} \subset \mathbb{K}$ s.t. $(V_k - \beta_k)g^* \in H'$, $1 \leq k \leq \mathcal{N}$, where g^* is as in (3).

We recall that, by Lemma 2.2.10, if G is a Gröbner basis of an ideal I with respect to a term ordering $>$ and let $g_1, g_2 \in G$ be such that $\mathbf{T}(g_1)|\mathbf{T}(g_2)$, then $G\backslash\{g_2\}$ is again a Gröbner basis of I. Therefore, any time there is a redundant basis element, we can remove it.

From the remainder of this section, we fix $1 \leq i \leq m$ and $1 \leq j \leq L$, and we extend the projection

$$\pi : \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1},\mathsf{a}_{j,i}}) \to \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1}}) \tag{8.12}$$

to

$$\pi : \overline{\mathbb{K}}^{N+(L-j)m+i} \to \overline{\mathbb{K}}^{N+(L-j)m+i-1}$$

Coherently, we consider only the variable $\mathsf{a}_{j,i}$ in the block A_j.

Remark 8.4.3. To simplify the notation in the proof, we use τ as a symbol with a special meaning, as follows. We introduce τ to single out the contribution of variable $\mathsf{a}_{j,i}$. Any non-zero element of $\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}]$ may be written as τ and we use $\approxeq$ to express this unconventional identification. For example, $\mathsf{a}_{L,1} \approxeq \tau$ and $1 \approxeq \tau$ but also $\tau\mathsf{a}_{L,1} \approxeq \tau$ and $\mathsf{a}_{L,1}\mathsf{a}_{j,i} \approxeq \tau\mathsf{a}_{j,i} \not\approxeq \tau$ and $s_1\mathsf{a}_{j,i}^2 \approxeq \tau\mathsf{a}_{j,i}^2 \approxeq \mathsf{a}_{L,2}\mathsf{a}_{j,i}^2$.

Let H be a zero-dimensional ideal in $\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}]$. Let W be its Gröbner basis. Denote with

$$\overline{W} = W \cap (\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}]\backslash\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}])$$

and $\widehat{W} = W \cap (\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}])$, so that $W = \overline{W} \sqcup \widehat{W}$. With the τ notation, we have

$$\widehat{W} \approxeq \{\tau, \ldots, \tau\} \text{ and } \overline{W} \subset \{\tau\mathsf{a}_{j,i} + \tau, \ldots, \tau\mathsf{a}_{j,i} + \tau, \tau\mathsf{a}_{j,i}^2 + \tau\mathsf{a}_{j,i} + \tau, \ldots\}.$$

In the same way we can denote

$$\overline{H} = H \cap (\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}]\backslash\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}])$$

and $\widehat{H} = H \cap (\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}])$.

Remark 8.4.4. Suppose we want to compute the ideal H' from H by adding a point $Q = (P, \overline{\mathsf{a}}_{j,i})$, with $P = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1})$. We apply Theorem 8.4.1 to compute W' from W using the point evaluation $\theta(g) = g(Q)$. In this case it is easy to see that we can take as β_i the i-th component of Q. There are two distinct cases:

1. *either* for all $g \in \widehat{W}$, $g(Q) = g(P) = 0$,

2. *or* there exists $g \in \widehat{W}$ such that $g(Q) = g(P) \neq 0$.

The first case implies $g^* \in \overline{W}$, the second case implies $g^* \in \widehat{W}$. Since these are logically distinct, we can conclude that there are only two (distinct) cases:

1. *either* for all $g \in \widehat{W}$, $g(Q) = g(P) = 0$, and this happens if and only if $g^* \in \overline{W}$,

2. *or* there exists $g \in \widehat{W}$ such that $g(Q) = g(P) \neq 0$ and this happens if and only if $g^* \in \widehat{W}$.

8.4.2 Sketch of proof

Let us consider $g = g^{(i)}_{j,\zeta(j,i),1}$ and $\Delta = \eta(j,i)$.
Let $I = J \cap (\mathbb{K}[S, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}])$. Since $\mathcal{V}(I) \subset \mathbb{A}_{j,i}$ and I is radical and zero-dimensional, by Hilbert Nullstellensatz Theorem (that is Theorem 2.2.19) $I = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\Sigma^{j,i}_1 \sqcup \ldots \sqcup \Sigma^{j,i}_\Delta)$. Since J is weakly-stratified, we will have $\Sigma^{j,i}_h \neq \emptyset$ for all $1 \leq k \leq \Delta$.
Our proof needs several steps:

- **Step** `I`.
  We consider $P_1 \in \Sigma^{j,i}_1$, $P_2 \in \Sigma^{j,i}_2$ and π as in (8.12). We are interested in the leading terms of the Gröbner basis of $\mathcal{I}(\pi^{-1}(P_1))$ and of $\mathcal{I}(\pi^{-1}(P_1) \cup \pi^{-1}(P_2))$. However, the exact knowledge of these leading terms is unnecessary and it is sufficient for us to determine their expression in the τ notation. We perform this step in Subsection 8.4.3.

- **Step** `II`.
  Generalising the previous argument, in Subsection 8.4.4 (Lemma 8.4.5) we take any $2 \leq t \leq \Delta$ and consider any point P_h in $\Sigma^{j,i}_h$ for all $1 \leq h \leq t$. We describe the leading terms of the Gröbner basis of $\mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_t))$. Since we need an induction on the number of points to prove Lemma 8.4.5, we give an intermediate lemma: Lemma 8.4.6.

- **Step** `III`.
  As the leading terms of the Gröbner basis of $\mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_\Delta))$ are already in the desired shape, in Lemma 8.4.8 we show that adding more points does not change the shape of the leading terms of the Gröbner basis, as long as the points come from some $\Sigma^{j,i}_h$ with $h \leq \Delta$.

8.4.3 First part of the proof

We use the approach of Remark 8.4.4.

- Let $P_1 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}) \in \Sigma_1^{j,i}$ and $H = \mathcal{I}(\pi^{-1}(P_1))$ be the vanishing ideal of $\pi^{-1}(P_1)$. Then $\pi^{-1}(P_1) = \{(\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i})\}$. The basis $W = \mathrm{GB}(H)$ is $W = \{s_1 - \overline{s}_1, \ldots, s_N - \overline{s}_N, \mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1} \ldots, \mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}\}$. Using our notation we have
$$\mathbf{T}(W) = \{\tau, \ldots, \tau, \mathsf{a}_{j,i}\}. \tag{8.13}$$

- We consider a point $P_2 \in \Sigma_2^{j,i}$ that, with abuse of notation[1], we write $P_2 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1})$. We can write
$$\pi^{-1}(P_2) = \begin{cases} Q_1 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(1)}) \\ Q_2 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(2)}) \end{cases}$$

  * We add the point Q_1.
  Using Theorem 8.4.1 we can build W' from W in (8.13). If $\forall g \in \widehat{W}$, $g(Q_1) = 0$, then $\pi(Q_1) \in \mathcal{V}(\widehat{H})$. But $\pi(Q_1) = P_2$ and $\mathcal{V}(\widehat{H}) = \{P_1\}$, so $P_1 = P_2$ and $|\pi^{-1}(P_2)| = 3$, which is impossible because $P_2 \in \Sigma_2^{j,i}$. Therefore, for Remark 8.4.4, $g^* \in \widehat{W}$.
  So the Gröbner basis $W' = W_1 \sqcup W_2 \sqcup W_3$, where

    - $W_1 = \{g \in \widehat{W} \mid g < g^*\}$ because $g^* \in \widehat{W}$, so we have $W_1 \approx \{\tau, \ldots, \tau\}$ and $\mathbf{T}(W_1) \approx \{\tau, \ldots, \tau\}$.
    - W_2 is composed by the following polynomials
    $$g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N)$$
    $$g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$$
    $$g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(1)})$$
    - $W_3 = \{g - \frac{g(Q_1)}{g^*(Q_1)} g^* \mid g > g^*\}$.

  We have $\mathbf{T}(W_2) \approx \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}\}$ and $\mathbf{T}(W_3) \subseteq \{\tau, \ldots, \tau, \mathsf{a}_{j,i}\}$ and $\mathsf{a}_{j,i} \in \mathbf{T}(W_3)$. With $\mathbf{T}(W_3) \subseteq \{\tau, \ldots, \tau, \mathsf{a}_{j,i}\}$ we actually mean that $\mathbf{T}(W_3)$ is a subset of a set S such that $S \approx \{\tau, \ldots, \tau, \mathsf{a}_{j,i}\}$. We will write similarly from now on without any further comment. Observe that $\mathbf{T}(W') \approx \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \mathsf{a}_{j,i}\}$. By Lemma 2.2.10, we have $\mathbf{T}(W') \approx \{\tau, \ldots, \tau, \mathsf{a}_{j,i}\}$.

  * We add the point Q_2.
  Let[2] $W := W'$ and let us use again Theorem 8.4.1. We have to find a

[1] Where we do not imply that the components of P_2 are the same as those of P_1, although we use the same symbols.

[2] With "let $W := W'$" we mean that in this proof step we remove all elements in set W and instead we insert into W all elements from W'. After that, we remove all elements from W'. We also forget the values of g^* and W_1, W_2, W_3.

polynomial $g^* \in W$ such that $g^*(Q_2) \neq 0$. Of course $g^* \notin \widehat{W}$, because $\pi(Q_1) = \pi(Q_2) = P_2$. Thus $g^* \in \overline{W}$ and $g^* = \mathsf{a}_{j,i} + \tau$. W' is formed by $W' = W_1 \sqcup W_2 \sqcup W_3$, where

- $W_1 \approxeq \{\tau, \ldots, \tau\}$,
- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$, so
  $\mathbf{T}(W_{2,1}) \approxeq \{\tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}\}$.
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}^{(2)}_{j,i})\} \implies \mathbf{T}(W_{2,2}) = \{\mathsf{a}^2_{j,i}\}$.
- $W_3 = \emptyset$.

So

$$\mathbf{T}(W') = \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \mathsf{a}^2_{j,i}\} \tag{8.14}$$

8.4.4 Second part of proof

If $\Delta \leq 2$, we have finished our proof. Otherwise, i.e. $\Delta \geq 3$, we want to prove, using induction on t with $1 \leq t \leq \Delta$, the following lemma.

Lemma 8.4.5. *The Gröbner basis W of $H = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_t))$, where $1 \leq t \leq \Delta$ and P_h is any point in $\Sigma^{j,i}_h$ for $1 \leq h \leq t$, is such that*

$$\mathbf{T}(W) \approxeq \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}^{t-1}_{j,i}, \ldots, \tau\mathsf{a}^{t-1}_{j,i}, \mathsf{a}^t_{j,i}\}. \tag{8.15}$$

Proof. The Gröbner basis with $t = 1$ and $t = 2$ were just shown in (8.13) and (8.14) respectively.
By induction we suppose to have $t-1$ points $\{P_1, \ldots, P_{t-1}\}$ and to have a Gröbner basis W such that:

$$\mathbf{T}(W) \approxeq \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}^{t-2}_{j,i}, \ldots, \tau\mathsf{a}^{t-2}_{j,i}, \mathsf{a}^{t-1}_{j,i}\} \tag{8.16}$$

Now we can prove the t-th step. In order to do it, we prove the following lemma, with its long proof between horizontal lines.

Lemma 8.4.6. *Let $3 \leq t \leq \Delta$ and $P_t \in \Sigma^{j,i}_t$ with $\pi^{-1}(P_t) = \{Q_1, \ldots, Q_t\}$. For any $1 \leq u \leq t-1$, let H^u be the vanishing ideal*

$$H^u = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_{t-1}) \cup \{Q_1, \ldots, Q_u\}) \text{ and}$$

$$H^0 = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_{t-1})).$$

Let W^u be its reduced Gröbner basis. Then

$$\mathbf{T}(W^u) \text{ has the same structure as } \mathbf{T}(W) \text{ in (8.16).}$$

Proof. Let $P_t = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1})$. Since $P_t \in \Sigma_t^{j,i}$, then

$$\pi^{-1}(P_t) = \begin{cases} Q_1 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(1)}) \\ Q_2 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(2)}) \\ \quad \vdots \\ Q_t = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(t)}) \end{cases}$$

We prove the lemma by induction on u.

(a) We know that W^0 is as in (8.16). We add point Q_1 to H^0.
Using Theorem 8.4.1 we can build W^1 from W^0 as usual. We adopt the "W, W'" notation. If $\forall g \in \widehat{W}$, $g(Q_1) = 0$, then $\pi(Q_1) \in \mathcal{V}(\widehat{H})$. But $\pi(Q_1) = P_t$ and $\mathcal{V}(\widehat{H}) = \{P_1, \ldots, P_{t-1}\}$, so $P_t = P_k$ for some $1 \leq k \leq t-1$, and $|\pi^{-1}(P_k)| = k+1$ which is impossible because $P_k \in \Sigma_k^{j,i}$. Therefore, for Remark 8.4.4, $g^* \in \widehat{W}$.
So the Gröbner basis W' is formed by the union of these sets:

- $W_1 = \{g \in \widehat{W} \mid g < g^*\}$. Since $g^* \in \widehat{W}$ then $\mathbf{T}(W_1) = \{\tau, \ldots, \tau\}$,
- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$,
  so $\mathbf{T}(W_{2,1}) = \{\tau, \ldots, \tau\}$.
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(1)})\} \implies \mathbf{T}(W_{2,2}) = \{\tau \mathsf{a}_{j,i}\}$.
- $W_3 = \{g - \frac{g(Q_1)}{g^*(Q_1)} g^* \mid g > g^*\}$ and so the leading terms of W_3 are those in $\mathbf{T}(W)$, except possibly for τ.

Therefore $W^1 = W'$ has the same structure of $W^0 = W$ in (8.16) (because $\tau \mathsf{a}_{j,i}$ is already present in (8.16)).

(b) We add the point Q_2 to H^1 and we compute W^2.
Let $W := W'$ and we use again Theorem 8.4.1.
We find $g^* \in W$ such that $g^*(Q_2) \neq 0$. We are sure that $g^* \notin \widehat{G}$, because $\pi(Q_1) = \pi(Q_2) = P_t$, and so $g^* \in \overline{G}$. We can claim:
Claim: $\mathbf{T}(g^*) \approxeq \tau \mathsf{a}_{j,i}$.

Proof. The Gianni-Kalkbrener theorem (2.3.3) says that there exists a polynomial $g \in \overline{W}$ such that

$$g(P_t, \mathsf{a}_{j,i}) = g(\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \mathsf{a}_{j,i}) \neq 0 \text{ in } \mathbb{K}[\mathsf{a}_{j,i}]$$

and the solutions of $g(P_t, \mathsf{a}_{j,i})$ are exactly the extensions of P_t. In $\mathcal{V}(H)$ we have only one extension of P_t (which is Q_1), so the degree of g w.r.t. $\mathsf{a}_{j,i}$ must be 1 and so $g \approxeq \tau \mathsf{a}_{j,i} + \tau$.
Let g be the smallest polynomial of this kind. We have that $g^* = g$, because $g(Q_1) = 0$, $g(Q_2) \neq 0$ and all smaller polynomials vanish at Q_2. □

So W' is the union of

- $W_1 = \{g \in \widehat{W} \mid g < g^*\}$.
  Since $g^* = \tau \mathsf{a}_{j,i} + \tau$ then $\mathbf{T}(W_1) = \{\tau, \ldots, \tau\}$ or $\mathbf{T}(W_1) = \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}\}$,
- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})\}$,
  so $\mathbf{T}(W_{2,1}) = \{\tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}\}$. $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}^{(2)}_{j,i})\} \implies \mathbf{T}(W_{2,2}) = \{\tau\mathsf{a}^2_{j,i}\}$.
- $W_3 = \{g - \frac{g(Q_2)}{g^*(Q_2)} g^* \mid g > g^*\}$ so the leading terms of W_3 are those in $\mathbf{T}(W)$, except possibly for τ and $\tau\mathsf{a}_{j,i}$.

If $t = 3$, we have that $\mathsf{a}^2_{j,i} \in \mathbf{T}(W)$, and so any leading term $\tau\mathsf{a}^2_{j,i}$ can be removed (by Lemma 2.2.10) and we obtain again that the structure of $W' = W^2$ is as in (8.16). Otherwise ($t \geq 4$), the leading term $\tau\mathsf{a}^2_{j,i}$ remains and we still have the structure of (8.16).

(*c*) We proceed inductively on u until we are left to add the point Q_{t-1}.

(*d*) We add Q_{t-1}.
In this case $H = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_{t-1}) \cup \{Q_1, \ldots, Q_{t-2}\})$ and W^{t-2} has (by induction on u) the structure of (8.16). Let $W = W^{t-2}$ and $W' = W^{t-1}$. We apply Theorem 8.4.1.
We have to find $g^* \in W$ such that $g^*(Q_{t-1}) \neq 0$. Exactly as before, $g^* \notin \widehat{W}$. We know that $\mathbf{T}(g^*) \approxeq \tau\mathsf{a}^{t-2}_{j,i}$. To prove it we might use the Gianni-Kalkbrener theorem repeating the reasoning of our Claim on page 123.

So W' is the union of the following sets:

- $W_1 = \{g \in W \mid g < g^*\}$. Since $\mathbf{T}(g^*) \approxeq \tau\mathsf{a}^{t-2}_{j,i}$,
  $\mathbf{T}(W_1) = \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}^{t-3}_{j,i}, \ldots, \tau\mathsf{a}^{t-3}_{j,i}\}$ or possibly also $\tau\mathsf{a}^{t-2}_{j,i} \in \mathbf{T}(W_1)$,
- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})\}$
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}^{(r+1)}_{j,i})\}$
- $W_3 = \{g - \frac{g(Q_{r+1})}{g^*(Q_{r+1})} g^* \mid g > g^*\}$.

Since $g^* = \tau\mathsf{a}^{t-2}_{j,i} + \ldots$, we have $\mathbf{T}(W_{2,1}) = \{\tau\mathsf{a}^{t-2}_{j,i}, \ldots, \tau\mathsf{a}^{t-2}_{j,i}\}$ and $\mathbf{T}(W_{2,2}) = \{\tau\mathsf{a}^{t-1}_{j,i}\}$.
But in the Gröbner basis W in (8.16) there exists a polynomial $\overline{g}$ such that $\mathbf{T}(\overline{g}) = \mathsf{a}^{t-1}_{j,i}$. So $\mathbf{T}(\overline{g}) | \tau\mathsf{a}^{t-1}_{j,i}$ and we can remove the new term. Hence $\mathbf{T}(W')$ does not change and it remains as in (8.16).

Lemma 8.4.6 is proved. □

Now we know $\mathbf{T}(W^{t-1})$, which are the leading terms for the basis of

$$H = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_{t-1}) \cup \{Q_1, \ldots, Q_{t-1}\}).$$

We can add the point Q_t and we use our "W, W'" notation. Using Gianni-Kalkbrener's theorem we may prove as usual that $\mathbf{T}(g^*) = \mathsf{a}_{j,i}^{t-1}$. So the leading terms of

$$g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$$

are all of the type $\tau\mathsf{a}_{j,i}^{t-1}$, while $g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(t)}) = \mathsf{a}_{j,i}^t + \ldots$, so its leading term is $\mathsf{a}_{j,i}^t$. The new leading terms are $\{\tau\mathsf{a}_{j,i}^{t-1}, \ldots, \tau\mathsf{a}_{j,i}^{t-1}, \mathsf{a}_{j,i}^t\}$. Therefore, by Lemma 2.2.10, the structure of W' becomes the same as in (8.15), because there are no other new terms, since $\{g > g^*\} = \emptyset$.
This concludes the proof of Lemma 8.4.5. □

Corollary 8.4.7. *With the above notation, if $H = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_\Delta))$, then*

$$\mathbf{T}(W) \approxeq \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}^{\Delta-1}, \ldots, \tau\mathsf{a}_{j,i}^{\Delta-1}, \mathsf{a}_{j,i}^{\Delta}\} \tag{8.17}$$

Proof. Apply Lemma 8.4.5 with $t = \Delta$. □

8.4.5 Third part of the proof

Lemma 8.4.8. *Let $\mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_\Delta)) \supset H \supset J$ be a radical zero-dimensional ideal. Suppose that the leading terms of its reduced Gröbner basis satisfy (8.17). Let $\dot{P}_h \in \Sigma_h^{j,i}$, $1 \leq h \leq \Delta$ and let $H' = \mathcal{I}(\mathcal{V}(H) \cup \pi^{-1}(\dot{P}_h))$.*
Then $\mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_\Delta)) \supset H \supset H' \supset J$ and the leading terms of its reduced Gröbner basis satisfy (8.17).

Proof. We use our "W, W'" notation, so that $W = \mathrm{GB}(H)$ and $W' = \mathrm{GB}(H')$. Let us take a point[3] $\dot{P}_k = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}) \in \Sigma_k^{j,i}$ with $1 \leq k \leq \Delta$.

$$\pi^{-1}(\dot{P}_k) = \begin{cases} Q_1 = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(1)}) \\ \quad \vdots \\ Q_k = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1}, \overline{\mathsf{a}}_{j,i}^{(k)}) \end{cases}$$

∗ We add the point Q_1.
We build W' using Theorem 8.4.1. We know that $g^* \in \widehat{W}$ (as in (a) of Lemma 8.4.6). So $W' = W_1 \sqcup W_2 \sqcup W_3$ where

- $W_1 \approxeq \{\tau, \ldots, \tau\}$, because $g^* \in \widehat{W}$. So $\mathbf{T}(W_1) \approxeq \{\tau, \ldots, \tau\}$,

[3] With our usual abuse of notation.

- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1}),$
  so $\mathbf{T}(W_{2,1}) = \{\tau, \ldots, \tau\}$.
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(1)})\}$ so $\mathbf{T}(W_{2,2}) = \{\tau\mathsf{a}_{j,i}\}$.
- $W_3 = \{g - \frac{g(Q_1)}{g^*(Q_1)}g^* \mid g > g^*\}$ and so the leading terms of W_3 are those in $\mathbf{T}(W)$, except possibly for new τ's.

Therefore the structure of W' is the same as that of W.

$*$ We add Q_{r+1} with $2 \leq r+1 \leq k$. We assume, using induction on r, that W verifies (8.17).
Let $W := W'$ and we use again Theorem 8.4.1.
To construct W' we have to find $g^* \in W$ such that $g^*(Q_{r+1}) \neq 0$. Exactly as in case (d) of Lemma 8.4.6, $\mathbf{T}(g^*) = \tau\mathsf{a}_{j,i}^r$. So $W' = W_1 \sqcup W_2 \sqcup W_3$, where

- $W_1 = \{g \in \widehat{W} \mid g < g^*\}$ where $\mathbf{T}(g^*) = \tau\mathsf{a}_{j,i}^r$.
  So $\mathbf{T}(W_1) = \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}^{r-1}, \ldots, \tau\mathsf{a}_{j,i}^{r-1}\}$ or possibly also $\tau\mathsf{a}_{j,i}^r \in \mathbf{T}(W_1)$.
- $W_2 = W_{2,1} \cup W_{2,2}$ where
  $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})\}$,
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(r+1)})\}$
- $W_3 = \{g - \frac{g(Q_{r+1})}{g^*(Q_{r+1})}g^* \mid g > g^*\}$.

Now

- If $r+1 \leq k \leq \Delta - 1$, then the structure of $\mathbf{T}(W')$ does not change. In fact $\mathbf{T}(W') = \mathbf{T}(W_1) \cup \mathbf{T}(W_2) \cup \mathbf{T}(W_3)$, where
  - $\mathbf{T}(W_1) = \{\tau, \ldots, \tau, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}^{r-1}, \ldots, \tau\mathsf{a}_{j,i}^{r-1}\}$ or possibly also $\tau\mathsf{a}_{j,i}^r \in \mathbf{T}(W_1)$,
  - $\mathbf{T}(W_2) = \mathbf{T}(W_{2,1}) \cup \mathbf{T}(W_{2,2})$ where $\mathbf{T}(W_{2,1}) = \{\tau\mathsf{a}_{j,i}^r, \ldots, \tau\mathsf{a}_{j,i}^r\}$ and $\mathbf{T}(W_{2,2}) = \{\tau\mathsf{a}_{j,i}^{r+1}\}$.
  - The leading terms of W_3 are those in $\mathbf{T}(W)$ with degree (in $\mathsf{a}_{j,i}$) at least $r+1$, plus possibly some terms in $\mathbf{T}(W)$ of degree r, that is, those greater than $\mathbf{T}(g^*)$.
- If $r+1 = \Delta$ then $\mathbf{T}(g^*) \approxeq \tau\mathsf{a}_{j,i}^{\Delta-1}$, so the leading terms of
  $$g^*(s_1 - \overline{s}_1), \ldots, g^*(s_N - \overline{s}_N), g^*(\mathsf{a}_{L,1} - \overline{\mathsf{a}}_{L,1}), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$$
  remain $\tau\mathsf{a}_{j,i}^{\Delta-1}$, but
  $$g^*(\mathsf{a}_{j,i} - \overline{\mathsf{a}}_{j,i}^{(\Delta)}) \approxeq \tau\mathsf{a}_{j,i}^{\Delta} + \ldots .$$

Since in W there is a $\overline{g}$ such that $\mathbf{T}(\overline{g}) = \mathsf{a}^{\Delta}_{j,i}$ and $\mathbf{T}(\overline{g}) | \tau \mathsf{a}^{\Delta}_{j,i}$, then, by Lemma 2.2.10, the structure of W' does not change and verifies (8.17).

□

We reiterate Lemma 8.4.8 starting from $H = \mathcal{I}(\pi^{-1}(P_1) \cup \ldots \cup \pi^{-1}(P_\Delta))$ and adding all the sets $\pi^{-1}(\dot{P}_h)$ until all points in $\mathcal{V}(J)$ have been added. When we obtain J, we will have that its leading terms satisfy (8.17), so point (1) and (2) of Proposition 8.3.13 are proved. In particular, (8.17) proves also (3) and (4).
The proof of Proposition 8.3.13 is complete.

8.5 Multi-dimensional general error locator polynomials

The following theorem ensures that our weak multi-dimensional general error locator polynomials (see Definition 8.2.5) exist for any code.

Theorem 8.5.1. *Let $C = C^{\perp}(I, L)$ be an affine–variety code with $d \geq 3$. Then*

i) $J^{C,t}_{*}$ is a radical strongly multi-stratified ideal w.r.t. the X variables.

ii) A Gröbner basis of $J^{C,t}_{*}$ contains a set of weak multi-dimensional general error locator polynomials for C.

Proof. *i)* We recall that $J^{C,t}_{*}$ is the ideal in $\mathbb{F}_q[s_1, \ldots, s_r, X_t, \ldots, X_1, e_1, \ldots, e_t]$ as defined in (8.6). We set $H = J^{C,t}_{*}$. We want to show that H is a radical strongly multi-stratified ideal with respect to the X variables. The radicality of H is obvious since it contains the field equations for all variables.
Let us consider π_j and ρ_i, $1 \leq j \leq t$ as in Definition 8.3.5

$$\pi_t : \mathcal{V}(H_{S,X_t}) \to \mathcal{V}(H_S), \quad \pi_j : \mathcal{V}(H_{S,X_t,\ldots,X_j}) \to \mathcal{V}(H_{S,X_t,\ldots,X_{j+1}})$$
$$\rho_j : \mathcal{V}(H_{\mathcal{S},X_t,\ldots,X_{j+1},X_j}) \longrightarrow \mathcal{V}(H_{X_j}),\ j = 1, \ldots, L.$$

By Definition 8.3.5, H is a strongly multi-stratified ideal with respect to the X variables if:

a0) Let $Z_j = \rho_j(\mathcal{V}(H_{\mathcal{S},X_t,\ldots,X_{j+1},X_j}))$, then $Z_j = Z_{\bar{j}}$ for any $1 \leq j \neq \bar{j} \leq t$. In this case we use $Z = Z_j$. Since the locations are only $\mathcal{V}(I) \cup \{P_0\}$, then $Z = \mathcal{V}(I) \cup \{P_0\}$.

a1) Let $1 \leq j \leq t-1$. For any $T \subset Z$ with $1 \leq |T| \leq j$, there is $\widetilde{v} \in \mathcal{V}(H_{S,X_t,\ldots,X_{j+1}})$ such that $\rho_j(\pi_j^{-1}\{\widetilde{v}\}) = T$.

a2) Moreover, for any $T \subset Z$, $1 \leq |T| \leq t$ there is $\bar{s} \in \mathcal{V}(H_S)$ such that $\rho_t(\pi_t^{-1}\{\bar{s}\}) = T$.

*b*1) For any $1 \leq j \leq t-1$ and for any $u \in \mathcal{V}(H_{\mathcal{S},X_t,\ldots,X_{j+1},X_j})$ we have that $|\pi_j^{-1}(\{u\})| \leq j$.

*b*2) Moreover, for any $\bar{s} \in \mathcal{V}(H_{\mathcal{S}})$ we have that $|\pi_t^{-1}(\{\bar{s}\})| \leq t$.

Let $\mathbf{s} = (\bar{s}_1, \ldots, \bar{s}_r)$ be a correctable syndrome corresponding to an error e of weight $\mu \leq t$. Let Q be a point in $\mathcal{V}(H)$ corresponding to $\mathbf{s}$. We have

$$Q = (\bar{s}_1, \ldots, \bar{s}_r, \bar{A}_t, \ldots, \bar{A}_1, \bar{e}_1, \ldots, \bar{e}_t).$$

We note that for any permutation $\sigma \in S_t$, there is $\widetilde{Q} \in \mathcal{V}(H)$,

$$\widetilde{Q} = (\tilde{s}_1, \ldots, \tilde{s}_r, \bar{A}_{\sigma(t)}, \ldots, \bar{A}_{\sigma(1)}, \bar{e}_{\sigma(1)}, \ldots, \bar{e}_{\sigma(t)}). \tag{8.18}$$

So (8.18) gives immediately *a*0).

We want to prove *a*1) and *a*2). Let $1 \leq j \leq t-1$ and let $T \subset Z$, $1 \leq |T| \leq j$. Let $k = |T|$. There are two cases to consider: either $P_0 \in T$ or $P_0 \notin T$.

- $P_0 \in T$. Let $Q \in \mathcal{V}(H)$ corresponding to an error with weight $\mu = t - j + k - 1$. Because of (8.18) we can assume that

  $$Q = (\bar{s}_1, \ldots, \bar{s}_r, \bar{A}_t, \ldots, \bar{A}_{j+1}, \bar{A}_j, \ldots, \bar{A}_1, \bar{e}_1, \ldots, \bar{e}_t)$$

  where $\{\bar{A}_t, \ldots, \bar{A}_{j+1}\}$ are $t-j$ elements in Z that are different from P_0, $\{\bar{A}_j, \ldots, \bar{A}_1\}$ are $(j-k+1)$ P_0's and $(k-1)$ is the number of the elements of T different from P_0. Let $u = (\bar{s}_1, \ldots, \bar{s}_r, \bar{A}_t, \ldots, \bar{A}_{j+1})$. At this point, we will obviously have $\rho_j(\pi_j^{-1}(u)) = T$.
- $P_0 \notin T$. Let $Q \in \mathcal{V}(H)$ corresponding to an error with weight $\mu = t - j + k - 1$. Similar to the previous case, because of (8.18), we can assume that $Q = (\bar{s}_1, \ldots, \bar{s}_r, \bar{A}_t, \ldots, \bar{A}_{j+1}, \bar{A}_j, \ldots, \bar{A}_1, \bar{e}_1, \ldots, \bar{e}_t)$, where $\{\bar{A}_t, \ldots, \bar{A}_{j+1}\}$ are $(t-j)$ elements of $\mathcal{V}(I) = Z \setminus \{P_0\}$, $\{\bar{A}_j, \ldots, \bar{A}_1\}$ contains $(j-k)$ points equal to P_0 and k points forming T. Let $u = (\bar{s}_1, \ldots, \bar{s}_r, \bar{A}_t, \ldots, \bar{A}_{j+1})$, then we have $\rho_j(\pi_j^{-1}(u)) = T$.

The proof of *a*2) is similar and is omitted.

To prove *b*1) and *b*2) it is enough to observe that if $t-j$ locations (including possibly the ghost point) are fixed, then at most j distinct locations can exist for that error.

ii) Since H is strongly multi-stratified, H is weakly stratified (by Proposition 8.3.11), and so we can apply Proposition 8.3.13. As weak locators, we take $\mathcal{P}_i = g^{(i)}_{t,\zeta(t,i),1}$,

where $\zeta(t,i) = \eta(t,i) \leq t$ and $\mathbf{T}(\mathcal{P}_i) = x_i^{t_i}$. In fact, the number of possible extensions is bounded by both t_i and $|\{\hat{\pi}_i(P) \mid P \in \mathcal{V}(I) \cup P_0\}|$. The first condition of Definition 8.2.5 is satisfied.

In order to prove the second condition we note that $\mathcal{P}_i(\mathbf{s}, \bar{x}_1, \ldots, \bar{x}_{i-1}, x_i)$ has among its solutions the $\bar{x}_i$'s such that $(\bar{x}_1, \ldots, \bar{x}_i)$ are the first i components of an error location corresponding to $\mathbf{s}$ (or $P_{0,i}$ value).

□

We can summarize our findings so far.

Using weak locators does not work because $\mathcal{P}_i(S, x_1, \ldots, x_i)$ depends also on $i-1$ x-variables. Thus, the point $(S, x_1, \ldots, x_{i-1}) \in \mathcal{V}(I)$ has the right multiplicity if and only if $t_i = 1$. If this fails, it is very likely to have parasite solutions.

On the other hand, if we use the general error evaluator polynomial $\mathcal{E}$, we can proceed in two ways (see Example 8.2.8), but both require an additional choice to discover parasite solutions. With non-trivial codes, this choice is very computationally expensive.

The strategy we propose here is to force point $(S, x_1, \ldots, x_{i-1}) \in \mathcal{V}(I)$ to have the right multiplicity. See Definition 8.2.5 for the t_i's.

Definition 8.5.2. *Let $C = C^{\perp}(I, L)$ be an affine-variety code.*
Let $P_0 = (\bar{x}_{0,1}, \ldots, \bar{x}_{0,m}) \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$ be a ghost point. For any $1 \leq i \leq m$, let $\mathcal{L}_i$ be a polynomial in $\mathbb{F}_q[S, x_1, \ldots, x_i]$, where $S = \{s_1, \ldots, s_r\}$. Then $\{\mathcal{L}_i\}_{1 \leq i \leq m}$ is a set of **multi-dimensional general error locator polynomials** *for C if for any i*

- *$\mathcal{L}_i(S, x_1, \ldots, x_i) = x_i^{t_i} + a_{t_i-1} x_i^{t_i-1} + \ldots + a_0$, $a_j \in \mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$ for $0 \leq j \leq t_i - 1$. In other words, $\mathcal{L}_i$ is a monic polynomial with degree t_i with respect to the variable x_i and its coefficients are in $\mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$.*

- *Given a syndrome $\bar{\mathbf{s}} = (\bar{s}_1, \ldots \bar{s}_r) \in (\mathbb{F}_q)^r$, corresponding to an error vector of weight $\mu \leq t$ and μ error locations $(\bar{x}_{1,1}, \ldots, \bar{x}_{1,m})$, $\ldots$, $(\bar{x}_{\mu,1}, \ldots, \bar{x}_{\mu,m})$, if we evaluate the S variables at $\bar{\mathbf{s}}$ and the variables $(x_1, \ldots, x_{i-1})$ at the truncated locations $\bar{\mathbf{x}}^j = (\bar{x}_{j,1}, \ldots, \bar{x}_{j,i-1})$ for any $0 \leq j \leq \mu$, then the roots of $\mathcal{L}_i(\bar{\mathbf{s}}, \bar{\mathbf{x}}^j, x_i)$ are $\{\bar{x}_{h,i} \mid \bar{\mathbf{x}}^h = \bar{\mathbf{x}}^j,\ 1 \leq h \leq \mu\}$ when $\mu = t$, and $\{\bar{x}_{h,i} \mid \bar{\mathbf{x}}^h = \bar{\mathbf{x}}^j,\ 0 \leq h \leq \mu\}$ when $\mu \leq t - 1$. That is, the polynomial $\mathcal{L}_i(\bar{\mathbf{s}}, \bar{\mathbf{x}}^j, x_i)$ does not have parasite solutions.*

Note that the number of distinct first components of error locations could be lower than μ and t_i.

To show how multi-dimensional general error locator polynomials can be applied, we redo the example on p. 155 of [FL98]. We postpone for the moment the problem of the existence of these polynomials and of the method to compute them.

Example 8.5.3. As in the Example 8.2.3, let us consider the Hermitian code C from the curve $y^2 + y = x^3$ over $\mathbb{F}_4$ and with defining monomials $\{1, x, y, x^2, xy\}$. Let us consider the lex term-ordering with $s_1 < \ldots < s_5 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$ in $\mathbb{F}_4[s_1, s_2, s_3, s_4, s_5, x_2, y_2, x_1, y_1, e_1, e_2]$.

We consider the ideal $J_*^{C,t}$. In this ideal we are lucky enough to find the two multi-dimensional general error locator polynomials that are $\mathcal{L}_{2,1}(s_1, \ldots, s_5, x_2)$ and $\mathcal{L}_{2,2}(s_1, \ldots, s_5, x_2, y_2)$, which are respectively the polynomials $\mathcal{L}_x$ and $\mathcal{L}_{xy}$ of degree two in x_2 and y_2. In this case $t_1 = t_2 = t = 2$ (a_x, b_x, a_y, b_y, c_y are in the Appendix).

$$\mathcal{L}_x = \mathbf{x}^2 + \mathbf{x}\, a_x + b_x \text{ and } \mathcal{L}_{xy} = \mathbf{y}^2 + \mathbf{y}\, a_y + \mathbf{x}\, b_y + c_y$$

Also in this example, we consider the three cases of Example 8.2.3.

- We suppose that two errors occurred in the points $P_6 = (\alpha, \alpha + 1)$ and $P_7 = (\alpha + 1, \alpha)$, so the syndrome vector corresponding to $(0, 0, 0, 0, 0, 1, 1, 0)$ is $\mathbf{s} = (0, 1, 1, 1, 0)$. In order to find the error positions we evaluate $\mathcal{L}_x$ in $\overline{\mathbf{s}}$ and we obtain the correct values of x, in fact $\mathcal{L}_x(\overline{\mathbf{s}}, x) = x^2+x+1 = (x-\alpha)(x-(\alpha+1))$. Now we have to evaluate $\mathcal{L}_y$ in $(\overline{\mathbf{s}}, \alpha)$ and in $(\overline{\mathbf{s}}, \alpha + 1)$. Also in this case we obtain the correct solutions (with the highest possible multiplicity)

  $$\mathcal{L}_{xy}(\overline{\mathbf{s}}, \alpha, y) = y^2 + \alpha = (y - (\alpha + 1))^2$$
  $$\mathcal{L}_{xy}(\overline{\mathbf{s}}, \alpha + 1, y) = y^2 + \alpha + 1 = (y - \alpha)^2.$$

- We consider the syndrome $(\alpha + 1, 0, \alpha, 0, 0)$, corresponding to the error vector $(1, \alpha, 0, 0, 0, 0, 0, 0)$, we obtain

  $$\mathcal{L}_x(\overline{\mathbf{s}}, x) = x^2 \text{ and } \mathcal{L}_{xy}(\overline{\mathbf{s}}, 0, y) = y^2 + y = y(y - 1).$$

  The solutions of the above system are $(0, 0), (0, 1)$. Also in this case the solutions of the equation $\mathcal{L}_x(\overline{\mathbf{s}}) = 0$ are correct.

- Again, when there is only one error of value $\alpha + 1$ in the third point, we have the correct answers, in fact

  $$\mathcal{L}_x(\alpha + 1, \alpha + 1, 1, \alpha + 1, 1, x) = x^2 + 1 = (x + 1)^2$$
  $$\mathcal{L}_{xy}(\alpha + 1, \alpha + 1, 1, \alpha + 1, 1, 1, y) = y^2 + (\alpha + 1)y + \alpha = (y - 1)(y - \alpha),$$

  so the solutions are $(1, 1)$, which is the ghost point, and $(1, \alpha)$ i.e. the coordinates of the right location.

The main difference between $\mathcal{L}_x$,$\mathcal{L}_{xy}$ of Example 8.2.3 and $\mathcal{L}_x$, $\mathcal{L}_{xy}$ of this example is that now we do not have spurious solutions, that is, now the roots of our locators are exactly the error locations and no more ambiguity exists.

As evident from the previous example, multidimensional general error locator polynomials are very convenient for decoding. However, to prove their existence we cannot use the theoretical methods developed so far, because these methods do not deal with multiplicities. In the next section we will develop more advanced theoretical methods, that will permit us to construct ideals where these polynomials lie and can be easily spotted.

8.6 Stuffed ideals

Let G be a reduced Gröbner basis of a radical weakly stratified ideal J as in Proposition 8.3.13. From now on we consider the ordering as in Proposition 8.3.13. In this section we fix $1 \leq i \leq m$ and $1 \leq j \leq L$ and we consider the projection

$$\pi : \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1},\mathsf{a}_{j,i}}) \to \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1}}).$$

We consider the variable $\mathsf{a}_{j,i}$ in block A_j.

Let $\mathcal{R} = \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i-1}]$. Let g be a polynomial in $G^{j,i}$ such that the degree in $\mathsf{a}_{j,i}$ of g is $\Delta = \zeta(j,i) = \eta(j,i)$. By Proposition 8.3.13, we know that this polynomial exists and it can be assumed to be monic in $\mathcal{R}[\mathsf{a}_{j,i}]$. Let $P_h \in \Sigma_h^{j,i}$ where $1 \leq h \leq \Delta - 1$, then

$$g(P_h, \mathsf{a}_{j,i}) = \mathsf{a}_{j,i}^{\Delta} + \alpha_{\Delta-1}\mathsf{a}_{j,i}^{\Delta-1} + \ldots + \alpha_0 \in \mathbb{K}[\mathsf{a}_{j,i}] \text{ where } \alpha_i \in \mathbb{K}.$$

We are interested in solutions of the equation

$$g(P_h, \mathsf{a}_{j,i}) = 0. \tag{8.19}$$

Since $P_h \in \Sigma_h^{j,i}$, there exist distinct $Q_1, \ldots, Q_h$ such that $\pi^{-1}(P_h) = \{Q_1, \ldots, Q_h\}$, with $Q_l = (P_h, \lambda_l)$ for any $1 \leq l \leq h$. So $\lambda_1, \ldots, \lambda_h$ are some solutions of (8.19). But there exist other $\Delta - h$ solutions (counting multiplicities) of (8.19), say $\lambda_{h+1}, \ldots, \lambda_\Delta$. There are two cases:

(a) It may be that $\lambda_{h+l} \notin \{\lambda_1, \ldots, \lambda_h\}$ for some l. In this case, point (P_h, λ_{h+l}) is not an extension of P_h, because $(P_h, \lambda_{h+l}) \notin \mathcal{V}(J_{\mathcal{S},\mathcal{A}_L,\ldots,\mathcal{A}_{j+1},\mathsf{a}_{j,1},\ldots,\mathsf{a}_{j,i-1},\mathsf{a}_{j,i}})$, and so λ_{h+l} is a parasite solution.

(b) But it may also be that $\{\lambda_{h+1}, \ldots, \lambda_\Delta\} \subset \{\lambda_1, \ldots, \lambda_h\}$, depending on the multiplicities of the $\{\lambda_1, \ldots, \lambda_h\}$. In this case, if we solve (8.19), we have exactly the extensions and we are not confused by parasite solutions.

We want to change slightly our variety in order to force case (b). To do that, we need that the sum of multiplicities of $\{\lambda_l\}_{1 \leq l \leq h}$ is equal to Δ. To increase the multiplicity of any λ_l, we can use the Hasse derivative (see Subsection 4.4.2 and in particular Theorem 4.4.6).

Definition 8.6.1. *Let $K \subset \mathcal{R}[\mathsf{a}_{j,i}]$ be a zero-dimensional ideal such that $\mathcal{V}(K) \subset \mathbb{A}_{j,i}$. Let $\Delta = \eta(j,i)$. Let $G = \mathrm{GB}(K)$ and $g = g_{\Delta}^{(i)}$. We say that K is **stuffed** if for any $1 \leq h \leq \Delta - 1$ and for any $P_h \in \Sigma_h^{j,i}$, the equation (8.19) has h distinct solutions in $\mathbb{K}$.*

Definition 8.6.2. *Let $H \subset \mathbb{K}[V_1, \ldots, V_{\mathcal{N}}]$ be a zero-dimensional ideal. Let $n \geq 1$. Let $f \in H$ and $Q \in \mathcal{V}(H)$ where $Q = (P, \overline{V}_{\mathcal{N}})$. Let $\vartheta_1 : H \longrightarrow \mathbb{K}$ such that*

$$\vartheta_1(f) = \varphi^{(1)}(f(P, V_{\mathcal{N}}))\big|_{V_{\mathcal{N}} = \overline{V}_{\mathcal{N}}}$$

and let $H^{[Q,1]} = \ker \vartheta_1$. We define inductively $\vartheta_n : H^{[Q,n-1]} \longrightarrow \mathbb{K}$ such that

$$\vartheta_n(f) = \varphi^{(n)}(f(P, V_{\mathcal{N}}))\big|_{V_{\mathcal{N}} = \overline{V}_{\mathcal{N}}}$$

and we write $H^{[Q,n]} = \ker \vartheta_n$.

We note that $H^{[Q,1]}$ is an ideal. In fact, if $f \in H^{[Q,1]}$, $g \in \mathbb{K}[V_{\mathcal{N}}]$ and $\overline{V}_{\mathcal{N}} \in \mathcal{V}(f)$ then we claim that

$$\varphi^{(1)}(fg)(\overline{V}_{\mathcal{N}}) = \varphi^{(1)}(f)(\overline{V}_{\mathcal{N}})g(\overline{V}_{\mathcal{N}}) + \varphi^{(1)}(g)(\overline{V}_{\mathcal{N}})f(\overline{V}_{\mathcal{N}}) = 0.$$

In fact, $\varphi^{(1)}(f)(\overline{V}_{\mathcal{N}}) = 0$, since $f \in \ker \vartheta_1$ and $f(\overline{V}_{\mathcal{N}}) = 0$, since $\overline{V}_{\mathcal{N}} \in \mathcal{V}(f)$. Inductively, we can similarly prove that $H^{[Q,n]}$ is an ideal.

Let us consider a zero-dimensional ideal $K \subset \mathcal{R}[\mathsf{a}_{j,i}]$. It is convenient to call our variables also as $\{V_1, \ldots, V_{\mathcal{N}}\} = \mathcal{S} \cup \mathcal{A}_L, \cup \ldots, \mathcal{A}_{j+1} \cup \{\mathsf{a}_{j,1}, \ldots, \mathsf{a}_{j,i}\}$, in such a way that $V_1 < \ldots < V_{\mathcal{N}}$ and $V_{\mathcal{N}} = \mathsf{a}_{j,i}$.
We suppose that $G = \mathrm{GB}(K)$ satisfies (8.17), that is

$$\mathbf{T}(G) \approxeq \{\tau, \ldots, \tau, \tau V_{\mathcal{N}}, \ldots, \tau V_{\mathcal{N}}, \ldots, \tau V_{\mathcal{N}}^{\Delta-1}, \ldots, \tau V_{\mathcal{N}}^{\Delta-1}, V_{\mathcal{N}}^{\Delta}\}$$

and τ is any elements in $V_1 < \ldots < V_{\mathcal{N}-1}$. In particular there is a polynomial $g \in G^{j,i}$ s.t. $\mathbf{T}(g) = {\mathsf{a}_{j,i}}^{\Delta} = {V_{\mathcal{N}}}^{\Delta}$.
For each $1 \leq h \leq \Delta - 1$ we perform the following operations:

(a) If for any $P_h \in \Sigma_h^{j,i}$ equation (8.19) has h distinct solutions in $\mathbb{K}$, we do nothing. Otherwise, we take any $P_h \in \Sigma_h^{j,i}$ such that (8.19) has more than h solutions.

(b) We consider $Q = (P_h, \overline{V}_{\mathcal{N}})$ which is any extension of P_h. We want to compute $H^{[Q,\Delta-h]}$. In order to do that, we iteratively compute $\ker \vartheta_n$ (see Definition 8.6.2) from $n = 1$ to $n = \Delta - h$.

(c) For any such n, we apply Theorem 8.4.1 to $H = H^{[Q,n-1]}$ and $H' = H^{[Q,n]}$, so that $H' = \ker \vartheta_n$. The hypotheses of Theorem 8.4.1 are trivially satisfied, because ϑ_n is $\mathbb{K}-$linear and $\ker \vartheta_n$ is an ideal. In the subsequent step (d), we get ready to apply Theorem 8.4.1.

(d) We consider the point $Q = (\overline{V}_1, \ldots, \overline{V}_{\mathcal{N}}) = (P, \overline{\mathsf{a}}_{j,i})$ with $P = (\overline{V}_1, \ldots, \overline{V}_{\mathcal{N}-1}) = (\overline{s}_1, \ldots, \overline{s}_N, \overline{\mathsf{a}}_{L,1}, \ldots, \overline{\mathsf{a}}_{j,i-1})$, Q is a solution of ideal H. To apply Theorem 8.4.1, we consider the smallest polynomial $g^* \in W$, with $W = \mathrm{GB}(H)$, such that

$$\vartheta_n(g^*) \neq 0, \text{ that is, } \varphi^{(n)}(g^*((P, V_{\mathcal{N}}))\big|_{V_{\mathcal{N}}=\overline{V}_{\mathcal{N}}} \neq 0.$$

We compute W' from W. To apply Theorem 8.4.1, we need to identify β_k's such that

$$\vartheta_n((V_k - \beta_k)g^*) = 0 \text{ where } 1 \leq k \leq \mathcal{N},$$

where we consider the weaker form (iii) in Remark 8.4.2.
We solve the previous equation as follows

$$\begin{array}{l} \vartheta_n((V_k - \beta_k)g^*) = (\overline{V}_k - \beta_k)\vartheta_n(g^*) = 0 \quad (1 \leq k \leq \mathcal{N} - 1) \\ \implies \beta_k \text{ is the } k\text{-th component of } Q. \end{array}$$

$$\begin{array}{l} \vartheta_n((V_{\mathcal{N}} - \beta_{\mathcal{N}})g^*) = g^*(Q) + \overline{V}_{\mathcal{N}}\vartheta_n(g^*) - \beta_{\mathcal{N}}\vartheta_n(g^*) = 0 \\ \implies \beta_{\mathcal{N}} = \frac{g^*(Q) + \overline{V}_{\mathcal{N}}\vartheta_n(g^*)}{\vartheta_n(g^*)} = \frac{g^*(Q)}{\vartheta_n(g^*)} + \overline{V}_{\mathcal{N}}. \end{array}$$

Lemma 8.6.3. *We claim that*

$$g^* \in G_r^{j,i}, \text{ i.e. } \boldsymbol{T}(g^*) \approxeq \tau \mathsf{a}_{j,i}^r \text{ where } n - 1 \leq r \leq \Delta - 1.$$

Proof. Recall that we use $\approxeq$ to express a unconventional identification (see Remark 8.4.3). If $\mathbf{T}(g^*) \approxeq \tau \mathsf{a}_{j,i}^r$ with $r < n-1$, then $\vartheta_n(g^*) = 0$. So $\mathbf{T}(g^*) \approxeq \tau \mathsf{a}_{j,i}^r$ with $r \geq n - 1$. However, $r \neq \Delta$, otherwise we have already finished. So $n - 1 \leq r \leq \Delta - 1$. □

(e) We build W' using Theorem 8.4.1. By Lemma 8.6.3 we have that

$$\mathbf{T}(g^*) \approxeq \tau \mathsf{a}_{j,i}^r \quad n - 1 \leq r \leq \Delta - 1.$$

So $W' = W_1 \cup W_2 \cup W_3$ where

- $W_1 = \{g \mid g < g^*\}$.
  So $\mathbf{T}(W_1) \approxeq \{\tau, \ldots, \tau \mathsf{a}_{j,i}, \ldots, \tau \mathsf{a}_{j,i}^{r-1}\}$, or possibly also $\tau \mathsf{a}_{j,i}^r \in \mathbf{T}(W_1)$.
- $W_2 = W_{2,1} \cup W_{2,2}$ where $W_{2,1} = \{g^*(s_1 - \overline{s}_1), \ldots, g^*(\mathsf{a}_{j,i-1} - \overline{\mathsf{a}}_{j,i-1})$,
  so $\mathbf{T}(W_{2,1}) = \{\tau \mathsf{a}_{j,i}^r, \ldots, \tau \mathsf{a}_{j,i}^r\}$.
  $W_{2,2} = \{g^*(\mathsf{a}_{j,i} - \frac{g^*}{\vartheta_r(g^*)} - \overline{\mathsf{a}}_{j,i})\}$. Then $\mathbf{T}(W_{2,2}) = \{\tau \mathsf{a}_{j,i}^{r+1}\}$.
- $W_3 = \{g - \frac{\vartheta_r(g)}{\vartheta_r(g^*)} g^* \mid g > g^*\}$ and hence the leading terms of W_3 are those in $\mathbf{T}(W)$, except for $\tau, \ldots, \tau \mathsf{a}_{j,i}^{r-1}$ and possibly $\tau \mathsf{a}_{j,i}^r$.

Therefore, the structure of W' is the same as that of W, except possibly if $r+1=\Delta$. In that case

- $\mathbf{T}(W_1) \approxeq \{\tau, \ldots, \tau\mathsf{a}_{j,i}, \ldots, \tau\mathsf{a}_{j,i}, \tau\mathsf{a}_{j,i}^{\Delta-2}, \ldots, \tau\mathsf{a}_{j,i}^{\Delta-2}\}$, or possibly also $\tau\mathsf{a}_{j,i}^{\Delta-1} \in \mathbf{T}(W_1)$,
- $\mathbf{T}(W_2) = \mathbf{T}(W_{2,1}) \cup \mathbf{T}(W_{2,2})$ where $\mathbf{T}(W_{2,1}) = \{\tau\mathsf{a}^{\Delta-1}, \ldots, \tau\mathsf{a}^{\Delta-1}\}$ and $\mathbf{T}(W_{2,2}) = \{\tau\mathsf{a}_{j,i}^{\Delta}\}$.
- $\mathbf{T}(W_3) = \emptyset$.

In the Gröbner basis W in (8.17) there exists a polynomial $\overline{g}$ s.t. $\mathbf{T}(\overline{g}) = \mathsf{a}_{j,i}^{\Delta}$. So $\mathbf{T}(\overline{g}) | \tau\mathsf{a}_{j,i}^{\Delta}$ and we can remove the new term. Thus $\mathbf{T}(W')$ does not change and it remains as in (8.17).

(f) Once all the above operations have been concluded, for any $1 \leq h \leq \Delta - 1$ and for any $P_h \in \Sigma_h^{j,i}$, (8.19) will have exactly h distinct solutions and the resulting ideal will be stuffed.

We have thus proved the following theorem:

Theorem 8.6.4. *Let $K \subset \mathcal{R}[\mathsf{a}_{j,i}]$ be a zero-dimensional ideal such that $G = \mathrm{GB}(K)$ verifies (8.17). Let g be the polynomial in G such that $\boldsymbol{T}(g) = \mathsf{a}_{j,i}^{\Delta}$, with $\Delta = \eta(j,i)$. We can obtain an ideal $\widetilde{K} \subset \mathcal{R}[\mathsf{a}_{j,i}]$ such that*

1. *$\widetilde{K}$ is stuffed.*
2. *$\mathrm{GB}(\widetilde{K})$ verifies (8.17).*
3. *$\mathcal{V}(\widetilde{K}) = \mathcal{V}(K)$.*

Although, in Theorem 8.6.4 we obtain $\widetilde{K}$ as in the procedure above, there are other ways to obtain $\widetilde{K}$, for example by simultaneously increasing the multiplicity of more λ_h's.

Note that, generally speaking, $\widetilde{K}$ will lose the radicality, but its Gröbner basis will retain (8.17), which is what we need.

Theorem 8.6.5. *If K and $\widetilde{K}$ are as in Theorem 8.6.4, then if K is, respectively, strongly multi-stratified, multi-stratified and weakly stratified, then $\widetilde{K}$ is as well.*

Proof. The stuffing procedure does not change the number of pre-images at any level. □

Now, we are finally able to prove the existence of our multi-dimensional general error locator polynomials for any code. Note that this is another constructive proof, since it tells us how to compute our polynomials, that is, simply by computing a suitable Gröbner bases of the corresponding stuffed ideal.

Theorem 8.6.6. *Let $C = C^{\perp}(I, L)$ be an affine-variety code with $d \geq 3$. Let $\widetilde{J}_*^{C,t}$ be a stuffed ideal of $J_*^{C,t}$. Then*

1. *$\widetilde{J}_*^{C,t}$ is a strongly multi-stratified ideal with respect to the X variables.*

2. *A Gröbner basis of $\widetilde{J}_*^{C,t}$ contains a set of multi-dimensional general error locator polynomials for C.*

Proof. 1. We can use Theorem 8.6.5 and so $\widetilde{J}_*^{C,t}$ is a strongly multi-stratified ideal.

2. As locators we can take for any i

$$\mathcal{L}_i = g^{(i)}_{t,\zeta(t,i),1},$$

where $\zeta(t,i) = \eta(t,i)$ and $\mathbf{T}(\mathcal{L}_i) = x_i^{t_i}, \quad t_i = \zeta(t,i) = \eta(t,i)$, thanks to Theorem 8.6.4. So the first condition of Definition 8.5.2 is satisfied.
Let $H = J_*^{C,t}$ and $\widetilde{H} = \widetilde{J}_*^{C,t}$. In order to prove the second condition we note that, since $\mathcal{L}_i$ is a polynomial of $\widetilde{H}_{S,x_{t,1},\ldots,x_{t,i}}$ it will vanish at $(\mathbf{s}, \bar{x}_1, \ldots, \bar{x}_i)$, where $\mathbf{s} = (\bar{s}_1, \ldots, \bar{s}_r)$ and $(\mathbf{s}, \bar{x}_1, \ldots, \bar{x}_i)$ can be extended to a point in $\mathcal{V}(H) = \mathcal{V}(\widetilde{H})$. Since $\widetilde{H}$ is stuffed, $\mathcal{L}_i(\mathbf{s}, \bar{x}_1, \ldots, \bar{x}_{i-1}, x_i)$ has as solutions only the $\bar{x}_i$'s such that $(\bar{x}_1, \ldots, \bar{x}_i)$ are the first i components of an error location corresponding to $\mathbf{s}$ (or $P_{0,i}$).

□

8.7 Families of affine–variety codes

In this section we consider some families of affine-variety codes.

8.7.1 SDG curves

We discuss codes from some curves introduced in [SDG06].

Definition 8.7.1 ([SDG06])**.** *Let $\mathbb{F}_s$ be a subfield of $\mathbb{F}_q$. A polynomial f in $\mathbb{F}_q[x]$ is called an $(\mathbb{F}_q, \mathbb{F}_s)$–polynomial if for each $\gamma \in \mathbb{F}_q$ we have $f(\gamma) \in \mathbb{F}_s$.*

Proposition 8.7.2 ([SDG06])**.** 1. *The polynomial $f(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_4[x]$ is an $(\mathbb{F}_4, \mathbb{F}_2)$–polynomial if and only if $b_0, b_3 \in \mathbb{F}_2$ and $b_2 = b_1^2$.*

2. *The polynomial $g(x) = b_7x^7 + \cdots + b_1x + b_0 \in \mathbb{F}_8[x]$ is an $(\mathbb{F}_8, \mathbb{F}_2)$–polynomial if and only if $b_0, b_7 \in \mathbb{F}_2$, $b_2 = b_1^2$, $b_4 = b_2^2$, $b_6 = b_3^2$ and $b_3 = b_5^2$.*

Let $\mathcal{F} = \{f(x) + g(y) \mid f, g \text{ are } (\mathbb{F}_8, \mathbb{F}_2)\text{-polynomials }, \deg(f) = 4, \deg(g) = 6\}$. In [SDG06] it is shown that the family $\mathcal{F}$ has 784 members and that each member of this family has 32 roots in $(\mathbb{F}_8)^2$. Let us consider the polynomial $\mathcal{G} = f(x) + g(y)$, with $f(x) = x^4 + x^2 + x$ and $g(y) = y^6 + y^5 + y^3 + 1$, so that $\mathcal{G} \in \mathcal{F}$. Let $I = \langle \mathcal{G} \rangle$ and $J_*^{C,t}$ be the ideal associated to the $C = C^\perp(I, L)$ code over $\mathbb{F}_8$ that can correct up to $t = 1$ errors and with defining monomials $L = \{1, y, x, y^2\}$. Ideal $J_*^{C,t}$ is generated by:

$$\{x_1^8 - x_1, y_1^8 - y_1, e_1^7 - 1, x_1^4 + x_1^2 + x_1 + y_1^6 + y_1^5 + y_1^3 + 1, e_1 - s_1, e_1 y_1 - s_2, e_1 x_1 - s_3, e_1 y_1^2 - s_4\}$$

and the reduced Gröbner basis G with respect to the lexicographic ordering with $s_1 < s_2 < s_3 < s_4 < x_1 < y_1 < e_1$ is

$$\{s_1^7 + 1, s_2^8 + s_2, s_3^4 + s_3^2 s_1^2 + s_3 s_1^3 + s_2^6 s_1^5 + s_2^5 s_1^6 + s_2^3 s_1 + s_1^4, s_4 + s_2^2 s_1^6,$$
$$\mathbf{x_1} + s_3 s_1^6, \mathbf{y_1} + s_2 s_1^6, e_1 + s_1\}$$

and then

$$\mathcal{L}_2 = \mathbf{y_1} + s_3 s_1^6, \qquad \mathcal{L}_1 = \mathbf{x_1} + s_2 s_1^6.$$

8.7.2 SDG surfaces I

We discuss codes from some surfaces introduced in [SDG06].
Let $\mathcal{F} = \{f(x) + g(y) + h(z) \mid f, g, h \text{ are } (\mathbb{F}_4, \mathbb{F}_2)\text{-polynomials}, \deg(f) = \deg(h) = 3, \deg(g) = 2\}$. In [SDG06] it is shown that the family $\mathcal{F}$ has 96 members and that each member of this family has 32 roots in $(\mathbb{F}_4)^3$. Let us consider the polynomial $\mathcal{G} = f(x) + g(y) + h(z)$, with $f(x) = x^3$, $g(y) = y^2 + y + 1$ and $h(z) = z^3 + 1$, so that $\mathcal{G} \in \mathcal{F}$. Let $I = \langle \mathcal{G} \rangle$ and $J_*^{C,t}$ be the ideal associated to the code $C = C^\perp(I, L)$ over $\mathbb{F}_4$ that can correct up to $t = 1$ error and with defining monomials $L = \{1, x, z, y\}$. The ideal $J_*^{C,t} \subset \mathbb{F}_4[s_1, s_2, s_3, s_4, x_1, y_1, z_1, e_1]$ is generated by

$$\{x_1^4 - x_1, y_1^4 - y_1, z_1^4 - z_1, e_1^3 - 1, g + f + h, e_1 - s_1, e_1 z_1 - s_3, e_1 x_1 - s_2, e_1 y_1 - s_4\}$$

and the reduced Gröbner basis G with respect to the lex ordering with $s_1 < s_2 < s_3 < s_4 < x_1 < y_1 < z_1 < e_1$ is

$$\{s_1^3 + 1,\ s_2^4 + s_2,\ s_3^4 + s_3,\ s_4^2 + s_4 s_1 + s_3^3 s_1^2 + s_2^3 s_1^2,\ \mathbf{y_1} + s_4 s_1^2,\ \mathbf{x_1} + s_2 s_1^2,\ \mathbf{z_1} + s_3 s_1^2,\ e_1 + s_1\},$$

and then

$$\mathcal{L}_1 = \mathbf{x_1} + s_2 s_1^2, \quad \mathcal{L}_2 = \mathbf{y_1} + s_4 s_1^2, \quad \mathcal{L}_3 = \mathbf{z_1} + s_3 s_1^2.$$

8.7.3 SDG surfaces II

We discuss codes from another family of surfaces introduced in [SDG06].

Let $\mathcal{F} = \{\beta x^2 z + \beta^2 x z^2 + f(x) + g(y) + h(z) \mid \beta \neq 0, f, g, h$ are $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials, $\deg(f) \leq 2, \deg(h) \leq 3, \deg(g) = 2\}$. In [SDG06] it is shown that the family $\mathcal{F}$ has 576 members and that each member of this family has 32 roots in $(\mathbb{F}_4)^3$. Let us consider the polynomial $\mathcal{G} = x^2 z + x z^2 + f(x) + g(y) + h(z)$, with $\beta = 1$, $f(x) = 1$, $g(y) = y^2 + y + 1$ and $h(z) = z^3 + 1$, so that $\mathcal{G} \in \mathcal{F}$. Let $I = \langle \mathcal{G} \rangle$ and $J_*^{C,t}$ be the ideal associated to the code $C = C^\perp(I, L)$ over $\mathbb{F}_4$ that can correct one error and with defining monomials $L = \{1, z, z^2, z^3, x, y\}$.
The ideal $J_*^{C,t} \subset \mathbb{F}_4[s_1, s_2, s_3, s_4, s_5, s_6, x_1, y_1, z_1, e_1]$ is generated by

$$\{x_1^4 - x_1, y_1^4 - y_1, z_1^4 - z_1, e_1^3 - 1, x_1^2 z_1 + x_1 z_1^2 + f + g + h,$$
$$e_1 - s_1, e_1 z_1 - s_2, e_1 z_1^2 - s_3, e_1 z_1^3 - s_4, e_1 x_1 - s_5, e_1 y_1 - s_6, \}$$

and the reduced Gröbner basis G with respect to the lex ordering with $s_1 < s_2 < s_3 < s_4 < s_5 < s_6 < x_1 < y_1 < z_1 < e_1$ is

$$\{s_1^3 + 1, s_2^4 + s_2, s_3 + s_2^2 s_1^2, s_4 + s_2^3 s_1, s_5^4 + s_5, s_6^2 + s_6 s_1 + s_5^2 s_2 s_1^2 + s_5 s_2^2 s_1^2 + s_2^3 s_1^2 + s_1^2,$$
$$\mathbf{x_1} + s_5 s_1^2, \mathbf{y_1} + s_6 s_1^2, \mathbf{z_1} + s_2 s_1^2, e_1 + s_1\}$$

and then

$$\mathcal{L}_1 = \mathbf{x_1} + s_5 s_1^2, \quad \mathcal{L}_2 = \mathbf{y_1} + s_6 s_1^2, \quad \mathcal{L}_3 = \mathbf{z_1} + s_2 s_1^2 .$$

8.7.4 Norm–trace curves

Let $C = C^\perp(I, L)$ be the code from the norm–trace curve $x^7 = y^4 + y^2 + y$ over $\mathbb{F}_8$ and with defining monomials $\{1, x, x^2, y\}$. This code can correct $t = 1$ error. Let $J_*^{C,t}$ be the ideal generated by:

$$\{x_1^8 - x_1, y_1^8 - y_1, e_1^7 - 1, e_1 - s_1, e_1 x_1 - s_2, e_1 x_1^2 - s_3, e_1 y_1 - s_4, x_1^7 - y_1^4 - y_1^2 - y_1\}$$

and the reduced Gröbner basis G with respect to the lex ordering with $s_1 < s_2 < s_3 < s_4 < x_1 < y_1 < e_1$ is

$$\{s_1^7 + 1, s_2^8 + s_2, s_3 + s_2^2 s_1^6, s_4^4 + s_4^2 s_1^2 + s_4 s_1^3 + s_2^7 s_1^4, \mathbf{x_1} + s_2 s_1^6, \mathbf{y_1} + s_4 s_1^6, e_1 + s_1\}.$$

Then

$$\mathcal{L}_1 = \mathbf{x_1} + s_2 s_1^6, \quad \mathcal{L}_2 = \mathbf{y_1} + s_4 s_1^6 .$$

Observe that in all our examples so far no stuffing was required, because we were considering the case $t = 1$, which clearly cannot contain multiplicities.

8.7.5 Hermitian curves

Let q be a power of a prime, then the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$ is defined by the affine equation $x^{q+1} = y^q + y$. Each member of this family has $n = q^3$ points in $\mathbb{F}_{q^2}$ and it is well-known that the function space is generated by monomials.

In Example 8.2.3 we considered the case $q = 2$ and $t = 2$, we now consider the code C corresponding to the case $q = 3$ and $t = 2$. The defining monomials are $L = \{1, x, y, x^2, xy, y^2, x^3\}$. As before, we choose as ghost point $(1, 1)$.
Our ideal $J_*^{C,2}$ is generated by

$$\{x_1^9 - x_1, y_1^9 - y_1, e_1^9 - e_1, e_2^9 - e_2, x_2^9 - x_2, y_2^9 - y_2, y_1^3 x_1 - y_1^3 + y_1 x_1 - y_1 - x_1^5 + x_1^4,$$
$$y_2^3 x_2 - y_2^3 + y_2 x_2 - y_2 - x_2^5 + x_2^4, y_1^4 - y_1^3 + y_1^2 - y_1 - y_1 x_1^4 + x_1^4, y_2^4 - y_2^3 + y_2^2 - y_2 - y_2 x_2^4 + x_2^4,$$
$$e_1 + e_2 - s_1, e_1 x_1 + e_2 x_2 - s_2, e_1 y_1 + e_2 y_2 - s_3, e_1 x_1^2 + e_2 x_2^2 - s_4, e_1 x_1 y_1 + e_2 x_2 y_2 - s_5,$$
$$e_1 y_1^2 + e_2 y_2^2 - s_6, e_1 x_1^3 + e_2 x_2^3 - s_7, e_1((x_1 - 1)^8 - 1)((y_1 - 1)^8 - 1), e_2((x_2 - 1)^8 - 1)((y_2 - 1)^8 - 1),$$
$$(e_1^8 - 1)(x_1 - 1), (e_1^8 - 1)(y_1 - 1), (e_2^8 - 1)(x_2 - 1), (e_2^8 - 1)(y_2 - 1), e_1 e_2((x_1 - x_2)^8 - 1)((y_1 - y_2)^8 - 1)\}.$$

We compute the Gröbner basis G with respect to the usual lex ordering with $s_1 < \cdots < s_7 < x_2 < y_2 < x_1 < y_1 < e_2 < e_1$. The general error evaluator polynomial of $\mathcal{C}$ contains 134 monomials and it is reported in the Appendix.

The first weak locator $\mathcal{P}_2$ contains 172 monomials, while the second weak locators $\mathcal{P}_1$ contains 494 monomials (see Appendix for all polynomials). However, these polynomials are by far not random. Indeed, we can prove the following general structure result for any $q \geq 2$ and $t = 2$.

Theorem 8.7.3. *Let p be any prime number and $m \in \mathbb{N}$ such that $q = p^m \geq 2$. Let $C = C^{\perp}(I, L)$ be any Hermitian code with $t = 2$ over $\mathbb{F}_q$. Then all sets of multi-dimensional general error locator polynomials for C are of the form*

$$\begin{gathered}\{\mathcal{L}_2 = \mathcal{L}_x = x^2 + ax + b, \mathcal{L}_1 = \mathcal{L}_{xy} = y^2 + cy + d\} \\ \{\mathcal{L}_2 = \mathcal{L}_y = y^2 + Ay + B, \mathcal{L}_1 = \mathcal{L}_{yx} = x^2 + Cx + D\}\end{gathered} \tag{8.20}$$

with $a, b, A, B \in \mathbb{F}_p[S]$, $c, d \in \mathbb{F}_p[S, x]$ and $C, D \in \mathbb{F}_p[S, y]$.
Moreover,

$$q \geq 2 \implies as_2 + bs_1 = -s_4\,, \tag{8.21}$$
$$q \geq 3 \implies As_3 + Bs_1 = -s_6\,. \tag{8.22}$$

Let $q \geq 2$ and $s_1 = s_2 = 0$. We have $e_1 = -e_2$, $x_1 = x_2$, $b = x_1^2$, $a = 2x_1$.
Let $q \geq 3$ and $s_1 = s_3 = 0$. We have $e_1 = -e_2$, $y_1 = y_2$, $B = y_1^2$, $A = 2y_1$.

All the results above hold also for any set of weak multi-dimensional general error locator polynomials

$$\begin{gathered}\{\mathcal{P}_2 = \mathcal{P}_x = x^2 + ax + b, \mathcal{P}_1 = \mathcal{P}_{xy} = y^2 + cy + d\} \\ \{\mathcal{P}_2 = \mathcal{P}_y = y^2 + Ay + B, \mathcal{P}_1 = \mathcal{P}_{yx} = x^2 + Cx + D\}\end{gathered} \tag{8.23}$$

Proof. Let $H = J_*^{C,2}$ be the non-stuffed ideal for C and $\widetilde{H}$ its stuffed ideal as in Theorem 8.6.6. There are two Gröbner bases of H and $\widetilde{H}$ that are relevant for us. If the order has $S < x_2 < y_2$ then we get G_x for H and $\widetilde{G}_x$ for $\widetilde{H}$. If the order has $S < y_2 < x_2$ then we get G_y for H and $\widetilde{G}_y$ for $\widetilde{H}$. As in Theorem 8.6.6, $\widetilde{G}_x$ contains polynomials $\mathsf{p}_x \in \mathbb{F}_q[S, x_2]$ and $\mathsf{p}_{x,y} \in \mathbb{F}_q[S, x_2, y_2]$ such that, once we replace x_2 with x and y_2 with y, we get a set of locators $\{\mathcal{L}_2 = \mathcal{L}_x, \mathcal{L}_1 = \mathcal{L}_{xy}\}$.
The degree of p_x in x_2 is, *a priori*, 1 or 2. However, since there are at least two points $\{P_1, P_2\}$ on the curve with two different x, then $\deg_{x_2} \mathsf{p}_x = 2$, since p_x must have two distinct roots once evaluated on a syndrome corresponding to a weight-2 error with $\{P_1, P_2\}$ as locations.
The degree of $\mathsf{p}_{x,y}$ in y_2 is, *a priori*, 1 or 2. However, for any $\bar{x} \in \mathbb{F}_q$ there are at least two points $\{P_1 = (\bar{x}, \bar{y}_1), P_2 = (\bar{x}, \bar{y}_2)\}$ on the curve with $\bar{y}_1 \neq \bar{y}_2$. Then $\deg_{y_2} \mathsf{p}_y = 2$, since it must have the two distinct roots $\{\bar{y}_1, \bar{y}_2\}$ once evaluated on a syndrome corresponding to a weight-2 error with $\{P_1, P_2\}$ as locations.
The previous argument can be trivially adapted to show that $\deg_{y_2}(\mathsf{p}_y) = 2$ and $\deg_{x_2}(\mathsf{p}_{y,x}) = 2$, where $\mathsf{p}_y \in \mathbb{F}_q[S, y_2]$ and $\mathsf{p}_{y,x} \in \mathbb{F}_q[S, y_2, x_2]$ come from $\widetilde{G}_y$, and so (8.20) is proved, except for our claim that all the coefficients of these polynomials actually lie in the base field $\mathbb{F}_p$, which follows from Remark 8.2.4.

To prove (8.21), we first claim that

$$f \in H \implies f^2 \in \widetilde{H}. \tag{8.24}$$

To see (8.24) we note that in the creation of $\widetilde{H}$ from H we only impose the vanishing of the first-order derivative at points of $\mathcal{V}(H)$, but if we take any point $Q \in \mathcal{V}(H)$ we have (see Definition 8.6.2 for θ_1)

$$\theta_1(f^2) = 2f(Q)\theta_1(f) = 0\theta_1(f) = 0\,.$$

Since $s_1 - e_1 - e_2, s_2 - e_1x_1 - e_2x_2, s_4 - e_1x_1^2 - e_2x_2^2 \in H$, we have that
$(s_1 - e_1 - e_2)^2, (s_2 - e_1x_1 - e_2x_2)^2, (s_4 - e_1x_1^2 - e_2x_2^2)^2 \in \widetilde{H}$ for (8.24). Passing from variables to values we observe that

$$\bar{s}_1 = \bar{e}_1 + \bar{e}_2, \quad \bar{s}_2 = \bar{e}_1\bar{x}_1 + \bar{e}_2\bar{x}_2, \quad \bar{s}_4 = \bar{e}_1\bar{x}_1^2 + \bar{e}_2\bar{x}_2^2 \tag{8.25}$$

and that

$$\bar{a} = a(\bar{S}) = -(\bar{x}_1 + \bar{x}_2), \quad \bar{b} = \bar{x}_1\bar{x}_2\,.$$

So

$$-(\bar{x}_1 + \bar{x}_2)(\bar{e}_1\bar{x}_1 + \bar{e}_2\bar{x}_2) + \bar{x}_1\bar{x}_2(\bar{e}_1 + \bar{e}_2) = -(\bar{e}_1\bar{x}_1^2 + \bar{e}_2\bar{x}_2^2), \text{ which proves (8.21).}$$

In the same way, we can compute the set of locators $\{\mathcal{L}_2 = \mathcal{L}_y, \mathcal{L}_1 = \mathcal{L}_{yx}\}$. If $q \geq 3$, we have also $s_1 - e_1 - e_2, s_3 - e_1y_1 - e_2y_2, s_6 - e_1y_1^2 - e_2y_2^2 \in H$, so we have that

$(s_1 - e_1 - e_2)^2, (s_3 - e_1 y_1 - e_2 y_2)^2, (e_6 - e_1 y_1^2 - e_2 y_2^2)^2 \in \widetilde{H}$ for (8.24). Again, we pass from variables to values, and we obtain

$$\bar{s}_1 = \bar{e}_1 + \bar{e}_2, \quad \bar{s}_3 = \bar{e}_1 \bar{y}_1 + \bar{e}_2 \bar{y}_2, \quad \bar{s}_6 = \bar{e}_1 \bar{y}_1^2 + \bar{e}_2 \bar{y}_2^2 \tag{8.26}$$

and that

$$\bar{A} = A(\bar{S}) = -(\bar{x}_1 + \bar{x}_2), \quad \bar{B} = B(\bar{S}) = \bar{x}_1 \bar{x}_2 \,.$$

So

$$-(\bar{x}_1 + \bar{x}_2)(\bar{e}_1 \bar{y}_1 + \bar{e}_2 \bar{y}_2) + \bar{y}_1 \bar{y}_2 (\bar{e}_1 + \bar{e}_2) = -(\bar{e}_1 \bar{y}_1^2 + \bar{e}_2 \bar{y}_2^2) \implies \bar{A} s_3 + \bar{B} s_1 = -s_6 \,.$$

The last part of theorem comes from direct computations, as follows.
From (8.25), in the case $\bar{s}_1 = \bar{s}_2 = 0$, we note $\bar{e}_1 = -\bar{e}_2$, $\bar{x}_1 = \bar{x}_2$. And so

1. If $p = 2$ then $\bar{a} = -(\bar{x}_1 + \bar{x}_2) = 2\bar{x}_1 = 0$ and $\bar{b} = \bar{x}_1 \bar{x}_2 = \bar{x}_1^2$.
2. If $p \neq 2$ then $\bar{a} = -(\bar{x}_1 + \bar{x}_2) = 2\bar{x}_1 \implies \bar{x}_1 = \frac{\bar{a}}{2}$.

From (8.26), if $s_1 = s_3 = 0$ then $e_1 = -e_2$ and $y_1 = y_2$. And thus

1. If $p = 2$ then $\bar{A} = 0$ e $\bar{B} = y_1^2$.
2. If $p \neq 2$ then $\bar{A} = 2y_1 \implies y_1 = \frac{A}{2}$ and $\bar{B} = y_1^2$.

Since in the proof so far we have used the relations on the syndromes coming from the non-stuffed ideal H, everything that we proved up to now holds also for the weak locators. □

The locator $\mathcal{P}_2$ computed for the Hermitian code with $q = 3$ and $t = 2$ is indeed of the form $\mathcal{P}_2 = \mathcal{P}_x = x^2 + ax + b$, with $|a| = 82$ and $|b| = 91$, so, for example when $s_1 \neq 0$, it is enough to evaluate $a(\bar{S})$ and then we obtain $b(\bar{S})$ as

$$b(\bar{S}) = -\frac{s_4 + a(\bar{S}) s_2}{s_1}.$$

Also $\mathcal{P}_1$ is as above, that is, of the form $\mathcal{P}_1 = \mathcal{P}_{xy} = y^2 + cy + d$.

Regrettably, we have not been able to compute explicitly $\mathcal{L}_2$ and $\mathcal{L}_1$ for $q = 3$, due to the high computation cost of the stuffing procedure.

Part III

Programs and Computations

Hermitian curve and Hermitian code

In this chapter we want to verify our formulas for the number of small weight codewords and for the intersection of Hermitian curve and parabolas. For these reason, we report some programs and results.

As software packages we used Singular and MAGMA [GPS07, MAG].

9.1 MAGMA programs to compute intersection between $\mathcal{H}$ and parabolas.

Here we report the MAGMA program that count the number of intersection between $\mathcal{H}$ and three types of parabolas.

```
q:=8;
K<u>:=GF(q^2);
Kpos:={c : c in K | c ne 0};

/////////Trace Function
Tr:=function(c)
return(c^q+c);
end function;

/////////Norm Function
N:=function(a)
return(a^(q+1));
end function;
//All c that have Tr(c)=0
Trnulla:={@@};
time for c in K do
 if Tr(c) eq 0 then
   Trnulla:=Include(Trnulla,c);
 end if;
end for;
```

```
#Trnulla;
TrNONzero:={c : c in K | c notin Trnulla};

////////Intersection between y=ax^2+bx+c and Hermitian curve
fabc:=function(a,b,c)
local count;
count:=0;
for x in K do
   for y in K do
      if ( N(x) eq Tr(y)) and (y eq a*x^2+b*x+c) then
      count:=count+1;
      end if;
   end for;
end for;
return(count);
end function;

///////Intersection between y=ax^2+c and Hermitian curve
f:=function(a,c)
local count;
count:=0;
for x in K do
    for y in K do
        if (x^(q+1) eq y^q+y) and (y eq a*x^2+c) then
        count:=count+1;
        end if;
    end for;
end for;
return(count);
end function;

 ////////Intersection between y=ax^2 and Hermitian curve
fa:=function(a)
local count;
count:=0;
for x in K do
    for y in K do
        if ( N(x) eq Tr(y)) and (y eq a*x^2) then
        count:=count+1;
        end if;
    end for;
end for;
return(count);
end function;
```

```
//Number of intersection y=ax^2
INTa:=[];
time for a in K do
 if a ne 0 then
sa:=fa(a);
   INTa:=Append(INTa,sa);
  end if;
end for;
#INTa;

int0a:=0;
int1a:=0;
intQm1a:=0;
intQa:=0;
intQp1a:=0;
int2Qm1a:=0;
int2Qa:=0;

for i in [1..#INTa] do
     if INTa[i] eq 0 then
        int0a:=int0a+1;
     else if INTa[i] eq 1 then
        int1a:=int1a+1;
     else if INTa[i] eq q-1 then
        intQm1a:=intQm1a+1;
     else if INTa[i] eq q then
        intQa:=intQa+1;
     else if INTa[i] eq q+1 then
        intQp1a:=intQp1a+1;
     else if INTa[i] eq 2*q-1 then
        int2Qm1a:=int2Qm1a+1;
     else if INTa[i] eq 2*q then
        int2Qa:=int2Qa+1;
    end if;
    end if;
    end if;
    end if;
    end if;
    end if;
    end if;
end for;
```

```
//Number of intersection y=ax^2+bx+c
int0:=0;
int1:=0;
intQm1:=0;
intQ:=0;
intQp1:=0;
int2Qm1:=0;
int2Q:=0;
INTabc:=[];

time for a in K do
         if a ne 0 then
            for b in K do
             for c in K do
          sabc:=fabc(a,b,c);
              INTabc:=Append(INTabc,sabc);
             end for;
            end for;
         end if;
 end for;
#INTabc;

for i in [1..#INTabc] do
    if INTabc[i] eq 0 then
       int0:=int0+1;
    else if INTabc[i] eq 1 then
       int1:=int1+1;
    else if INTabc[i] eq q-1 then
       intQm1:=intQm1+1;
    else if INTabc[i] eq q then
       intQ:=intQ+1;
    else if INTabc[i] eq q+1 then
       intQp1:=intQp1+1;
    else if INTabc[i] eq 2*q-1 then
       int2Qm1:=int2Qm1+1;
    else if INTabc[i] eq 2*q then
       int2Q:=int2Q+1;
    end if;
    end if;
    end if;
    end if;
    end if;
    end if;
    end if;
    end if;
end for;
```

We report the results and the timing for some q, that are $q = 3, 5, 8$.

```
\\\\\\\\\\\\\\  q=3   \\\\\\\\\\\\\\\\\
> //Number of intersection y=ax^2
Time: 0.000
> #INTa;
8
> int0a;
0
> int1a;
0
> intQm1a;
0
> intQa;
4
> intQp1a;
0
> int2Qm1a;
4
> int2Qa;
0
```

```
\\\\\\\\\\\\\\  q=3   \\\\\\\\\\\\\\\\\
> //Number of intersection y=ax^2+bx+c
Time: 0.060
> #INTabc;
648
> int0;
36
> int1;
0
> intQm1;
216
> intQ;
252
> intQp1;
0
> int2Qm1;
108
> int2Q;
36
```

```
\\\\\\\\\\\\\\  q=5   \\\\\\\\\\\\\\\\\
> //Number of intersection y=ax^2
Time: 0.010
> #INTa;
24
> int0a;
0
> int1a;
6
> intQm1a;
0
> intQa;
6
> intQp1a;
0
> int2Qm1a;
12
> int2Qa;
0
```

```
\\\\\\\\\\\\\\  q=5   \\\\\\\\\\\\\\\\\
> //Number of intersection y=ax^2+bx+c
Time: 10.600
> #INTabc;
15000
> int0;
300
> int1;
750
> intQm1;
6000
> intQ;
3150
> intQp1;
3000
> int2Qm1;
1500
> int2Q;
300
```

```
\\\\\\\\\\\\\\  q=8   \\\\\\\\\\\\\\\\  \\\\\\\\\\\\\\  q=8   \\\\\\\\\\\\\\\\
//Number of intersection y=ax^2         //Number of intersection y=ax^2+bx+c
Time: 0.240                             Time: 1393.720
> #INTa;                                > #INTabc;
63                                      258048
> int0a;                                > int0;
0                                       0
> int1a;                                > int1;
27                                      13824
> intQm1a;                              > intQm1;
0                                       129024
> intQa;                                > intQ;
0                                       0
> intQp1a;                              > intQp1;
0                                       96768
> int2Qm1a;                             > int2Qm1;
36                                      18432
> int2Qa;                               > int2Q;
0                                       0
```

9.2 MAGMA programs to compute the number of minimum-weight words of Hermitian code.

The command `HermitianCode(q,m)` is use in magma to find n, k, d and generator matrix of an Hermitian code in $\mathbb{F}_{q^2}$. For example

```
> q:=3;
> K<u>:=GF(q^2);
> HermitianCode(q,5);
[27, 3, 23] Linear Code over GF(3^2)
Generator matrix:
[1 0 2 0 u u^6 u^7 2 1 u^3 u 0 1 u^2 u^2 u^2 u^2 u^7 0 u^7 u^5 2 u u^7 2 1 u]
[0 1 2 0 2 u u^2 u^2 2 u^2 u^7 u^3 u^5 u^2 1 u^7 0 u u 2 u^7 1 1 0 u^6 u^7 u]
[0 0 0 1 u^6 2 u^2 u^3 1 2 u^7 u u u^7 u^6 u^2 u^5 u^7 u^3 u^5 2 1 u^5 u^6 u u^3 u^2]
```

Now we report the number of minimum weight codewords of some Corner and Edge codes. To do these we use the following commands:

```
C:=HermitianCode(3,5);
D:=Dual(C);
d:=MinimumDistance(D);
WeightDistribution(D);
```

The command `WeightDistribution(D)` gives us a sequence of couples `<a,b>`, where `b` is the number of words having weight `a`. In the following example, we want to verify Theorem 7.3.2 and Theorem 7.3.4, in two special cases, which are $q = 3$ and $q = 7$.

```
/////////////      q=3        /////////////

//         m=2 --->   Corner Code
> MinimumDistance(D);
2
> WeightDistribution(D);
[ <0, 1>, <2, 2808>, <3, 163800>, ... ]
> q^2*(q^2-1)*Binomial(q,d-1)*(q^3-d+1)/d;
2808

//          m=3 --->   Edge Code
> MinimumDistance(D);
2
> WeightDistribution(D);
[ <0, 1>, <2, 216>, <3, 18648>, ... ]
> q^2*(q^2-1)*Binomial(q,d);
216

//          m=4,5 --->   Corner Code
> MinimumDistance(D);
3
> WeightDistribution(D);
[ <0, 1>,  <3, 1800>, <4, 101088>, ... ]
> q^2*(q^2-1)*Binomial(q,d-1)*(q^3-d+1)/d;
1800

//          m=6 --->   Edge Code
> MinimumDistance(D);
3
> WeightDistribution(D);
[ <0, 1>,  <3, 72>, <4, 11664>, ... ]
> q^2*(q^2-1)*Binomial(q,d);
72

//          m=7 --->   Edge Code
> MinimumDistance(D);
3
> WeightDistribution(D);
[ <0, 1>,  <3, 72>, <4, 432>, ... ]
> q^2*(q^2-1)*Binomial(q,d);
72
```

```
/////////////      q=7        /////////////

//           m=1,..,6  --->   Corner Code
> WeightDistribution(D)[2];
<2, 2815344>
> WeightDistribution(D)[3];
<3, 15040506096>
> q^2*(q^2-1)*Binomial(q,d-1)*(q^3-d+1)/d;
2815344
//            m=7 --->   Edge Code
> WeightDistribution(D)[2];
<2, 49392>
> WeightDistribution(D)[3];
<3, 307201776>
> q^2*(q^2-1)*Binomial(q,d);
49392
//            m= 8,..13 --->   Corner Code
> WeightDistribution(D)[2];
<3, 246000>
> WeightDistribution(D)[3];
<4, 207156000>
> q^2*(q^2-1)*Binomial(q,d-1)*(q^3-d+1)/d;
246000
//            m=14 --->   Edge Code
> WeightDistribution(D)[2];
<3, 82320>
> WeightDistribution(D)[3];
<4, 549140256>
> q^2*(q^2-1)*Binomial(q,d);
82320
//            m=15 --->   Edge Code
> WeightDistribution(D)[2];
<3, 82320>
> WeightDistribution(D)[3];
<4, 10701600>
//            m=16,..,20 --->   Corner Code
> WeightDistribution(D)[2];
<4, 6997200>
> WeightDistribution(D)[3];
<5, 251158320>
> q^2*(q^2-1)*Binomial(q,d-1)*(q^3-d+1)/d;
6997200
```

9.3 Singular programs to compute the number of words of weight $d+1$.

In this section, using Singular, we want to verify some results of Section 7.4. The verification has been done by computing a Gröbner basis of ideal J_w as in Proposition 4.2.1 for the corresponding case, when $q = 3$.

```
////////////////    q=3     ////////////////////////
//=============================================================================//
//         m=3 --->   Edge Code
//=============================================================================//

//We count the number of minimum words.
ring R=3,(y1,x1,y2,x2,z2,z1),dp;
ideal I=x1^9-x1,x2^9-x2,y1^9-y1,y2^9-y2,
z1^8-1, z2^8-1,
z1+z2,
z1*x1+z2*x2,
( (x1-x2)^8-1) * ( (y1-y2)^8-1),
x1^4-y1^3-y1,
x2^4-y2^3-y2;

ideal G=std(I);
> G;
G[1]=z2+z1
G[2]=x1-x2
G[3]=y1^2+y1*y2+y2^2+1
G[4]=x2^4-y2^3-y2
G[5]=y2^6*x2-y2^4*x2+y2^2*x2-x2
G[6]=z1^8-1
G[7]=y2^9-y2
> vdim(G);
432
//the number of minimum words is 432/2!=216

//=============================================================================//

//We count the number of words having weight d+1.
ring R=3,(y1,x1,y2,x2,y3,x3,z3,z2,z1),dp;
int q=3;
int d=2;
ideal I=x1^9-x1,x2^9-x2,y1^9-y1,y2^9-y2,
x3^9-x3,y3^9-y3,
z1^8-1, z2^8-1, z3^8-1,
z1+z2+z3,
z1*x1+z2*x2+ z3*x3,
```

```
( (x1-x2)^8-1) * ( (y1-y2)^8-1),
( (x1-x3)^8-1) * ( (y1-y3)^8-1),
( (x3-x2)^ 8-1) * ( (y3-y2)^8-1),
x1^4-y1^3-y1,
x2^4-y2^3-y2,
x3^4-y3^3-y3;
ideal G=std(I);
> vdim(G);
111888
//The number of words having weight d+1=3 is 111888/3!=18648

//=============================================================================//

//We count the number of words having weight d+1=3 and all the x's equal.
ideal I1=I,x1-x2,x1-x3;
ideal G1=std(I1);
vdim(G1);
> vdim(G1);
3024

//The number of words having weight d+1=3 and all the x's are equal is 3024/3!=504
//Verify using MAGMA:
q:=3;
d:=2;
> (q^2)*(q^4-(d+1)*q^2+d)*Binomial(q,d+1);
504
> 3024/6;
504

//=============================================================================//

//We count the number of words having weight d+1=3 and all the y's are equal
ideal I2=I,y1-y2,y1-y3;
ideal G2=std(I2);
vdim(G2);
> vdim(G2);
1152

//The number of words having weight d+1=3 and all the y's are equal is 1152/3!=192
//Verify using MAGMA:
> (q^2-q)*(q^2-1)*Binomial(q+1,d+1);
192
> 1152/6;
192
```

```
//=============================================================================//
//          m=4,5 --->   Corner Code
//=============================================================================//
ring R=3,(y1,x1,y2,x2,y3,x3,y4,x4,z4,z3,z2,z1),dp;
int q=3;
int d=3;
ideal I=x1^9-x1,x2^9-x2,y1^9-y1,y2^9-y2,
x3^9-x3,y3^9-y3,x4^9-x4,y4^9-y4,
z1^8-1, z2^8-1, z3^8-1,  z4^8-1,
z1+z2+ z3+z4,
z1*x1+z2*x2+ z3*x3+z4*x4,
z1*y1+z2*y2+ z3*y3+z4*y4,
( (x1-x2)^8-1) * ( (y1-y2)^8-1),
( (x1-x3)^8-1) * ( (y1-y3)^8-1),
( (x3-x2)^ 8-1) * ( (y3-y2)^8-1),
( (x1-x4)^ 8-1) * ( (y1-y4)^ 8-1),
( (x4-x2)^ 8-1) * ( (y4-y2)^ 8-1),
( (x3-x4)^ 8-1) * ( (y3-y4)^ 8-1),
x1^4-y1^3-y1,
x2^4-y2^3-y2,
x3^4-y3^3-y3,
x4^4-y4^3-y4;

///We count the number of words having weight d+1=3 and all the x's are equal.
///We know that is 3024/3!=504 = (q^2)*(q^4-(d+1)*q^2+d)*Binomial(q,d+1)
ideal I1=I,x1-x2,x1-x3,x1-x4;
ideal G1=std(I1);
vdim(G1);

> vdim(G1);
3024
> 3024/6;
504

//=============================================================================//

///We count the number of words having weight d+1=3 and all the y's are equal.
///We know that is 182/3!=192 = (q^2-q)*(q^2-1)*Binomial(q+1,d+1)
ideal I2=I,y1-y2,y1-y3;
ideal G2=std(I2);
vdim(G2);

> vdim(G2);
182
> 182/6;
192
```

Decoding affine–variety code

In this chapter we report Singular [GPS07] programs needed to find the multi-dimensional general error locators of the Hermitian code $C = C^{\perp}(I, L)$ over $\mathbb{F}_4$. In particular we following step by step our main example providing results and programs. In Section 10.2, we report a program used to stuffed our ideal $J_*^{C,t}$.

10.1 Singular programs to find weak locators.

We analyse the decoding of Hermitian codes following the main example, that is, the Hermitian code $C = C^{\perp}(I, L)$ from the curve $y^2 + y = x^3$ over $\mathbb{F}_4$ and with defining monomials $\{1, x, y, x^2, xy\}$.

We start with Example 8.2.3 writing ideal $J_*^{C,t}$ and computing the Gröbner basis $\mathcal{G}$ using the command `G=std(I)`.

```
> ring R=(4,a),(e1,e2,y1,x1,y2,x2,s5,s4,s3,s2,s1),lp;
> ideal I=x1^4-x1,x2^4-x2,y1^4-y1,y2^4-y2,e1^4-e1,e2^4-e2,
  y1^2*x1+y1^2+y1*x1+y1+x1^3+x1,
  y2^2*x2+y2^2+y2*x2+y2+x2^3+x2,
  y1^3+y1*x1^3+y1+x1^3,
  y2^3+y2*x2^3+y2+x2^3,
  e1+e2-s1,
  e1*x1+e2*x2-s2,
  e1*y1+e2*y2-s3,
  e1*x1^2+e2*x2^2-s4,
  e1*x1*y1+e2*x2*y2-s5,
  e1*e2*( (x1-x2)^3-1) * ( (y1-y2)^3-1),
  e1*( (x1-1)^3-1) *( (y1-1)^3-1 ),
  e2*( (x2-1)^3-1) *( (y2-1)^3-1 ),
 (e1^3-1)*(x1-1),
 (e1^3-1)*(y1-1),
 (e2^3-1)*(x2-1),
 (e2^3-1)*(y2-1);
> option(redTail);
> option(redSB);
> ideal  G=std(I);
//used time: 30.88 sec
```

The two commands `option(redTail)` and `option(redSB)` is needed to reduce a Gröbner basis. To find the two multi-dimensional general error locator polynomials $\mathcal{L}_x = \mathcal{L}_{2,1}(s_1, \ldots, s_5, x_2)$ and $\mathcal{L}_{xy} = \mathcal{L}_{2,2}(s_1, \ldots, s_5, x_2, y_2)$, we have to see the leading term of $g \in \mathcal{G}$:

```
  > lead(G);
 _[1]=s1^4
 _[2]=s2^4
 _[3]=s3^4
 _[4]=s4*s2^3*s1^3
 _[5]=s4^3*s1^3
 _[6]=s4^4
 _[7]=s5*s1
 _[8]=s5*s3^3*s2^3
 _[9]=s5*s4*s2^3
 _[10]=s5*s4^3
 _[11]=s5^2*s2
 _[12]=s5^2*s3^3
 _[13]=s5^2*s4
 _[14]=s5^4
 _[15]=x2*s2^3*s1^3
 _[16]=x2*s4^3*s2^3
 _[17]=x2*s4^3*s3^2
 _[18]=x2*s5*s2^3
 _[19]=x2*s5^2
 _[20]=x2^2
 _[21]=y2*s2*s1^3
 _[22]=y2*s3^2*s2
 _[23]=y2*s3^3*s1^3
 _[24]=y2*s4
 _[25]=y2*s5*s2
 _[26]=y2*s5*s3^3
 _[27]=y2*x2
 _[28]=y2^2
 _[29]=x1
 _[30]=y1
 _[31]=e2
 _[32]=e1
```

Hence $\mathcal{L}_x$ is `G[20]` and $\mathcal{L}_{xy}$ is `G[28]`:

```
>  poly Lx=G[20];
>  Lx;
x2^2+s1^2*s2*s4^3*x2+s4^3*x2+s1*s2^3*s4^2*x2+s1^2*s2^2*s4^2*x2+s1*s4^2*x2+s2^2*s4*x2+s1*s2*s4*x2+
s2^3*x2+s1^2*s2*x2+s1^3*x2+s3*s5^2+s2*s3*s5+s1*s2^2*s4^3+s1^2*s2*s4^3+s2*s3^3*s4^2+s1*s2*s3^2*s4^2+
s1^2*s2*s3*s4^2+s1*s2^3*s4^2+s1^3*s2*s4^2+s2*s4^2+s1^2*s3^3*s4+s1^3*s3^2*s4+s1*s3*s4+s1^2*s2^3*s4+
s1^3*s2^2*s4+s1^2*s4+s1^3*s2^3*s3^3+s2^3*s3^3+s1*s2^2*s3^3+s1^3*s3^3+s3^3+s1^2*s2^2*s3^2+s1^3*s2^2*s3+
s2^2*s3+s1^3*s2^3+s2^3+s1*s2^2+s1^3+1

>  poly Lxy=G[28];
>  Ly;
y2^2+s3^3*y2+s1*s3^2*y2+s1^2*s2^3*s3*y2+s1^2*s3*y2+s1^3*y2+s2^2*s3*s4^3*x2+s1*s2^2*s4^3*x2+
s1^2*s2*s3*s4^2*x2+s1^2*s3^3*s4*x2+s3^2*s4*x2+s1*s3*s4*x2+s1^2*s2^3*s4*x2+s5^3+s2*s3^2*s4^2*s5+
s3*s4*s5+s2^2*s5+s3^3*s4^3+s1*s2^3*s3^2*s4^3+s2^3*s4^3+s1^2*s2^2*s3^3*s4^2+s1^2*s2*s3^2*s4+
s1^3*s2*s3*s4+s1*s2*s4+s2^3*s3^3+s3^3+s1*s2^3*s3^2+s1^2*s2^3*s3+s1^2*s3+s1^3*s2^3+s1^3+1
```

These two polynomials are exactly the two weak multi-dimensional general error locators that we find at page 104. To evaluate the polynomials in the syndrome (and the variable x if it is necessary) we just use the command `subst( )`

```
// Occur 2 errors in P6=(a,a+1) e P7=(a+1,a) --> The syndrome is s = (0,1,1,1,0).
> subst(Lx,s1,0,s2,1,s3,1,s4,1,s5,0);
x2^2+x2+1
> subst(Lxy,s1,0,s2,1,s3,1,s4,1,s5,0,x2,a+1);
y2^2+y2+1
> subst(Lxy,s1,0,s2,1,s3,1,s4,1,s5,0,x2,a);
y2^2+y2+1

// Occur 2 errors in P1=(0,0) e P2=(0,1) --> The syndrome is s=(a+1,0,a,0,0)
> subst(Lx,s1,a+1,s2,0,s3,a,s4,0,s5,0);
```

```
x2^2+x2
> subst(Lxy,s1,a+1,s2,0,s3,a,s4,0,s5,0,x2,1);
y2^2+y2
> subst(Lxy,s1,a+1,s2,0,s3,a,s4,0,s5,0,x2,0);
y2^2+y2

// Occur only one error. --> The syndrome is s=(a+1,a+1,1,a+1,1)
> subst(Lx,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1);
x2^2+1
> subst(Lxy,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1,e2,a+1,x2,1);
y2^2+a^2*y2+a
```

To find the general error evaluator polynomial $\mathcal{E}(S, e)$ (see Definition 8.2.6) we just change the ordering as in Example 8.2.8 in this way (we do not report the ideal since it is as above).

```
> ring R=(4,a),(e1,y1,x1,y2,x2,e2,s5,s4,s3,s2,s1),lp;
...
> ideal  G=std(I);
//used time: 72.28 sec
> size(G);
33
> lead(G);
```

```
_[1]=s1^4                  _[12]=s5^2*s3^3            _[23]=x2^2
_[2]=s2^4                  _[13]=s5^2*s4              _[24]=y2*s1
_[3]=s3^4                  _[14]=s5^4                 _[25]=y2*s2
_[4]=s4*s2^3*s1^3          _[15]=e2*s1^3              _[26]=y2*s3^3
_[5]=s4^3*s1^3             _[16]=e2*s5                _[27]=y2*s4
_[6]=s4^4                  _[17]=e2^2                 _[28]=y2*e2
_[7]=s5*s1                 _[18]=x2*s1                _[29]=y2*x2
_[8]=s5*s3^3*s2^3          _[19]=x2*s2^3              _[30]=y2^2
_[9]=s5*s4*s2^3            _[20]=x2*s4^3              _[31]=x1
_[10]=s5*s4^3              _[21]=x2*s5^2              _[32]=y1
_[11]=s5^2*s2              _[22]=x2*e2                _[33]=e1
```

So the general error evaluator polynomial $\mathcal{E}(S, e)$ is `G[17]`

```
> poly E=G[17];
> E;
e2^2+e2*s1+s4^3*s3^2+s4^3*s3*s1+s4^3*s2^3*s1^2+s4^3*s1^2+s4^2*s3^2*s2^2*s1^2+
s4^2*s3*s2^2*s1^3+s4*s3^2*s2*s1+s4*s3*s2*s1^2+s4*s2*s1^3+s4*s2+s3^2*s2^3*s1^3+
s3^2+s3*s2^3*s1+s3*s1+s2^3*s1^2;
```

and two weak multi-dimensional general error locator polynomials with error $\mathcal{P}_x^e = f_x$ =G[23] and g_x =G[31]. Changing again the ordering, we find the other two polynomials, that are $\mathcal{P}_y^e = f_y$ =G[23] and g_y =G[33].

```
 >  ring Q=(4,a),(e1,y1,x1,x2,y2,e2,s5,s4,s3,s2,s1),lp;
 >   ideal I=imap(R,G);
 >   ideal G=std(I);
 >   size(G);
 34
```

The explicit polynomials can be found at Appendix at page 167. Finally, we evaluate these polynomial in the usual way.

```
// Occur 2 errors in P6=(a,a+1) e P7=(a+1,a)
> subst(E,s1,0,s2,1,s3,1,s4,1,s5,0);
e2^2+1
> subst(Pey,s1,0,s2,1,s3,1,s4,1,s5,0,e2,1);
y2^2+y2+1 -
> subst(Pex,s1,0,s2,1,s3,1,s4,1,s5,0,e2,1);
x2^2+x2+1

// Occur 2 errors. The syndrome is s=(a+1,0,a,0,0)
> subst(E,s1,a+1,s2,0,s3,a,s4,0,s5,0);
e2^2+a^2*e2+a
> subst(Pey2,s1,a+1,s2,0,s3,a,s4,0,s5,0,e2,1);
y2^2+y2
> subst(Pey2,s1,a+1,s2,0,s3,a,s4,0,s5,0,e2,a);
y2^2+y2
> subst(Pex,s1,a+1,s2,0,s3,a,s4,0,s5,0,e2,1);
x2^2
> subst(Pex,s1,a+1,s2,0,s3,a,s4,0,s5,0,e2,a);
x2^2

// Occur only one error. The syndrome is s=(a+1,a+1,1,a+1,1)
> subst(E,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1);
e2^2+a^2*e2
> subst(gy,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1,e2,a+1,y2,1);
y1+a
> subst(gx,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1,e2,a+1,x2,1);
x1+1
```

10.2 Singular programs to find the locators.

In this section, we analyse Example 8.5.3 and a method to stuff the ideal.
That is, we find the *multi-dimensional general error locator polynomials* $\mathcal{L}_x$ and $\mathcal{L}_{xy}$

stuffing the ideal $J_*^{C,t}$.

```
LIB "general.lib";
LIB "matrix.lib";
ring r1 = (2,a),(s1,s2,s3,s4,s5,x2),rp;
minpoly= a^2+a+1;
string s=read("Base_G2X")+";";
execute(s);
ring r = (2,a),x(1..7),rp;
minpoly= a^2+a+1;
map f = r1,x(1),x(2),x(3),x(4),x(5),x(6),x(7);
ideal GGX=f(G2X);

//Compute the hasse derivative
proc hasse (poly f,int n)
{ intvec v=0,0,0,0,0,1,0;
  poly g = 0;
  poly g1= 0;
  poly g2 = 0;
  poly f1=f;
  while(deg(f1,v)>n-1)
  { g1=lead(f1);
      if (deg(g1,v) == 0)
      { f1=f1-g1;}
      else
      { g2=coef(g1,x(6))[2,1]*x(6)^(deg(g1,v)-n);
    g2=coeffs((x(1)+1)^(deg(g1,v)),x(1))[n+1,1]*g2;
    f1=f1-g1;
    g=g+g2;
}
   }
  return(g);
};

proc n_functional (ideal I,i1,i2,i3,i4,i5,j,int ndiff)
{
   ideal J=I;
   int n;
   int r;
   int m =ncols(J);
   poly val =0;
   poly pp;
   poly gstar=0;
   n=0;
   while ((val==0) and (n <m))
   { n=n+1;
     pp=J[n];
```

```
     val= subst(hasse(subst(pp,x(1),i1,x(2),i2,x(3),i3,x(4),i4,x(5),i5),ndiff),x(6),j);
    }
    if (val!=0)
    { n;
      gstar= subst(pp,x(1),i1,x(2),i2,x(3),i3,x(4),i4,x(5),i5,x(6),j);
      return(n,val,gstar);
    }
 return(0) ;
 };

proc HnFunc(poly f,i1,i2,i3,i4,i5,j, int ndiff)
{ int k;
  poly val =subst(f,x(1),i1,x(2),i2,x(3),i3,x(4),i4,x(5),i5);
  val= hasse(val,ndiff);
  val =subst(val,x(6),j);
  val;
  if (val!=0){ return(val);}
  return(0);
};

//Use Buchberger-Moeller algorithm
proc HBM_func (ideal I, i1,i2,i3,i4,i5,j, int ndiff)
{ int k;
  ideal J;
  ideal T=I;
  def n,Hgs,gs = n_functional (I,i1,i2,i3,i4,i5,j,ndiff);
  if (n==0){ return(T);}
  else
  { int m =ncols(T);
    poly a;
    for(k=1;k<n;k=k+1)
     {J=J,T[k];}
    J=J,(T[n])*(x(1)-i1),(T[n])*(x(2)-i2),(T[n])*(x(3)-i3),
    (T[n])*(x(4)-i4),(T[n])*(x(5)-i5);
    poly p= gs-j*Hgs+x(7)*Hgs;
    if(jet(p,0)==0)
  {J=J,(I[n])*(x(6));}
    else
  {J=J,(T[n])*(x(6)+((coef(p,x(7))[2,2])/(coef(p,x(7))[2,1])));}
    for(k=n+1;k<=m;k=k+1)
     { def Divg = HnFunc((T[k]),i1,i2,i3,i4,i5,j,ndiff)/HnFunc((T[n]),i1,i2,i3,i4,i5,j,ndiff);
       a=I[k]-(Divg*I[n]);
       J=J,a;
     }
     return(J);
   }
```

```
};

matrix E[8][36]=0;
matrix B [2][9]=1,1,1,a,a,a,a+1,a+1,a+1,1,a,a+1,1,a,a+1,1,a,a+1;
int j;
for(j=0;j<4;j=j+1)
{ E[1+j*2,1+9*j..9*(j+1)]=B[1,1..9];
  E[2+j*2,1+9*j..9*(j+1)]=B[2,1..9];
};

matrix H[5][8] = 1,1,1,1,1,1,1,1,0,0,1,1,a,a,a+1,a+1,0,1,a,
a+1,a,a+1,a,a+1,0,0,1,1,a+1,a+1,a,a,0,0,a,a+1,a+1,1,1,a;
matrix S=H*E;
matrix VS[6][36];
VS[1..5,1..36]=S;

int i;
  for(i=1;i<=9;i=i+1)
   { VS[6,i]=0;}
  for(i=10;i<=18;i=i+1)
   { VS[6,i]=1;}
  for(i=19;i<=27;i=i+1)
   { VS[6,i]=a;}
  for(i=28;i<=36;i=i+1)
   { VS[6,i]=a+1;}

proc add_points(matrix A, ideal I)
{ int n = ncols(A);
  ideal J=I;
  int i;
  for(i=1;i<=n;i=i+1)
   {J= HBM_func(J,A[1,i],A[2,i],A[3,i],A[4,i],A[5,i],A[6,i],1);
    J=interred(J);i;
    }
  return(J);
};

timer=1;
ideal J= add_points(VS,GGX);
ring r2 = (2,a),(s1,s2,s3,s4,s5,x2),rp;
minpoly= a^2+a+1;
map ff=r,s1,s2,s3,s4,s5,x2;
ideal JJ=ff(J);
ideal JJrid=std(JJ);
write(":w G2X_FINITA", "ideal G2X=", JJrid);
```

```
// We stuff the ideal adding ghost point

LIB "general.lib";
LIB "matrix.lib";
ring r1 = (2,a),(s1,s2,s3,s4,s5,x2),rp;
minpoly= a^2+a+1;
string s=read("G2X_FINITA")+";";
execute(s);
ring r = (2,a),x(1..7),rp;
minpoly= a^2+a+1;
map f = r1,x(1),x(2),x(3),x(4),x(5),x(6),x(7);

ideal GGX=f(G2X);

...

//construct matrix E
matrix E[2][6]=1,a,a+1,0,0,0,0,0,0,1,a,a+1;
matrix H[5][2] = 1,1,1,1,a,a+1,1,1,a,a+1;
matrix S=H*E;
matrix VS[6][6]=0;
VS[1..5,1..6]=S;

int i;
for(i=1;i<7;i=i+1)
 { VS[6,i]=1;}

proc add_points(matrix A, ideal I)
 {int n = ncols(A);
  ideal J=I;
  int i;
  for(i=1;i<=n;i=i+1)
   { J= HBM_func(J,A[1,i],A[2,i],A[3,i],A[4,i],A[5,i],A[6,i],1);
     J=interred(J);i;
    }
  return(J);
 };

timer=1;
ideal J=add_points(VS,GGX);
ring r2 = (2,a),(s1,s2,s3,s4,s5,x2),rp;
minpoly= a^2+a+1;
map ff=r,s1,s2,s3,s4,s5,x2;
ideal JJ=ff(J);
ideal JJrid=std(JJ);
write(":w G2X_ghostTOT", "ideal G2XT=", JJrid);
```

The two locators that we found in Example 8.5.3 are $\mathcal{L}_x$ =G[20] and $\mathcal{L}_{xy}$ =G[23]:

```
> ring R=(4,a),(e1,e2,y1,x1,y2,x2,s5,s4,s3,s2,s1),lp;
> string s=read("G2XY_ghostTOT")+";";
> execute(s);
> ideal G=G2XY;
```

```
> lead(G);
_[1]=s1^4
_[2]=s2^4
_[3]=s3^4
_[4]=s4*s2^3*s1^3
_[5]=s4^3*s1^3
_[6]=s4^4
_[7]=s5*s1
_[8]=s5*s3^3*s2^3
_[9]=s5*s4*s2^3
_[10]=s5*s4^3
_[11]=s5^2*s2
_[12]=s5^2*s3^3
_[13]=s5^2*s4
_[14]=s5^4
_[15]=x2*s2^3*s1^3
_[16]=x2*s4^3*s2^3
_[17]=x2*s4^3*s3^2
_[18]=x2*s5*s2^3
_[19]=x2*s5^2
_[20]=x2^2
_[21]=y2*s3^3*s2^3*s1^3
_[22]=y2*x2
_[23]=y2^2
```

```
> poly Lx=G[20];
> poly Lxy=G[23];

//Compute error values and locations
//Occur 2 errors in P6=(a,a+1) e P7=(a+1,a)
> subst(Lx,s1,0,s2,1,s3,1,s4,1,s5,0);
x2^2+x2+1
> subst(Lxy,s1,0,s2,1,s3,1,s4,1,s5,0,x2,a+1);
y2^2+a^2
> subst(Lxy,s1,0,s2,1,s3,1,s4,1,s5,0,x2,a);
y2^2+a

//Occur 2 errors. The syndrome is s=(a+1,0,a,0,0)
> subst(Lx,s1,a+1,s2,0,s3,a,s4,0,s5,0);
x2^2
> subst(Lxy,s1,a+1,s2,0,s3,a,s4,0,s5,0,x2,0);
y2^2+y2

//Occur only one error. The syndrome is s=(a+1,a+1,1,a+1,1)
> subst(Lx,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1);
x2^2+1
> subst(Lxy,s1,a+1,s2,a+1,s3,1,s4,a+1,s5,1,e2,a+1,x2,1);
y2^2+a^2*y2+a
```

Appendix - Some locator polynomials

In Example 8.2.1 we have the following polynomial

$$\begin{aligned}\mathcal{L}_{xy} =&\mathbf{y}^2+\mathbf{y}(2s_4^6+2s_4^5s_3+2s_4^5s_2s_1^6-2s_4^5s_2+2ys_4^4s_3^2-2s_4^4s_2^2+2s_4^4s_2s_1+2s_4^3s_3^3-2s_4^3s_2^3+2s_4^3s_2s_1^2+\\&2s_4^2s_3^4-2s_4^2s_2^4+2s_4^2s_2s_1^3+2s_4s_3^5-s_4s_3s_2^4-s_4s_3s_2s_1^3+2s_4s_3s_1^4-s_4s_2^5+s_4s_2s_1^4-2s_3^6+2s_3^5s_2s_1^6-\\&2s_3^5s_2+2s_3^4s_2^2-2s_3^4s_2s_1+3s_3^3s_2^3-3s_3^3s_2s_1^2+3s_3^2s_2^6s_1^4+2s_3^2s_2^5s_1^5-3s_3^2s_2^4s_1^6-s_3^2s_2^4+2s_3^2s_2^3s_1-\\&s_3^2s_2^2s_1^2-2s_3^2s_1^4-s_3s_2^6s_1^5+s_3s_2^5s_1^6+s_3s_2^4s_1-2s_3s_2^3s_1^2+s_3s_2^2s_1^3-3s_2^6-s_2^5s_1-s_2^4s_1^2-s_2^3s_1^3-s_2^2s_1^4-\\&s_2s_1^5-s_1^6)-s_4^6s_3^6+2s_4^6s_2^6+3s_4^6s_2s_1^5-2s_4^6s_1^6-s_4^5s_3-s_4^5s_2s_1^6+s_4^5s_2-s_4^4s_3^2+s_4^4s_2^2-s_4^4s_2s_1-\\&s_4^3s_3^3+s_4^3s_2^3-s_4^3s_2s_1^2-s_4^2s_3^4+s_4^2s_2^4-s_4^2s_2s_1^3-s_4s_3^5+2s_4s_3s_2^4-s_4s_3s_1^4-s_4s_2^5+s_4s_2s_1^4-3s_3^6s_2^6+\\&2s_3^6s_2s_1^5-s_3^6s_1^6-s_3^6-2s_3^5s_2s_1^6+2s_3^5s_2+3s_3^3s_2^3-3s_3^3s_2s_1^2-s_3^2s_2^6s_1^4-s_3^2s_2^5s_1^5+s_3^2s_2^4s_1^6+3s_3^2s_2^3s_1-\\&s_3^2s_2^2s_1^2-3s_3^2s_2s_1^3+s_3^2s_1^4-3s_3s_2^6s_1^5+3s_3s_2^5s_1^6-3s_3s_2^5+2s_3s_2^4s_1+2s_3s_2^3s_1^2+s_3s_2^2s_1^3-2s_3s_2s_1^4+\\&2s_2^6s_1^6+2s_2^6+2s_2^5s_1+2s_2^4s_1^2+2s_2^3s_1^3+2s_2^2s_1^4+2s_2s_1^5.\end{aligned}$$

In Example 8.2.2 we the have following polynomial

$$\begin{aligned}\mathcal{L}_{xy} =&\mathbf{y}^2+\mathbf{y}(3s_4s_3s_2^4+2s_4s_3s_2s_1^3-3s_4s_2^5+3s_4s_2s_1^4+s_3^6-s_3^5s_2s_1^6+s_3^5s_2+s_3^4s_2^2-s_3^4s_2s_1+s_3^3s_2^3-\\&s_3^3s_2s_1^2-3s_3^2s_2^5s_1^5-s_3^2s_2^4s_1^6-2s_3^2s_2^4-2s_3^2s_2^3s_1-s_3^2s_2^2s_1^2-3s_3^2s_2s_1^3-s_3s_2^6s_1^5+2s_3s_2^5s_1^6-s_3s_2^4s_1-\\&2s_3s_2^3s_1^2-s_3s_2^2s_1^3+3s_3s_2s_1^4-3s_2^5s_1-3s_2^4s_1^2-3s_2^3s_1^3-3s_2^2s_1^4-3s_2s_1^5-3s_1^6-3)+\\&\mathbf{x}(2s_3^6+2s_2^6+3s_2s_1^5+s_1^6-3)+3s_4s_3s_2^4-3s_4s_3s_2s_1^3-2s_4s_3s_1^4-3s_4s_2^5+3s_4s_2s_1^4+2s_3^6s_2^6-\\&3s_3^6s_2s_1^5-3s_3^6s_1^6+3s_3^5s_2s_1^6-3s_3^5s_2-3s_3^4s_2^2+3s_3^4s_2s_1-3s_3^3s_2^3+3s_3^3s_2s_1^2+2s_3^2s_2^6s_1^4-s_3^2s_2^5s_1^5+\\&s_3^2s_2^4+s_3^2s_2^3s_1+s_3^2s_2^2s_1^2+3s_3^2s_2s_1^3+2s_3^2s_1^4-2s_3s_2^6s_1^5+3s_3s_2^5s_1^6+3s_3s_2^5-3s_3s_2^4s_1-3s_3s_2^3s_1^2-\\&2s_3s_2^2s_1^3-3s_3s_2s_1^4-2s_2^6s_1^6+3s_2^6-s_2^5s_1-s_2^4s_1^2-s_2^3s_1^3-s_2^2s_1^4+3s_2s_1^5.\end{aligned}$$

In Example 8.2.8 we have the following polynomials

$$\begin{aligned}f_x =&\mathbf{x}^2+\mathbf{x}s_4s_2^2+\mathbf{e}(s_4^3s_3^2s_2s_1^2+s_4^3s_3^2+s_4^3s_3s_2+s_4^3s_3s_1+s_4^3s_2^3s_1^2+s_4^3s_2^2+s_4^3s_1^2+s_4^2s_3^2s_2^3s_1+s_4^2s_3^2s_2^2s_1^2+\\&s_4^2s_3s_2^3s_1^2+s_4^2s_3s_2^2+s_4s_3^2s_2^2+s_4s_3s_2s_1^2+s_4s_2^3s_1+s_4s_1+s_3^2s_2^3+s_3^2+s_3s_2^3s_1+s_3s_1+s_2^3s_1^2+s_2^2+s_1^2)+\\&s_5^2s_3+s_5s_3s_2+s_4^3s_3^2s_2+s_4^3s_3^2s_1+s_4^3s_3s_2s_1+s_4^3s_3s_1^2+s_4^3s_2^2+s_4^3s_2^2s_1+s_4^3+s_4^2s_3^3s_2+s_4^2s_3^2s_2^3s_1^2+\\&s_4^2s_3^2s_2^2+s_4^2s_3^2s_2s_1+s_4^2s_3s_2^3+s_4^2s_3s_2^2s_1+s_4^2s_3s_2s_1^2+s_4^2s_2s_1^3+s_4^2s_2+s_4s_3^3s_1^2+s_4s_3^2s_2^2s_1+s_4s_3^2s_2s_1^2+\\&s_4s_3^2s_1^3+s_4s_3s_2^2s_1^2+s_4s_3s_2+s_4s_3s_1+s_3^3s_2^2s_1+s_3^2s_2^3s_1+s_3^2s_2^2s_1^2+s_3^2s_1+s_3s_2^3s_1^2+s_3s_2^2s_1^3+s_3s_2^2+\\&s_3s_1^2+s_2^3+s_2^2s_1+1,\end{aligned}$$

$$\begin{aligned}g_x =&\mathbf{x}_1+\mathbf{x}_2+s_4^3s_3^2s_2+s_4^3s_3^2s_1+s_4^3s_3s_2s_1+s_4^3s_3s_1^2+s_4^3s_2^3+s_4^3+s_4^2s_3^2s_2^3s_1^2+s_4^2s_3^2s_2^2s_1^3+s_4^2s_3s_2^3+s_4^2s_3s_2^2s_1+\\&s_4^2s_3s_1^3+s_4^2s_3+s_4^2s_1+s_4s_3^2s_2^2s_1+s_4s_3^2s_2s_1^2+s_4s_3s_2^2s_1^2+s_4s_3s_2s_1^3+s_4s_2^2s_1^3+s_4s_2^2+s_3^2s_2^3s_1+s_3^2s_2s_1^3+\\&s_3^2s_2+s_3^2s_1+s_3s_2^3s_1^2+s_3s_1^2+s_2^2s_1^3+s_2s_1^2+s_1^3\end{aligned}$$

$$\begin{aligned}f_y =&\mathbf{y}^2+\mathbf{y}(s_4s_3s_2+s_2^3+1)+\mathbf{e}(s_4^3s_3^3s_2^3s_1^2+s_4^3s_3s_2^3s_1+s_4^3s_2^3s_1^2+s_4^2s_3^3s_2^2s_1+s_4^2s_2^2s_1+s_4s_3^2s_2s_1+s_4s_3s_2s_1^2+\\&s_3^2s_2^3+s_3s_2^3s_1+s_2^3s_1^2)+s_5^3+s_5s_4^2s_3^2s_2+s_5s_3^3s_2^2+s_5s_2^2+s_4^3s_3^3s_2^3+s_4^3s_3^2s_2^3s_1+s_4^3s_2^3s_1+s_4^3s_3s_2^3s_1^2+\\&s_4^3s_3s_1^2+s_4^3s_2^3+s_4^2s_3^2s_2^3s_1^2+s_4^2s_3^2s_2^2s_1+s_4^2s_2^2s_1^2+s_4s_3^3s_2s_1+s_4s_3s_2^3s_1^2+s_4s_3s_2+s_3s_2^3s_1^2+s_3^2s_2^3s_1+s_2^3,\end{aligned}$$

$$\begin{aligned}g_y =&\mathbf{y_1}+\mathbf{y_2}+s_4^3s_3^3+s_4^3s_3s_2^3s_1^2+s_4^3s_2^3+s_4^2s_3^3s_2^2s_1^2+s_4^2s_3s_2^2s_1+s_4s_3^3s_2s_1+s_4s_3s_2+s_4s_2s_1+s_3^3s_2^3s_1^3+s_3^3+\\&s_3^2s_1+s_3s_1^2+s_2^3s_1^3+s_2^3+s_1^3.\end{aligned}$$

In Example 8.5.3 we have the following polynomials

$$\begin{aligned}\mathcal{L}_x =&\mathbf{x}^2+\mathbf{x}(s_2s_3^2s_4^3+s_1s_3^2s_4^3+s_1s_2s_3s_4^3+s_1^2s_3s_4^3+s_2^3s_4^3+s_4^3+s_1^2s_2^3s_3^2s_4^2+s_1^3s_2^2s_3^2s_4^2+s_1^3s_2^3s_3s_4^2+s_1^4s_2^2s_3s_4^2+\\&s_2^4s_4^2+s_2s_4^2+s_1^4s_4^2+s_1s_2^2s_3^2s_4+s_1^2s_2s_3^2s_4+s_1^2s_2^2s_3s_4+s_1^3s_2s_3s_4+s_1s_2^4s_4+s_1^3s_2^2s_4+s_2^2s_4+s_1s_2s_4+\\&s_2^4s_3^2+s_1s_2^3s_3^2+s_1^3s_2s_3^2+s_1^4s_3^2+s_1s_2^4s_3+s_1^2s_2^3s_3+s_1s_2s_3+s_1^2s_3+s_1^3s_2^2+s_1^4s_2^2+s_1s_2^2+s_1^2s_2+s_1^2+s_1^3)+\\&s_3s_5^2+s_2s_3s_5+s_1^2s_2^2s_3^2s_4^3+s_1^3s_2s_3^2s_4^3+s_2^2s_3s_4^3+s_1s_2s_3s_4^3+s_1^2s_2^4s_4^3+s_1^3s_2^3s_4^3+s_2^3s_4^3+s_1^2s_2s_4^3+s_2s_3^3s_4^2+\\&s_1s_2^4s_3^2s_4^2+s_1^2s_2^3s_3^2s_4^2+s_1s_2s_3^2s_4^2+s_1^2s_2^4s_3s_4^2+s_1^3s_2^2s_3s_4^2+s_1^2s_2s_3s_4^2+s_2s_4^2+s_1^2s_3^3s_4+s_1^3s_2^2s_3^2s_4+\\&s_1^4s_2^2s_3^2s_4+s_1^3s_3^2s_4+s_1s_2^3s_3s_4+s_1^2s_2^2s_3s_4+s_1s_3s_4+s_1s_2^4s_4+s_1^4s_2s_4+s_1^2s_4+s_1^3s_2^3s_3^3+s_2^3s_3^3+s_1s_2^2s_3^3+\\&s_1^3s_3^3+s_3^3+s_1^2s_2^2s_3^2+s_1^4s_2s_3+s_1s_2s_3+s_1^4s_2^2+s_1^3+1.\end{aligned}$$

$$\begin{aligned}\mathcal{L}_{xy} =&\mathbf{y}^2+\mathbf{y}(s_2^3s_3^3s_4^3+s_1s_2^2s_3^3s_4^3+s_1^2s_2s_3^3s_4^3+s_1s_3^2s_4^3+s_1^2s_2^3s_3s_4^3+s_2^2s_3s_4^3+s_1s_2s_3s_4^3+s_1^2s_3s_4^3+s_2^3s_4^3+\\&s_1s_2^3s_3^3s_4^2+s_1^2s_2^2s_3^3s_4^2+s_1^3s_2s_3^3s_4^2+s_1^3s_2^2s_3^2s_4^2+s_2^3s_3s_4^2+s_1^2s_2s_3s_4^2+s_1^3s_3s_4^2+s_3s_4^2+s_1^2s_2^2s_4^2+\\&s_1^2s_2^3s_3^3s_4+s_1^3s_2^2s_3^3s_4+s_1s_2s_3^3s_4+s_1^2s_2^2s_3^2s_4+s_1^2s_2^3s_3s_4+s_1s_2^2s_3s_4+s_1^2s_3^2s_4+s_1s_2s_4+s_1^3s_3^3+s_3^3+s_1s_2^3s_3^2+\\&s_1s_3^2+s_1^2s_2^3s_3+s_1^3s_2^2s_3+s_2^2s_3+s_1^2s_3+s_1^3s_2^3+s_2^3)+x(s_2^2s_3s_4^3+s_1^2s_3s_4^3+s_1s_2^2s_4^3+s_1^2s_2s_4^3+s_4^3+\\&s_1s_2^2s_3s_4^2+s_1^2s_2s_3s_4^2+s_1s_3^2s_4^2+s_1^2s_2^2s_4^2+s_3^2s_4+s_1s_2^3s_3s_4+s_1^3s_2s_3s_4+s_1s_3s_4+s_1^3s_2^2s_4+s_1s_2s_4+\\&s_1^2s_4+s_1^2s_2^2s_3^2+s_1^2s_2^3s_3+s_2^2s_3+s_1^2s_3+s_2^3+s_1s_2^2+s_1^3+s_5^3)+s_2s_3^2s_4^2s_5+s_3s_4s_5+s_2^2s_3^3s_5+s_2^2s_5+\\&s_1^2s_2^2s_3^2s_4^3+s_2s_3^2s_4^3+s_1s_3^2s_4^3+s_2^2s_3s_4^3+s_2^3s_4^3+s_1s_2^2s_4^3+s_1^2s_2s_4^3+s_1^2s_3^2s_3^2s_4^2+s_1^3s_2^2s_3^2s_4^2+s_1s_2s_3^2s_4^2+\\&s_1s_2^2s_3s_4^2+s_1^2s_2s_3s_4^2+s_1s_2^3s_4^2+s_1^3s_2s_4^2+s_1s_2s_3^3s_4+s_2^3s_3^2s_4+s_1s_2^2s_3^2s_4+s_1^2s_2s_3^2s_4+s_1^3s_3^2s_4+s_2^3s_4+\\&s_1s_2^3s_3s_4+s_1^3s_2s_3s_4+s_2s_3s_4+s_1^2s_3^3s_4+s_1^3s_2^2s_4+s_1s_2s_4+s_1^3s_2^3s_3^3+s_3^3+s_1s_2^3s_3^2+s_1^3s_2s_3^2+s_2s_3^2+\\&s_1s_3^2+s_1^3s_2^2s_3+s_2^2s_3+s_1^2s_3+s_1^3+1.\end{aligned}$$

In Subsection 8.7.5 we have the following polynomials

$$\begin{aligned}\mathcal{E} =&\mathbf{e}_2^2-\mathbf{e}_2s_1-s_7s_5^3s_2^6-s_7s_5-s_7s_4s_3^3s_2^7s_1^6-s_7s_4s_3s_2^7-s_7s_4s_2^3s_1^5+s_7s_3^4s_2^5s_1^8-s_7s_3^4s_2^5-s_7s_3^3s_2s_1^5-\\&s_7s_3s_2s_1^7+s_7s_2^5s_1^4-s_6s_1-s_5^4s_4s_3^3s_2^6s_1^4-s_5^4s_4s_3s_2^6s_1^6+s_5^4s_4s_2^2s_1^3+s_5^4s_3^3s_2^8s_1^3+s_5^4s_3^3s_1^3+s_5^4s_3s_2^8s_1^5+\\&s_5^4s_3s_1^5+s_5^4s_2^4s_1^2+s_5^3s_4^2s_3^3s_2s_1+s_5^3s_4^2s_3s_2s_1^3-s_5^3s_4^2s_2^5+s_5^3s_4s_3^4s_2^7s_1^3+s_5^3s_4s_3^2s_2^7s_1^5-s_5^3s_4s_3s_2^3s_1^2+\\&s_5^3s_4s_2^7s_1^7-s_5^3s_3^6s_2s_1^8+s_5^3s_3^6s_2+s_5^3s_3^4s_2s_1^2-s_5^3s_3^3s_2^5s_1^7+s_5^3s_3^2s_2s_1^4+s_5^3s_3s_2^5s_1+s_5^3s_2s_1^6-s_5^2s_5^4s_3^3s_1^8-\\&s_5^2s_5^3s_3s_1^2+s_5^2s_5^4s_2^4s_1^7-s_5^2s_4^4s_3^3s_2^2s_1^7-s_5^2s_4^4s_3s_2^2s_1-s_5^2s_4^4s_2^6s_1^6+s_5^2s_4^3s_3^6s_1^7-s_5^2s_4^3s_4^3s_1+s_5^2s_4^3s_2^3s_1^3+\\&s_5^2s_4^3s_2^8s_1^5-s_5^2s_4s_3^3s_1^4-s_5^2s_4s_3s_1^6-s_5^2s_4^3s_3^6s_2^4s_1^4+s_5^2s_4^3s_2^6s_1^6-s_5^2s_3^2s_2^6s_1^8+s_5^2s_2^6s_1^2-s_5s_4^5s_3^4s_2s_1^7-\\&s_5s_4^5s_3^2s_2s_1+s_5s_4^5s_3s_2^5s_1^6+s_5s_4^5s_2s_1^3-s_5s_4^4s_3^4s_2^3s_1^6+s_5s_4^4s_3^3s_2^7s_1^3-s_5s_4^4s_3^2s_2^3s_1^8+s_5s_4^3s_3^7s_2s_1^6-\\&s_5s_4^3s_3^5s_2s_1^8+s_5s_4^3s_3^3s_2s_1^2+s_5s_4^3s_3s_2s_1^4+s_5s_4^3s_2^5s_1+s_5s_4^2s_2^7s_1^8-s_5s_4^2s_2^7+s_5s_4s_3^6s_2s_1+s_5s_4s_3^3s_2^5s_1^8-\\&s_5s_4s_3^2s_2s_1^5-s_5s_5s_4s_3s_2^5s_1^2-s_3^7s_2^7s_1^3-s_5s_3^6s_2^3s_1^8+s_5s_3^6s_2^3+s_5s_3^5s_2^7s_1^5-s_5s_3^4s_2^3s_1^2-s_5s_3^2s_2^3s_1^4-\\&s_4^8s_3^6s_1^4+s_4^8s_3^4s_1^6-s_4^8s_3^3s_2^4s_1^3-s_4^8s_2^3s_1^8-s_4^8s_3s_2^4s_1^5-s_4^8s_2^8s_1^2+s_4^8s_1^2-s_4^7s_3^6s_2^2s_1^3+s_4^7s_3^4s_2^2s_1^5-s_4^7s_3^3s_2^6s_1^2-\\&s_4^7s_3^2s_2^2s_1^7-s_4^7s_3s_2^6s_1^4-s_4^6s_3^6s_2^4s_1^2+s_4^6s_3^4s_2^4s_1^4-s_4^6s_3^3s_2^8s_1+s_4^6s_3^3s_1-s_4^6s_3^2s_2^4s_1^6-s_4^6s_3s_2^8s_1^3+s_4^6s_3s_1^3-\\&s_4^6s_2^4s_1^8+s_4^6s_2^4-s_4^5s_3^5s_2^2s_1^6-s_4^5s_3^3s_2^2s_1^8-s_4^5s_3^3s_2^2+s_4^5s_3^2s_2^6s_1^5+s_4^5s_3s_2^2s_1^2-s_4^4s_3^6-s_4^4s_3^5s_2^4s_1^5-s_4^4s_3^4s_2^8s_1^2+\\&s_4^4s_3^4s_1^2+s_4^4s_3^2s_2^8s_1^4-s_4^4s_3^2s_1^4+s_4^4s_3s_2^4s_1+s_4^4s_2^8s_1^6+s_4^4s_1^6+s_4^3s_3^8s_2^2s_1^5-s_4^3s_3^2s_2^2s_1^3+s_4^3s_3s_2^6s_1^8+s_4^3s_3s_2^6+\\&s_4^3s_2^2s_1^5+s_4^2s_3^4s_2^4s_1^8+s_4^2s_3^2s_2^4s_1^2-s_4^2s_3s_2^8s_1^7-s_4^2s_2^4s_1^4+s_4s_3^7s_2^2s_1^8+s_4s_3^7s_2^2-s_4s_3^6s_2^6s_1^5+s_4s_3^5s_2^2s_1^2-\\&s_4s_3^3s_2^2s_1^4+s_4s_3s_2^6s_1^6+s_4s_2^6s_1^3-s_3^8s_2^8s_1^2-s_3^6s_2^8s_1^4+s_3^5s_2^4s_1-s_3^4s_2^8s_1^6-s_3^4s_2^4s_1^3-s_3^2s_2^8s_1^8+s_3^2-s_3s_2^4s_1^5.\end{aligned}$$

$$\begin{aligned}\mathcal{P}_x =&\mathbf{x}_2^2+\mathbf{x}_2(s_7s_4s_3^3s_1^3+s_7s_4s_3s_1^5-s_7s_4s_2^4s_1^2-s_7s_3^3s_2^2s_1^2-s_7s_3s_2^2s_1^4+s_7s_2^6s_1-s_5^3s_4^5-s_5^3s_4^4s_2^2s_1^7+\\&s_5^3s_4^3s_3^3s_1^7+s_5^3s_4^3s_3s_1+s_5^3s_4^3s_2^4s_1^6+s_5^3s_4^2s_2^6s_1^5-s_5^3s_4s_3^6s_1^6+s_5^3s_4s_3^4-s_5^3s_4s_3^3s_2^4s_1^5-s_5^3s_4s_3^2s_1^2-\\&s_5^3s_4s_3s_2^4s_1^7+s_5^3s_3^6s_2^2s_1^5-s_5^3s_3^4s_2^2s_1^7+s_5^3s_3^2s_2^2s_1-s_5s_4^6s_1+s_5s_4^5s_2^2s_1^8-s_5s_4^5s_2^2+s_5s_4^4s_3^3s_1^8+s_5s_4^4s_3s_1^2-\\&s_5s_4^4s_2^4s_1^7-s_5s_4^3s_3^3s_2^2s_1^7-s_5s_4^3s_3s_2^2s_1-s_5s_4^2s_3^6s_1^7+s_5s_4^2s_4^3s_1-s_5s_4^2s_3^4s_2^4s_1^6-s_5s_4^2s_3^2s_1^3-s_5s_4^2s_3s_2^4s_1^8-\\&s_5s_4^2s_2^8s_1^5-s_5s_4s_3^6s_2^2s_1^6+s_5s_4s_3^4s_2^2+s_5s_4s_3^3s_2^6s_1^5-s_5s_4s_3^2s_2^2s_1^2+s_5s_4s_3^6s_2^4s_1^7-s_5s_3^6s_2^4s_1^5+s_5s_3^4s_2^4s_1^7-\\&s_5s_3^2s_2^4s_1+s_4^8s_1^8+s_4^7s_3^2s_1^6+s_4^7s_2^2s_1^7-s_4^6s_3^3s_2s_1^6+s_4^6s_2^4s_1^6+s_4^5s_3^4s_2^7s_1^8-s_4^5s_3^4s_2^7-s_4^5s_3s_2^3s_1^7+s_4^5s_2^7s_1^4+\\&s_4^5s_2^6s_1^5+s_4^4s_3^6s_2s_1^5+s_4^4s_3^4s_2s_1^7+s_4^4s_3^3s_2^5s_1^4+s_4^4s_3s_2^5s_1^6+s_4^4s_2^8s_1^4-s_4^3s_3^6s_2^3s_1^4+s_4^3s_3^3s_2^3s_1^8+s_4^3s_3s_2^7s_1^5+\end{aligned}$$

$$s_4^3s_2^3s_1^2+s_4^3s_2^2s_1^3+s_4^2s_3^7s_2s_1^6-s_4^2s_3^5s_2s_1^8+s_4^2s_3^4s_2^5s_1^5+s_4^2s_3^3s_2s_1^2+s_4^2s_3^2s_2^5s_1^7-s_4^2s_3s_2s_1^4-s_4^2s_2^5s_1+s_4^2s_2^4s_1^2+$$
$$s_4s_3^8s_2^7s_1^8-s_4s_3^8s_2^7+s_4s_3^4s_2^7s_1^4+s_4s_3^2s_2^7s_1^6-s_4s_2^7s_1^8+s_4s_2^7+s_4s_2^6s_1-s_3^7s_2^5s_1^4+s_3^5s_2^5s_1^6-s_3^3s_2^5s_1^8+s_2^8-1)-$$
$$s_7s_4s_3^3s_2s_1^2-s_7s_4s_3s_2s_1^4+s_7s_4s_2^5s_1+s_7s_3^3s_2^3s_1+s_7s_3s_2^3s_1^3-s_7s_2^7+s_5^3s_4^5s_2s_1^7+s_5^3s_4^4s_2^3s_1^6-s_5^3s_4^3s_3^3s_2s_1^6-$$
$$s_5^3s_4^3s_3s_2-s_5^3s_4^3s_2^5s_1^5-s_5^3s_4^2s_2^7s_1^4+s_5^3s_4s_3^6s_2s_1^5-s_5^3s_4s_3^4s_2s_1^7+s_5^3s_4s_3^3s_2^5s_1^4+s_5^3s_4s_3^2s_2s_1+s_5^3s_4s_3s_2^5s_1^6-$$
$$s_5^3s_3^6s_2^3s_1^4+s_5^3s_3^4s_2^3s_1^6-s_5^3s_3^2s_2^3-s_5^2s_3^6s_2^8s_1^8+s_5^2s_3^6s_2^8+s_5^2s_3^6s_1^8-s_5^2s_3^6+s_5s_4^6s_2s_1^8-s_5s_4^4s_3^3s_2s_1^7-s_5s_4^4s_3s_2s_1+$$
$$s_5s_4^4s_2^5s_1^6+s_5s_4^3s_3^3s_2^3s_1^6-s_5s_4^3s_3s_2^3s_1^8-s_5s_4^3s_3s_2^3+s_5s_4^2s_3^6s_2s_1^6-s_5s_4^2s_3^4s_2s_1^8+s_5s_4^2s_3^3s_2^5s_1^5+s_5s_4^2s_3^2s_2s_1^2+$$
$$s_5s_4^2s_3s_2^5s_1^7+s_5s_4^2s_2s_1^4+s_5s_4s_3^6s_2^3s_1^5-s_5s_4s_3^4s_2^3s_1^7-s_5s_4s_3^3s_2^7s_1^4+s_5s_4s_3^2s_2^3s_1-s_5s_4s_3s_2^7s_1^6+s_5s_3^7s_2^8s_1^8-$$
$$s_5s_3^7s_2^8-s_5s_3^7s_1^8+s_5s_3^7+s_5s_3^6s_2^5s_1^4-s_5s_3^4s_2^5s_1^6-s_5s_3^2s_2^5s_1^8-s_5s_3^2s_2^5-s_4^8s_2s_1^7+s_4^7s_3s_1^8-s_4^7s_3-s_4^7s_2^4s_1^5-$$
$$s_4^7s_2^3s_1^6+s_4^6s_3^3s_2^2s_1^5-s_4^6s_2^5s_1^5+s_4^5s_3s_2^4s_1^6-s_4^5s_2^8s_1^3-s_4^5s_2^7s_1^4-s_4^4s_3^6s_2^2s_1^4-s_4^4s_3^4s_2^2s_1^6-s_4^4s_3^3s_2^6s_1^3+s_4^4s_3^2s_2^2s_1^8-$$
$$s_4^4s_3^2s_2^2-s_4^4s_3s_2^6s_1^5-s_4^4s_2s_1^3+s_4^3s_3^6s_2^4s_1^3-s_4^3s_3^5s_1^8+s_4^3s_3^5-s_4^3s_3^2s_2^4s_1^7-s_4^3s_3s_2^8s_1^4-s_4^3s_2^4s_1-s_4^3s_2^3s_1^2-$$
$$s_4^2s_3^7s_2^2s_1^5+s_4^2s_3^5s_2^2s_1^7-s_4^2s_3^4s_2^6s_1^4-s_4^2s_3^3s_2^2s_1-s_4^2s_3^2s_2^6s_1^6+s_4^2s_3s_2^2s_1^3+s_4^2s_2^6-s_4^2s_2^5s_1-s_4s_3^4s_2^8s_1^3-$$
$$s_4s_3^2s_2^8s_1^5-s_4s_2^7s_1^8-s_4s_1^7+s_3^7s_2^6s_1^3-s_3^6s_2^2s_1^8+s_3^6s_2^2-s_3^5s_2^6s_1^5+s_3^3s_2^6s_1^7.$$

$$\begin{aligned}\mathcal{P}_{xy}=&\mathbf{y}_2^2-\mathbf{y}_2(s_6^2s_3^3s_1^3-s_6^2s_3s_1^5+s_6^2s_2^4s_1^2-s_6s_3^7+s_6s_3^6s_1-s_6s_3^4s_2^4s_1^7-s_6s_3^4s_1^3+s_6s_3^3s_2^4+s_6s_3^2s_1^5-s_6s_3s_2^8s_1^6+\\&s_6s_3s_2^4s_1^2+s_6s_2^8s_1^7+s_6s_2^4s_1^3-s_6s_1^7-s_3^8+s_3^6s_2^4s_1^6-s_3^6s_1^2-s_3^5s_2^4s_1^7-s_3^5s_1^3+s_3^4s_2^4+s_3^4s_1^4+s_3^3s_2^8s_1^5-s_3^3s_1^5-\\&s_3^2s_2^8s_1^6+s_3^2s_2^4s_1^2-s_3^2s_1^6-s_3s_2^8s_1^7+s_3s_2^4s_1^3+s_2^8+s_1^8+1)+\mathbf{x}_2(s_7s_4s_3^3s_2^6s_1^5+s_7s_4s_3s_2^6s_1^7-s_7s_4s_2^5s_1^4-\\&s_7s_3^3s_2^8s_1^4-s_7s_3s_2^8s_1^6+s_7s_2^4s_1^3+s_5^4s_2^3s_1+s_5^3s_4^4s_1-s_5^3s_4^3s_2^2-s_5^3s_4^2s_3^7s_1^4+s_5^3s_4^2s_3^6s_1^5+s_5^3s_4^2s_3^5s_1^6-s_5^3s_4^2s_3^4s_2^4s_1^3-\\&s_5^3s_4^2s_3^4s_1^7+s_5^3s_4^2s_3^3s_2^4s_1^4-s_5^3s_4^2s_3^3s_2^4s_1^5+s_5^3s_4^2s_3^2s_1-s_5^3s_4^2s_3s_2^8s_1^2+s_5^3s_4^2s_3s_2^4s_1^6-s_5^3s_4^2s_3s_1^2+s_5^3s_4^2s_2^8s_1^3-\\&s_5^3s_4^2s_2^4s_1^7-s_5^3s_4^2s_1^3-s_5^3s_4s_3^7s_2^2s_1^3-s_5^3s_4s_3^6s_2^6+s_5^3s_4s_3^6s_2^2s_1^4+s_5^3s_4s_3^5s_2^2s_1^5-s_5^3s_4s_3^4s_2^2s_1^6+s_5^3s_4s_3^3s_2^6s_1^3-\\&s_5^3s_4s_3^3s_2^2s_1^7+s_5^3s_4s_3^2s_2^6s_1^4+s_5^3s_4s_3^2s_2^2+s_5^3s_4s_3s_2^6s_1^5-s_5^3s_3^7s_2^4s_1^2+s_5^3s_3^6s_2^8s_1^7+s_5^3s_3^6s_2^4s_1^3-s_5^3s_3^5s_2^4s_1^4-\\&s_5^3s_3^5s_1^8+s_5^3s_3^5+s_5^3s_3^4s_2^8s_1-s_5^3s_3^4s_2^4s_1^5+s_5^3s_3^4s_1+s_5^3s_3^3s_2^8s_1^2+s_5^3s_3^3s_2^4s_1^7-s_5^3s_3^2s_1^3+s_5^3s_3s_2^8s_1^4-s_5^3s_3s_2^4s_1^8+\\&s_5^3s_3s_2^4+s_5^3s_1^5+s_5^2s_4^3s_3^3s_2^3s_1^5+s_5^2s_4^3s_3s_2^3s_1^7-s_5^2s_4^3s_2^7s_1^4+s_5^2s_4^3s_2^3s_1^2-s_5^2s_2^5s_1+s_5s_4^7s_3s_1^7-s_5s_4^7s_1^8-\\&s_5s_4^6s_3s_2^6s_1^6+s_5s_4^6s_2^6s_1^3+s_5s_4^6s_2^2s_1^7-s_5s_4^5s_3^4s_1^6+s_5s_4^5s_3^3s_1^7-s_5s_4^5s_3^2s_1^8+s_5s_4^5s_3s_2^4s_1^5+s_5s_4^5s_3s_1-s_5s_4^5s_2^4s_1^6-\\&s_5s_4^5s_1^2-s_5s_4^4s_3^4s_2^2s_1^5+s_5s_4^4s_3^3s_2^2s_1^6-s_5s_4^4s_3^2s_2^2s_1^7-s_5s_4^4s_3s_2^6s_1^4+s_5s_4^4s_3s_2^2s_1^8+s_5s_4^4s_2^6s_1^5-s_5s_4^4s_2^2s_1-\\&s_5s_4^3s_3^7s_1^5+s_5s_4^3s_3^6s_1^6+s_5s_4^3s_3^5s_1^7-s_5s_4^3s_3^4s_2^4s_1^4-s_5s_4^3s_3^4s_1^8-s_5s_4^3s_3^3s_2^4s_1^5+s_5s_4^3s_3^3s_1-s_5s_4^3s_3^2s_2^4s_1^6+\\&s_5s_4^3s_3^2s_1^2+s_5s_4^3s_3s_2^8s_1^3-s_5s_4^3s_3s_2^4s_1^7+s_5s_4^3s_2^8s_1^4+s_5s_4^3s_2^4s_1^8-s_5s_4^3s_2^4-s_5s_4^3s_1^4-s_5s_4^2s_3^6s_2^6s_1-\\&s_5s_4^2s_3^4s_2^6s_1^3-s_5s_4^2s_3^3s_2^2s_1^8-s_5s_4^2s_3^2s_2^8s_1^2-s_5s_4^2s_3s_2^6s_1^6+s_5s_4^2s_3s_2^2s_1^2+s_5s_4^2s_2^2s_1^3-s_5s_4s_3^6s_2^8+s_5s_4s_3^6s_2^4s_1^8-\\&s_5s_4s_3^4s_2^8s_1^2+s_5s_4s_3^4s_1^2-s_5s_4s_3^3s_2^8s_1^3+s_5s_4s_3^3s_1^3-s_5s_4s_3^2s_2^4s_1^8+s_5s_4s_3^2s_2^4-s_5s_4s_3s_2^8s_1^5-s_5s_4s_3s_2^4s_1+\\&s_5s_4s_3s_1^5+s_5s_4s_2^8s_1^6-s_5s_4s_2^4s_1^2+s_5s_3^7s_2^6s_1^2-s_5s_3^6s_2^6s_1^3+s_5s_3^6s_2^2s_1^7-s_5s_3^5s_2^6s_1^4+s_5s_3^5s_2^2s_1^8-s_5s_3^5s_2^2+\\&s_5s_3^4s_2^6s_1^5-s_5s_3^4s_3^2s_2^2s_1+s_5s_3^3s_2^6s_1^7+s_5s_3^3s_2^2s_1^3+s_5s_3s_2^6+s_5s_2^6s_1-s_5s_2^2s_1^5+s_4^8s_3s_2^3s_1^4-s_4^8s_3^2s_1^5-s_4^7s_3^2s_2s_1^6+\\&s_4^7s_3s_2^5s_1^3+s_4^7s_3s_2s_1^7-s_4^7s_2^5s_1^4-s_4^7s_2s_1^8-s_4^7s_2+s_4^6s_3^4s_2^3s_1^3-s_4^6s_3^3s_2^3s_1^4-s_4^6s_3^2s_2^3s_1^5-s_4^6s_3s_2^7s_1^2+s_4^6s_3s_2^3s_1^6+\\&s_4^6s_2^3s_1^7+s_4^5s_3^7s_2s_1^3+s_4^5s_3^6s_2^5s_1^8-s_4^5s_3^6s_2^5-s_4^5s_3^5s_2^2s_1^8+s_4^5s_3^4s_2^5s_1^2-s_4^5s_3^3s_2^5s_1^3+s_4^5s_3^2s_2^8s_1+s_4^5s_3^2s_2^5s_1^4-\\&s_4^4s_3^7s_2^3s_1^2+s_4^4s_3^6s_2^7s_1^7+s_4^4s_3^6s_2^3s_1^3-s_4^4s_3^5s_2^7s_1^8+s_4^4s_3^5s_2^7-s_4^4s_3^5s_2^3s_1^4+s_4^4s_3^4s_2^7s_1+s_4^4s_3^4s_2^3s_1^5+s_4^4s_3^3s_2^7s_1^2-\\&s_4^4s_3^3s_2^3s_1^6+s_4^4s_3^2s_2^7s_1^3+s_4^4s_3s_2^3+s_4^3s_3^8s_2s_1^4-s_4^3s_3^7s_2s_1^5+s_4^3s_3^5s_2s_1^7+s_4^3s_3^4s_2^5s_1^4+s_4^3s_3^4s_2s_1^8+s_4^3s_3^4s_2-\\&s_4^3s_3^3s_2^5s_1^5+s_4^3s_3^3s_2s_1+s_4^3s_3^2s_2^5s_1^6+s_4^3s_3^2s_2s_1^2-s_4^3s_3s_2^5s_1^7-s_4^3s_2^5s_1^8-s_4^2s_3^8s_2^3s_1^3+s_4^2s_3^7s_2^3s_1^8+s_4^2s_3^7s_2^3s_1^4-\\&s_4^2s_3^6s_2^3s_1^6-s_4^2s_3^5s_2^7s_1^5-s_4^2s_3^5s_2^3s_1+s_4^2s_3s_2^7s_1^6+s_4^2s_3s_2^3s_1^2-s_4^2s_2^3s_1^3-s_4s_3^8s_2^5s_1^2+s_4s_3^7s_2^5s_1^3-s_4s_3^7s_2s_1^7-s_4s_3^6s_2^5s_1^4-s_4s_3^5s_2^5s_1^5-s_4s_3^4s_2^5s_1^6+s_4s_3^4s_2s_1^2+s_4s_3^2s_2^5s_1^8+\\&s_4s_3^2s_2^5+s_4s_3^2s_2s_1^4-s_4s_3s_2s_1^5+s_4s_2^5s_1^2-s_4s_2s_1^6+s_3^8s_2^7s_1-s_3^7s_2^7s_1^2-s_3^6s_2^7s_1^3-s_3^6s_2^3s_1^7+s_3^5s_2^7s_1^4+\\&s_3^5s_2^3s_1^8+s_3^5s_2^3-s_3^4s_2^3s_1-s_3^3s_2^7s_1^6+s_3^2s_2^7s_1^7+s_3s_2^7s_1^8+s_3s_2^7-s_3s_2^3s_1^4-s_2^7s_1+s_2^3s_1^5)-\\&s_7s_4s_3^3s_2^7s_1^4-s_7s_4s_3s_2^7s_1^6+s_7s_4s_2^3s_1^3+s_7s_3^3s_2s_1^3+s_7s_3^2s_2^5s_1^8-s_7s_3^2s_2^5+s_7s_3s_2s_1^5-s_7s_2^5s_1^2+s_6^2s_3^6+\\&s_6^2s_3^3s_2^4s_1^7-s_6^2s_3^2s_1^4+s_6^2s_2^8s_1^6-s_6^2s_1^6-s_6s_3^8s_1^7-s_6s_3^7s_1^8-s_6s_3^5s_2^4s_1^6+s_6s_3^5s_1^2-s_6s_3^4s_2^4s_1^7-s_6s_3^3s_2^4-s_6s_3^3s_1^4-\\&s_6s_3^2s_2^8s_1^5-s_6s_3^2s_2^4s_1-s_6s_3s_2^8s_1^6+s_6s_3s_1^6+s_6s_2^8s_1^7+s_6s_1^7-s_5^4s_3^4s_2^8s_1^8+s_5^4s_3^4s_2^8+s_5^4s_3^4s_1^8-s_5^4s_3^4-s_5^4s_2^4s_1^8-\\&s_5^3s_4^4s_2+s_5^3s_4^3s_3^6s_2^3s_1-s_5^3s_4^3s_3^4s_2^3s_1^3+s_5^3s_4^3s_3^3s_2^7+s_5^3s_4^3s_2^3s_1^5+s_5^3s_4^3s_3s_2^7s_1^2+s_5^3s_4^3s_2^3s_1^7+s_5^3s_4^2s_3^7s_2s_1^3-\end{aligned}$$

$$s_5^3s_4^2s_3^6s_2s_1^4 - s_5^3s_4^2s_3^5s_2s_1^5 + s_5^3s_4^2s_3^4s_2^5s_1^2 + s_5^3s_4^2s_3^4s_2s_1^6 - s_5^3s_4^2s_3^3s_2^5s_1^3 + s_5^3s_4^2s_3^2s_2^5s_1^4 - s_5^3s_4^2s_3^2s_2 - s_5^3s_4^2s_3s_2^5s_1^5 -$$
$$s_5^3s_4^2s_3s_2s_1 + s_5^3s_4^2s_2^5s_1^6 + s_5^3s_4s_3^7s_2^3s_1^2 + s_5^3s_4s_3^6s_2^7s_1^7 - s_5^3s_4s_3^6s_2^3s_1^3 - s_5^3s_4s_3^5s_2^3s_1^4 + s_5^3s_4s_3^4s_2^3s_1^5 - s_5^3s_4s_3^3s_2^7s_1^2 +$$
$$s_5^3s_4s_3^3s_2^3s_1^6 - s_5^3s_4s_3^2s_2^7s_1^3 - s_5^3s_4s_3^2s_2^3s_1^7 - s_5^3s_4s_3s_2^7s_1^4 - s_5^3s_3^8s_2^5s_1^8 + s_5^3s_3^8s_2^5 + s_5^3s_3^7s_2^5s_1 - s_5^3s_3^6s_2^5s_1^2 - s_5^3s_3^6s_2s_1^6 -$$
$$s_5^3s_3^5s_2^5s_1^3 + s_5^3s_3^4s_2^5s_1^4 - s_5^3s_3^4s_2 - s_5^3s_3^3s_2^5s_1^5 - s_5^3s_3^3s_2s_1 - s_5^3s_3^2s_2^5s_1^6 - s_5^3s_3s_2^5s_1^7 - s_5^3s_3s_2s_1^3 - s_5^3s_2s_1^4 - s_5^2s_4^3s_3^3s_2^4s_1^4 -$$
$$s_5^2s_4^3s_3s_2^4s_1^6 + s_5^2s_4^3s_2^8s_1^3 - s_5^2s_4s_2^4s_1 - s_5^2s_3^8s_2^6s_1^8 + s_5^2s_3^8s_2^6 - s_5^2s_3^4s_2^2s_1^8 + s_5^2s_3^4s_2^2 - s_5^2s_2^6s_1^8 - s_5^2s_2^6 - s_5s_4^7s_3s_2s_1^6 +$$
$$s_5s_4^7s_2s_1^7 + s_5s_4^6s_3s_2^3s_1^5 - s_5s_4^6s_3^7s_2^2s_1^2 - s_5s_4^6s_2^3s_1^6 + s_5s_4^5s_3^4s_2s_1^5 - s_5s_4^5s_3^3s_2s_1^6 + s_5s_4^5s_3^2s_2s_1^7 - s_5s_4^5s_3s_2^5s_1^4 -$$
$$s_5s_4^5s_3s_2s_1^8 + s_5s_4^5s_2^5s_1^5 + s_5s_4^5s_2s_1 - s_5s_4^4s_3^6s_2^3s_1^2 - s_5s_4^4s_3^4s_2^3s_1^4 - s_5s_4^4s_3^3s_2^7s_1 - s_5s_4^4s_3^3s_2^3s_1^5 - s_5s_4^4s_3s_2^3s_1^7 -$$
$$s_5s_4^4s_2^7s_1^4 - s_5s_4^4s_2^3s_1^8 - s_5s_4^4s_2^3 + s_5s_4^3s_3^7s_2s_1^4 + s_5s_4^3s_3^6s_2^5s_1 - s_5s_4^3s_3^6s_2s_1^5 - s_5s_4^3s_3^5s_2s_1^6 + s_5s_4^3s_3^4s_2s_1^7 +$$
$$s_5s_4^3s_3^3s_2^5s_1^4 - s_5s_4^3s_3^3s_2s_1^8 + s_5s_4^3s_3^3s_2 - s_5s_4^3s_3^2s_2^5s_1^5 - s_5s_4^3s_3^2s_2s_1 + s_5s_4^3s_3s_2^5s_1^6 - s_5s_4^3s_3s_2s_1^2 + s_5s_4^3s_2s_1^3 +$$
$$s_5s_4^2s_3^6s_2^7s_1^8 + s_5s_4^2s_3^4s_2^7s_1^2 + s_5s_4^2s_3^3s_2^7s_1^3 + s_5s_4^2s_3^3s_2^3s_1^7 + s_5s_4^2s_3^2s_2^3s_1^8 - s_5s_4^2s_3^2s_2^3 + s_5s_4^2s_3s_2^7s_1^5 - s_5s_4^2s_3s_2^3s_1 -$$
$$s_5s_4^2s_2^3s_1^2 + s_5s_4s_3s_2^5s_1^8 + s_5s_4s_2^5s_1 - s_5s_4s_2s_1^5 + s_5s_3^8s_2^7s_1^8 - s_5s_3^8s_2^7 - s_5s_3^7s_2^7s_1 + s_5s_3^6s_2^7s_1^2 - s_5s_3^6s_2^3s_1^6 +$$
$$s_5s_3^5s_2^7s_1^3 - s_5s_3^4s_2^7s_1^4 + s_5s_3^4s_2^3s_1^8 + s_5s_3^2s_2^7s_1^6 - s_5s_3^2s_2^3s_1^2 - s_5s_3s_2^7s_1^7 + s_5s_2^7s_1^8 + s_5s_2^7 + s_5s_2^3s_1^4 - s_4^8s_3s_2^4s_1^3 +$$
$$s_4^8s_2^4s_1^4 + s_4^8s_1^8 - s_4^8 - s_4^7s_3^3s_2^6s_1^8 + s_4^7s_3^3s_2^6 + s_4^7s_3^2s_2^2s_1^5 - s_4^7s_3s_2^6s_1^2 - s_4^7s_3s_2^2s_1^6 + s_4^7s_2^6s_1^3 - s_4^7s_2^2s_1^7 - s_4^6s_3^6s_2^4s_1^8 -$$
$$s_4^6s_3^3s_2^8s_1^7 + s_4^6s_3^3s_2^4s_1^3 + s_4^6s_3^2s_1^8 - s_4^6s_3^2 - s_4^6s_3s_2^4s_1^5 - s_4^6s_2^4s_1^6 - s_4^5s_3^7s_2^2s_1^2 + s_4^5s_3^6s_2^6s_1^7 + s_4^5s_3^6s_2^2s_1^3 + s_4^5s_3^4s_2^6s_1 +$$
$$s_4^5s_3^3s_2^6s_1^2 + s_4^5s_3^3s_2^2s_1^6 + s_4^5s_3^2s_2^6s_1^3 - s_4^5s_3^2s_2^2s_1^7 + s_4^5s_3s_2^2s_1^8 + s_4^5s_2^6s_1^5 + s_4^5s_2^2s_1 - s_4^4s_3^8s_2^4s_1^8 + s_4^4s_3^8s_2^4 - s_4^4s_3^7s_2^4s_1 -$$
$$s_4^4s_3^6s_2^4s_1^2 + s_4^4s_3^6s_1^6 - s_4^4s_3^4s_2^8 - s_4^4s_3^4s_2^4s_1^4 + s_4^4s_3^4s_1^8 + s_4^4s_3^4 - s_4^4s_3^3s_2^8s_1 + s_4^4s_3^3s_2^4s_1^5 + s_4^4s_3^2s_2^8s_1^2 + s_4^4s_3^2s_1^2 +$$
$$s_4^4s_3s_2^4s_1^7 + s_4^4s_2^8s_1^4 - s_4^4s_1^4 - s_4^3s_3^8s_2^2s_1^3 + s_4^3s_3^7s_2^6s_1^8 - s_4^3s_3^7s_2^6 + s_4^3s_3^7s_2^2s_1^4 + s_4^3s_3^6s_2^2s_1^5 - s_4^3s_3^5s_2^2s_1^6 - s_4^3s_3^4s_2^6s_1^3 -$$
$$s_4^3s_3^3s_2^6s_1^4 - s_4^3s_3^3s_2^2s_1^8 - s_4^3s_3^2s_2^6s_1^5 - s_4^3s_3s_2^6s_1^6 + s_4^3s_2^6s_1^7 + s_4^2s_3^8s_2^4s_1^2 - s_4^2s_3^7s_2^8s_1^7 - s_4^2s_3^7s_2^4s_1^3 + s_4^2s_3^5s_2^4s_1^5 +$$
$$s_4^2s_3^4s_2^8s_1^2 + s_4^2s_3^3s_2^8s_1^3 + s_4^2s_3^2s_2^8s_1^4 + s_4^2s_3s_2^8s_1^5 - s_4^2s_3^4s_2s_1 + s_4^2s_2^4s_1^2 + s_4s_3^8s_2^6s_1 - s_4s_3^7s_2^6s_1^2 + s_4s_3^7s_2^2s_1^6 + s_4s_3^6s_2^6s_1^3 +$$
$$s_4s_3^5s_2^6s_1^4 + s_4s_3^4s_2^6s_1^5 - s_4s_3^4s_2^2s_1 + s_4s_3^2s_2^6s_1^7 - s_4s_3^2s_2^2s_1^3 - s_4s_3s_2^6s_1^8 + s_4s_3s_2^6 + s_4s_3s_2^2s_1^4 - s_4s_2^6s_1 + s_4s_2^2s_1^5 +$$
$$s_3^8s_2^8s_1^8 + s_3^8s_2^8 + s_3^8s_1^8 + s_3^7s_2^8s_1 - s_3^7s_2^4s_1^5 + s_3^7s_1 - s_3^6s_2^8s_1^2 - s_3^6s_2^4s_1^6 - s_3^5s_2^8s_1^3 + s_3^5s_2^4s_1^7 - s_3^5s_1^3 + s_3^4s_2^8s_1^4 - s_3^4s_2^4s_1^8 -$$
$$s_3^4s_2^4 - s_3^4s_1^4 - s_3^3s_2^8s_1^5 + s_3^3s_2^4s_1 + s_3^3s_1^5 - s_3^2s_2^8s_1^6 - s_3^2s_2^4s_1^2 - s_3^2s_1^6 - s_3s_2^4s_1^3 - s_3s_1^7 - s_2^8s_1^8 - s_2^8 - s_2^4s_1^4 - s_1^8 + 1.$$

Bibliography

[AE09] D. Betti Augot and Orsini E. E., *An introduction to linear and cyclic codes*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 47–68.

[BKvT99] A. M. Barg, E. Krouk, and H. C. A. van Tilborg, *On the complexity of minimum distance decoding of long linear codes*, IEEE Trans. on Inf. Th. **45** (1999), no. 5, 1392–1405.

[BMvT78] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. on Inf. Th. **24** (1978), no. 3, 384–386.

[BR12a] E. Ballico and A. Ravagnani, *On Goppa codes on the Hermitian curve*, Arxiv preprint arXiv:1202.0894 (2012).

[BR12b] ———, *On the geometry of Hermitian one-point codes*, Arxiv preprint arXiv:1203.3162 (2012).

[Buc98] B. Buchberger, *An algorithmical criterion for the solvability of algebraic systems of equations*, London Math. Soc. LNS **251** (1998), 535–545.

[Buc06] ———, *Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symb. Comput. **41** (2006), no. 3-4, 475–511.

[CLO07] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, third ed., Springer, 2007, An introduction to computational algebraic geometry and commutative algebra.

[CM90] L. Cerlienco and M. Mureddu, *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* $\geq$ 2., preprint (1990), http://www.emis.ams.org/journals/SLC/opapers/s24cerlien.pdf.

[CM95] ———, *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. **139** (1995), no. 1-3, 73–87.

[CM02a] M. Caboara and T. Mora, *The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 3, 209–232.

[CM02b] L. Cerlienco and M. Mureddu, *Multivariate interpolation and standard bases for Macaulay modules*, J. Algebra **251** (2002), no. 2, 686–726.

[Coo90] A. B. III Cooper, *Direct solution of BCH decoding equations*, Comm., Cont. and Sign. Proc. (1990), 281–286.

[Coo91] ———, *Finding BCH error locator polynomials in one step*, Electronic Letters **27** (1991), no. 22, 2090–2091.

[Coo93] ———, *Toward a new method of decoding algebraic codes using Gröbner bases*, Transactions of the Tenth Army Conference on Applied Mathematics and Computing (1992), vol. 93, U.S. Army, 1993, pp. 1–11.

[Cou11] A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic–geometric codes*, Journal of Algebra (2011).

[CRHT94a] X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, *Algebraic decoding of cyclic codes: a polynomial ideal point of view*, Finite fields, Contemp. Math., vol. 168, Amer. Math. Soc., 1994, pp. 15–22.

[CRHT94b] X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, *Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance*, IEEE Trans. on Inf. Th. **40** (1994), no. 5, 1654–1661.

[DD10] G. Donati and N. Durante, *On the intersection of a Hermitian curve with a conic*, Designs, Codes and Cryptography **57** (2010), no. 3, 347–360.

[DDK09] G. Donati, N. Durante, and G. Korchmaros, *On the intersection pattern of a unital and an oval in pg (2, q2)*, Finite Fields and Their Applications **15** (2009), no. 6, 785–795.

[FL98] J. Fitzgerald and R. F. Lax, *Decoding affine variety codes using Gröbner bases*, Des. Codes Cryptogr. **13** (1998), no. 2, 147–158.

[FM11] C. Fontanari and C. Marcolla, *On the geometry of small weight codewords of dual algebraic geometric codes*, Arxiv preprint arXiv:1104.1320 (2011).

[FRR06] B. Felszeghy, B. Ráth, and L. Rónyai, *The lex game and some applications*, J. Symbolic Comput. **41** (2006), no. 6, 663–681.

[Gei03] O. Geil, *On codes from norm-trace curves*, Finite Fields Appl. **9** (2003), 351–371.

[Gei09] ———, *Algebraic geometry codes from order domains*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 121–141.

[Gia89] P. Gianni, *Properties of Gröbner bases under specializations*, Proc. of EUROCAL1987, LNCS, vol. 378, Springer, 1989, pp. 293–297.

[Gio06] Marta Giorgetti, *On some algebraic interpretation of classical codes*, Ph.D. thesis, University of Milan, 2006.

[GPS07] G.-M. Greuel, G. Pfister, and H. Schönemann, *Singular 3.0. A computer algebra system for polynomial computations*, http://www.singular.uni-kl.de, 2007, Centre for Computer Algebra, University of Kaiserslautern.

[GRS03] S. Gao, V. M. Rodrigues, and J. Stroomer, *Gröbner basis structure of finite sets of points*, preprint (2003), http://www.researchgate.net/publication/2870598.

[GS06] M. Giorgetti and M. Sala, *A commutative algebra approach to linear codes*, BCRI preprint, www.bcri.ucc.ie, 58, UCC, Cork, Ireland, 2006.

[GS09] ———, *A commutative algebra approach to linear codes*, Journal of Algebra **321** (2009), no. 8, 2259–2286.

[HKT08] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ Pr, 2008.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[HvLP98] T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry of codes*, Handbook of coding theory, Vol. I, II (V. S. Pless and W.C. Huffman, eds.), North-Holland, 1998, pp. 871–961.

[Kal89] M. Kalkbrener, *Solving systems of algebraic equations by using Gröbner bases*, Proc. of EUROCAL 1987, LNCS, vol. 378, 1989, pp. 282–292.

[Led08] M. Lederer, *The vanishing ideal of a finite set of closed points in affine space*, J. Pure Appl. Algebra **212** (2008), no. 5, 1116–1133.

[LN86] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986.

[LN97] ———, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[Lun10] S. Lundqvist, *Vector space bases associated to vanishing ideals of points*, J. Pure Appl. Algebra **214** (2010), no. 4, 309–321.

[LY97] P. Loustaunau and E. V. York, *On the decoding of cyclic codes using Gröbner bases*, AAECC **8** (1997), no. 6, 469–483.

[MAG] *MAGMA: Computational Algebra System for Algebra, Number Theory and Geometry*, The University of Sydney Computational Algebra Group., http://magma.maths.usyd.edu.au/magma.

[MB82] H. M. Möller and B. Buchberger, *The construction of multivariate polynomials with preassigned zeros*, LNCS **144** (1982), 24–31.

[MO09] T. Mora and E. Orsini, *Decoding cyclic codes: the Cooper philosophy*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 69–91.

[Mor09] T. Mora, *The FGLM problem and Moeller's algorithm on zero-dimensional ideals*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 27–45.

[MOS12] C. Marcolla, E. Orsini, and M. Sala, *Improved decoding of affine-variety codes*, Journal of Pure and Applied Algebra **216** (2012), no. 7, 1533–1565.

[MPS12] Chiara Marcolla, Marco Pellegrini, and Massimiliano Sala, *On the hermitian curve, its intersections with some conics and their applications to affine-variety codes and hermitian codes*, arXiv preprint arXiv:1208.1627 (2012).

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I and II*, North-Holland Publishing Co., Amsterdam, 1977.

[OS05] E. Orsini and M. Sala, *Correcting errors and erasures via the syndrome variety*, J. Pure Appl. Algebra **200** (2005), 191–226.

[RS94] H.G. Ruck and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, Journal fur die Reine und Angewandte Mathematik **457** (1994), 185–188.

[S.02] Lang S., *Algebra revised third edition*, Springer-Verlag, 2002.

[Sal07] M. Sala, *Gröbner basis techniques to compute weight distributions of shortened cyclic codes*, Journal of Algebra and Its Applications **6** (2007), no. 3, 403–404.

[SDG06] G. Salazar, D. Dunn, and S. B. Graham, *An improvement of the Feng-Rao bound on minimum distance*, Finite Fields Appl. **12** (2006), no. 3, 313–335.

[Sha48] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656.

[ST09] M. Mora T. Perret L. Sakata S. Sala and C. Traverso, *Gröbner Bases, Coding, and Cryptography*, RISC Book Series, Springer, Heidelberg, 2009.

[Sti88] H. Stichtenoth, *A note on Hermitian codes over GF(q^2)*, IEEE Trans. Inform. Theory **34** (1988), no. 5, 1345–1348.

[Sti93] ———, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[Var97] A. Vardy, *Algorithmic complexity in coding theory and the minimum distance problem*, Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, 1997, pp. 92–109.

[Xin95] C. Xing, *On automorphism groups of the Hermitian codes*, Information Theory, IEEE Transactions on **41** (1995), no. 6, 1629–1635.

[YK92] K. Yang and P.V. Kumar, *On the true minimum distance of Hermitian codes*, Proceedings of AGCT–3, LNCS, Springer, 1992, pp. 99–107.