An introduction to Algebraic Geometry codes

Carlos Munuera and Wilson Olaya-León

Abstract. We present an introduction to the theory of algebraic geometry codes. Starting from evaluation codes and codes from order and weight functions, special attention is given to one-point codes and, in particular, to the family of Castle codes.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. A *linear code of length n and dimension k* over $\mathbb{F}_q$, a $[n,k]$ code for short, is a k-dimensional linear space $\mathcal{C} \subseteq \mathbb{F}_q^n$. The *minimum distance* of $\mathcal{C}$ is by definition

$$d = \min\{d(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\} = \min\{wt(\mathbf{u}) : \mathbf{u} \in \mathcal{C}, \mathbf{u} \neq \mathbf{0}\}$$

where d stands for the Hamming distance, $d(\mathbf{u},\mathbf{v}) = \#\{i : u_i \neq v_i\}$, and wt for the Hamming weight, $wt(\mathbf{u}) = d(\mathbf{u},\mathbf{0})$. A "good code" is one that optimizes simultaneously the ratios d/n and k/n.

The problem of finding good codes is central to the theory of error correcting codes. For many years coding theorists have addressed this problem by adding more and more algebraic and combinatorial structure to $\mathcal{C}$. In particular, codes with excellent properties have been obtained by using techniques and resources from algebra and algebraic geometry, the so-called *algebraic geometry* codes. Most of these techniques are highly specialized and the study of the obtained codes is very elegant but in general difficult. Indeed, given such a code, often it is not possible to calculate its exact minimum distance, and sometimes even its dimension.

In this chapter we present a short introduction to algebraic geometry codes. We use the order bounds on the minimum distance as a motivation to introduce evaluation and algebraic geometry codes. Then we center our attention on one-point codes, and later on the family of Castle codes. As a result of this orientation we can overview quickly much of the basic theory. However we warn the reader that many important parts and facts have been omitted. For a complete treatment we refer to the excellent texts [**27**] and [**45**]. The canonical reference for general error correcting codes is the very complete book [**30**] (although it does not contain the theory of AG codes).

2000 *Mathematics Subject Classification.* Primary: 94B27; Secondary: 14G50.

2. The order bounds on the minimum distance

2.1. Bounds. As noted above, computing the true minimum distance d of a linear code $\mathcal{C}$ is in general a difficult problem (it is an NP-complete problem, see [**5**]). Often we have to settle for an estimate of d based on some available lower bound. And then evaluate the quality of our parameters by comparing them with several upper bounds. Usually upper bounds are general, valid for all linear codes. Let us show an important example.

THEOREM 2.1 (Singleton bound). *The parameters n, k, d of a linear code $\mathcal{C}$ verify $k + d \leq n + 1$.*

PROOF. Let $\pi : \mathcal{C} \to \mathbb{F}_q^{n-d+1}$ be the projection obtained by deleting $d-1$ fixed coordinates. Since each codeword of $\mathcal{C}$ has at least d nonzero coordinates, π is an injective linear map, hence $\dim(\pi(\mathcal{C})) = k$ and thus $k \leq n - d + 1$. □

Codes reaching equality in the Singleton bound are called *maximum distance separable* (or MDS) codes.

Lower bounds on the minimum distance are designed to be applied to some particular families or constructions of codes. Significant examples could be BCH and Goppa bounds (BCH and algebraic geometry codes respectively). Besides uniform ones, other interesting lower bounds are of order type. They are based on obtaining different estimates for different subsets of codewords. Such a bound is successful if for each subset we can find estimates better than a uniform bound for all codewords. In this chapter we shall explain two bounds of this type.

2.2. $\mathbb{F}_q$-algebras. Throughout this chapter, an *$\mathbb{F}_q$-algebra* will be a commutative ring R with a unit, containing $\mathbb{F}_q$ as a subring. Then R is a vector space over $\mathbb{F}_q$. The most interesting examples of $\mathbb{F}_q$-algebras are the polynomial ring in m variables $\mathbb{F}_q[X_1, \ldots, X_m]$ and its quotients $\mathbb{F}_q[X_1, \ldots, X_m]/I$, where I is an ideal. Other important example is $\mathbb{F}_q^n$. Since $\mathbb{F}_q$ is naturally isomorphic to $\{(\lambda, \ldots, \lambda) | \lambda \in \mathbb{F}_q\}$, it turns out that $\mathbb{F}_q^n$ is also an algebra with the coordinate wise product $*$,

$$(u_1, \ldots, u_n) * (v_1, \ldots, v_n) = (u_1 v_1, \ldots, u_n v_n).$$

Note that $(\lambda, \ldots, \lambda) * (u_1, \ldots, u_n) = \lambda(u_1, \ldots, u_n)$ hence the ring and vector space structures on $\mathbb{F}_q^n$ are fully compatible.

2.3. The Andersen-Geil bound. Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a basis of $\mathbb{F}_q^n$. We consider the linear codes $\mathcal{C}_0 = (\mathbf{0})$, and for $k = 1, \ldots, n$,

$$\mathcal{C}_k = \langle \mathbf{b}_1, \ldots, \mathbf{b}_k \rangle.$$

$\mathcal{C}_k$ is a $[n, k]$ code. Associated to the chain $\mathcal{C}_0 = (\mathbf{0}) \subset \mathcal{C}_1 \subset \cdots \subset \mathcal{C}_n = \mathbb{F}_q^n$, we define the sorting map $\rho_{\mathcal{B}} : \mathbb{F}_q^n \to \{0, \ldots, n\}$ by $\rho_{\mathcal{B}}(\mathbf{v}) = \min\{r : \mathbf{v} \in \mathcal{C}_r\}$.

LEMMA 2.2. *Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{F}_q^n$. Then*

1. *$\rho_{\mathcal{B}}(\mathbf{v}_1 + \cdots + \mathbf{v}_m) \leq \max\{\rho_{\mathcal{B}}(\mathbf{v}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v}_m)\}$. If there exists j such that $\rho_{\mathcal{B}}(\mathbf{v}_i) < \rho_{\mathcal{B}}(\mathbf{v}_j)$ for all $i \neq j$, then equality holds.*
2. *If $\mathbf{v} \neq \mathbf{0}$ then there exist $\lambda_1, \ldots, \lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \in \mathbb{F}_q$ with $\lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \neq 0$ such that $\mathbf{v} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})}$.*
3. *$\dim(\langle \mathbf{v}_1, \ldots, \mathbf{v}_m \rangle) \geq \#\{\rho_{\mathcal{B}}(\mathbf{v}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{v}_m)\}$. Conversely, if $D \subseteq \mathbb{F}_q^n$ is a linear subspace of dimension m, then there exists a basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ of D such that $\#\{\rho_{\mathcal{B}}(\mathbf{u}_1), \ldots, \rho_{\mathcal{B}}(\mathbf{u}_m)\} = m$.*

PROOF. (1) Both statements follow from the linear structure of our codes. (2) follows from (1).(3) Assume $\#\{\rho_{\mathcal{B}}(\mathbf{v}_1),\dots,\rho_{\mathcal{B}}(\mathbf{v}_m)\} = t$ and $\rho_{\mathcal{B}}(\mathbf{v}_1) < \cdots < \rho_{\mathcal{B}}(\mathbf{v}_t)$. If $\lambda_1\mathbf{v}_1 + \cdots + \lambda_t\mathbf{v}_t = 0$ then $0 = \rho_{\mathcal{B}}(\mathbf{0}) = \rho_{\mathcal{B}}(\lambda_1\mathbf{v}_1 + \cdots + \lambda_t\mathbf{v}_t) = \max\{\rho_{\mathcal{B}}(\mathbf{v}_i) : \lambda_i \neq 0\}$. By (1) this implies $\lambda_1 = \cdots = \lambda_t = 0$. Conversely write $D_i = D \cap C_i$. For all $i = 1,\dots,n$, it holds that $D_i = D_{i-1} \oplus (D \cap \langle \mathbf{b}_i\rangle)$, hence $\dim(D_{i-1}) \leq \dim(D_i) \leq \dim(D_{i-1}) + 1$ and the last inequality is an equality precisely m times. If $D_i \neq D_{i-1}$, take a vector $\mathbf{u}_i \in D_i \setminus D_{i-1}$. Then $\#\{\rho_{\mathcal{B}}(\mathbf{u}_1),\dots,\rho_{\mathcal{B}}(\mathbf{u}_m)\} = m$ and $\{\mathbf{u}_1,\dots,\mathbf{u}_m\}$ is a basis of D. □

We consider in $\mathbb{N}^2$ the partial order $(r,s) \prec (i,j)$ if and only if $r \leq i$, $s \leq j$ and $(r,s) \neq (i,j)$. A pair of nonzero vectors $(\mathbf{u},\mathbf{v})$ is called *well-behaving* (with respect to the basis $\mathcal{B}$) if for any pair $(\mathbf{b}_r,\mathbf{b}_s)$ such that $(r,s) \prec (\rho_{\mathcal{B}}(\mathbf{u}),\rho_{\mathcal{B}}(\mathbf{v}))$ it holds that $\rho_{\mathcal{B}}(\mathbf{b}_r * \mathbf{b}_s) < \rho_{\mathcal{B}}(\mathbf{u} * \mathbf{v})$. For $i = 1,\dots,n$, define the set

$$\Lambda_i = \{\mathbf{b}_j \in \mathcal{B} : (\mathbf{b}_i,\mathbf{b}_j) \text{ is well-behaving}\}.$$

Let $\mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{v} \neq \mathbf{0}$. According to Lemma 2.2 (2), we can write $\mathbf{v}$ as a linear combination $\mathbf{v} = \lambda_1\mathbf{b}_1 + \cdots + \lambda_{\rho_{\mathcal{B}}(\mathbf{v})}\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})}$ with $\lambda_{\rho_{\mathcal{B}}(\mathbf{v})} \neq 0$. Then, if $\mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$ we have

$$\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_j) = \rho_{\mathcal{B}}\Big(\sum_{i=1}^{\rho_{\mathcal{B}}(\mathbf{v})} \lambda_i\mathbf{b}_i * \mathbf{b}_j\Big) = \rho_{\mathcal{B}}(\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})} * \mathbf{b}_j).$$

PROPOSITION 2.3. *Let $\mathbf{v} \in \mathbb{F}_q^n$. If $\mathbf{v} \neq \mathbf{0}$ then $wt(\mathbf{v}) \geq \#\Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$.*

PROOF. Consider the space $V(\mathbf{v}) = \{\mathbf{u} \in \mathbb{F}_q^n : \mathrm{supp}(\mathbf{u}) \subseteq \mathrm{supp}(\mathbf{v})\} = \{\mathbf{u} * \mathbf{v} : \mathbf{u} \in \mathbb{F}_q^n\}$. Then $wt(\mathbf{v}) = \dim(V(\mathbf{v})) \geq \dim(\langle \mathbf{v} * \mathbf{b}_1,\dots,\mathbf{v} * \mathbf{b}_n\rangle) \geq \#\{\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_1),\dots,\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_n)\} \geq \#\{\rho_{\mathcal{B}}(\mathbf{v} * \mathbf{b}_j) : \mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}\} = \#\{\rho_{\mathcal{B}}(\mathbf{b}_{\rho_{\mathcal{B}}(\mathbf{v})} * \mathbf{b}_j) : \mathbf{b}_j \in \Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}\} = \#\Lambda_{\rho_{\mathcal{B}}(\mathbf{v})}$. □

This result directly leads to the following bound.

THEOREM 2.4. *For $k = 1,\dots,n$, the minimum distance of $\mathcal{C}_k$ satisfies*

$$d(\mathcal{C}_k) \geq \min\{\#\Lambda_r : r = 1,\dots,k\}.$$

The inequality stated in the above theorem is called the *Andersen-Geil bound on the minimum distance of the primary code $\mathcal{C}_k$*, or *order bound with respect to the basis $\mathcal{B}$ on the minimum distance of the primary code $\mathcal{C}_k$*. Note that the sets Λ_r depend on the basis $\mathcal{B}$. So the bound depends on $\mathcal{B}$ as well. This bound can be applied to an arbitrary linear code $\mathcal{C}$, just by including it into any increasing chain of codes $\mathcal{C}_1 \subset \cdots \subset \mathcal{C}_{k-1} \subset \mathcal{C} \subset \mathcal{C}_{k+1} \subset \cdots \subset \mathcal{C}_n = \mathbb{F}_q^n$. However the best results are obtained when all the codes in the chain have been obtained by the same construction. This is the case of some types of codes arising from algebraic geometry.

A similar bound can be stated for codes $\mathcal{C}_I = \langle\{\mathbf{b}_i : i \in I\}\rangle$ where I is an arbitrary subset of $\{1,\dots,n\}$ (without changing the order on the basis elements nor the map ρ). We leave this generalization as an exercise to the reader (or see [**21**]).

2.4. The Feng-Rao bound on the minimum distance of dual codes. Given a linear $[n,k]$ code $\mathcal{C}$, its *dual code* is defined as

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$$

where $\cdot$ denotes the usual inner product in $\mathbb{F}_q^n$

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i.$$

Then $\mathcal{C}^\perp$ is a linear $[n, n-k]$ code. By using similar ideas to those explained in the previous subsection, we can give a bound on the minimum distance of dual codes. Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a basis of $\mathbb{F}_q^n$ and consider the chain of dual codes

$$\mathcal{C}_n^\perp = (\mathbf{0}) \subset \mathcal{C}_{n-1}^\perp \subset \cdots \subset \mathcal{C}_0^\perp = \mathbb{F}_q^n.$$

Given a vector $\mathbf{u} \in \mathbb{F}_q^n$, define the *syndromes* of $\mathbf{u}$

$$s_1 = s_1(\mathbf{u}) = \mathbf{b}_1 \cdot \mathbf{u}, \ldots, s_n = s_n(\mathbf{u}) = \mathbf{b}_n \cdot \mathbf{u}$$

or equivalently $\mathbf{B}\mathbf{u}^T = \mathbf{s}^T$, where $\mathbf{s} = (s_1, \ldots, s_n)$ and $\mathbf{B}$ is the matrix whose rows are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Then $\mathbf{u} \in \mathcal{C}_r^\perp \setminus \mathcal{C}_{r+1}^\perp$ if and only if $s_1 = \cdots = s_r = 0$ and $s_{r+1} \neq 0$. Consider also the *two dimensional syndromes*

$$s_{ij} = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{u}, \ 1 \leq i, j \leq n.$$

Let $\mathbf{S}$ be the matrix $\mathbf{S} = (s_{ij})$, $1 \leq i, j \leq n$. Note that this matrix can be written also as $\mathbf{S} = \mathbf{B}\mathbf{D}(\mathbf{u})\mathbf{B}^T$, where $\mathbf{D}(\mathbf{u})$ is the diagonal matrix with $\mathbf{u}$ in its diagonal. Since $\mathbf{B}$ has full rank, we have $\operatorname{rank}(\mathbf{S}) = \operatorname{rank}(\mathbf{D}(\mathbf{u})) = wt(\mathbf{u})$.

LEMMA 2.5. *Let $\mathbf{u} \in \mathcal{C}_r^\perp$.*

(1) *$s_{ij} = 0$ for all (i,j) such that $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) \leq r$.*
(2) *If $\mathbf{u} \notin \mathcal{C}_{r+1}^\perp$ then $s_{ij} \neq 0$ for all (i,j) such that $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r+1$.*

PROOF. As $\mathbf{u} \in \mathcal{C}_r^\perp$ we have $s_1 = \cdots = s_r = 0$. (1) If $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) \leq r$ then, according to Lemma 2.2(2), $\mathbf{b}_i * \mathbf{b}_j = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_r \mathbf{b}_r$ and $s_{ij} = \lambda_1 s_1 + \cdots + \lambda_r s_r = 0$. (2) If $\mathbf{u} \notin \mathcal{C}_{r+1}^\perp$ then $s_{r+1} \neq 0$. When $\rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r+1$, we have $\mathbf{b}_i * \mathbf{b}_j = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_r \mathbf{b}_r + \lambda_{r+1} \mathbf{b}_{r+1}$ with $\lambda_{r+1} \neq 0$. Then $s_{ij} = \lambda_1 s_1 + \cdots + \lambda_r s_r + \lambda_{r+1} s_{r+1} = \lambda_{r+1} s_{r+1} \neq 0$. □

For $r = 0, \ldots, n-1$, define the sets

$$N_r = \{(i,j) : (\mathbf{b}_i, \mathbf{b}_j) \text{ is well-behaving and } \rho_{\mathcal{B}}(\mathbf{b}_i * \mathbf{b}_j) = r+1\}.$$

Let $N_r = \{(i_1, j_1), \ldots, (i_t, j_t)\}$. The well-behaving property implies that all i's in this set are distinct. Write $i_1 < i_2 < \cdots < i_t$. By symmetry, $j_t = i_1, \ldots, j_1 = i_t$, hence $j_t < \cdots < j_1$. Let $\mathbf{S}_r$ be the submatrix of $\mathbf{S}$

$$\mathbf{S}_r = \begin{bmatrix} s_{i_1,j_t} & \cdots & s_{i_1,j_1} \\ \vdots & & \vdots \\ s_{i_t,j_t} & \cdots & s_{i_t,j_1} \end{bmatrix}.$$

LEMMA 2.6. *If $\mathbf{u} \in \mathcal{C}_r^\perp \setminus \mathcal{C}_{r+1}^\perp$ then $\mathbf{S}_r$ has full rank.*

PROOF. Let (l,m) be an entry in the anti-diagonal of $\mathbf{S}_r$. Then $l = i_h, m = j_h$ for some h and $s_{lm} \neq 0$ by Lemma 2.5(2). If (l,m) is above the anti-diagonal, then $l = i_h, m < j_h$, hence $\rho_{\mathcal{B}}(\mathbf{b}_l * \mathbf{b}_m) < \rho_{\mathcal{B}}(\mathbf{b}_{i_h} * \mathbf{b}_{j_h}) = r+1$. Thus $s_{lm} = 0$ by Lemma 2.5(1) and $\det(\mathbf{S}_r) \neq 0$. □

As a consequence of this lemma, if $\mathbf{u} \in \mathcal{C}_r^\perp \setminus \mathcal{C}_{r+1}^\perp$ we have $wt(\mathbf{u}) = \operatorname{rank}(\mathbf{S}) \geq \operatorname{rank}(\mathbf{S}_r) = \#N_r$. The *Feng-Rao* or *dual order bound* on the minimum distance of $\mathcal{C}_k^\perp$ *with respect to the basis* $\mathcal{B}$ states the following

THEOREM 2.7. *For $k = 0, 1, \dots, n-1$, the minimum distance of $\mathcal{C}_k^\perp$ satisfies*

$$d(\mathcal{C}_k^\perp) \geq \min\{\#N_r : r = k, \dots, n-1\}.$$

As in case of primary codes, this bound depends on the choice of the basis $\mathcal{B}$.

3. Evaluation codes and order domains

The theory introduced in the previous section directly leads to the problem of finding basis $\mathcal{B}$ producing good codes. This subject will be addressed in this section.

Let R be a $\mathbb{F}_q$-vector space and let Φ be a linear map $\Phi : R \to \mathbb{F}_q^n$. For every linear subspace $L \subseteq R$ we have a linear code

$$\mathcal{C}(L) = \Phi(L)$$

and its dual

$$\mathcal{C}(L)^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}(L)\}.$$

If we consider a basis $\{f_1, f_2, \dots\}$ of R, we get a chain of linear codes, $\mathcal{C}_r = \langle \Phi(f_1), \dots, \Phi(f_r) \rangle$, $r = 1, 2, \dots$. When Φ is surjective, then there exists r such that $\mathcal{C}_r = \mathbb{F}_q^n$, and the order bounds can be applied to obtain estimates on the minimum distance of these codes.

3.1. Evaluation codes. The most interesting case of the above construction arises when R is a set of functions that can be evaluated at points $P_1, \dots, P_n$ belonging to a geometrical object $\mathcal{X}$. Set $\mathcal{P} = \{P_1, \dots, P_n\}$ and let $\Phi = ev_{\mathcal{P}} : R \to \mathbb{F}_q^n$ defined by $ev_{\mathcal{P}}(f) = (f(P_1), \dots, f(P_n))$. The obtained codes are called *evaluation codes*.

EXAMPLE 3.1 (Reed-Muller codes). To give a concrete example take the $\mathbb{F}_q$-algebra $R = \mathbb{F}_q[X_1, \dots, X_m]$ and let $\mathcal{P}$ be the set of all $n = q^m$ points $P_1, \dots, P_n$ in $\mathbb{F}_q^m$. The evaluation map

$$ev_{\mathcal{P}} : \mathbb{F}_q[X_1, \dots, X_m] \to \mathbb{F}_q^n$$

$ev_{\mathcal{P}}(f) = (f(P_1), \dots, f(P_n))$, is linear and verifies $(fg)(P) = f(P) * g(P)$, so it is a morphisms of $\mathbb{F}_q$-algebras. To see surjectivity, given a point $P = (a_1, \dots, a_m) \in \mathbb{F}_q^m$, the polynomial

$$f_P = \prod_{i=1}^{m} \prod_{\alpha \in \mathbb{F}_q, \alpha \neq a_i} (X_i - \alpha)$$

verifies $f_P(P) \neq 0$ and $f_P(Q) = 0$ for all $Q \neq P$. Thus the vectors $\{ev_{\mathcal{P}}(f_P) : P \in \mathbb{F}_q^m\}$ span $\mathbb{F}_q^n$. Consider the basis $\{f_1, f_2, \dots\}$ of $\mathbb{F}_q[X_1, \dots, X_m]$ consisting of all monomials ordered according to a graded order (for example the graded lexicographic order: first compare degrees; then apply lexicographic order to break ties). Then we obtain an increasing chain of codes $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \dots$, where

$$\mathcal{C}_i = ev_{\mathcal{P}}(\langle f_1, \dots, f_i \rangle).$$

Among these codes, particular interest have the ones of the form $\mathcal{RM}(r, m) = ev_{\mathcal{P}}(\mathbb{F}_q[X_1, \dots, X_m]_{(r)})$, where $\mathbb{F}_q[X_1, \dots, X_m]_{(r)}$ stands for the linear space of all polynomials of degree at most r. They are called *Reed-Muller* codes. The same construction can be done by considering homogeneous polynomials and evaluating them at points in the projective space. In this case we obtain the so-called Projective Reed-Muller codes.

Reed Muller codes are important from both theoretical and practical reasons and much is known about them. For example, in 1972 a Reed-Muller code was used by Mariner 9 to transmit black and white photographs from Mars. The case $m = 1$ is particularly simple and interesting, so it deserves a special attention.

EXAMPLE 3.2 (Reed-Solomon codes). Let $R = \mathbb{F}_q[X]$ and consider the basis $\{1, X, X^2, \dots\}$. Let $\mathcal{P}$ be the set of points in the affine line $\mathbb{F}_q$. The obtained evaluation codes, called *Reed Solomon* codes, are widely used (CD players, bar codes, etc.). Their parameters are easy to obtain: as a polynomial of degree r has at most r roots, for $r < n$ the code $ev_{\mathcal{P}}(\langle 1, X, \dots, X^r\rangle)$ has length $n = q$, dimension $k = r + 1$ and minimum distance $d = n - r$ (it is a MDS code).

In the above two examples, note that for all $f \in \mathbb{F}_q[X_1, \dots, X_m]$ it holds that $ev_{\mathcal{P}}(f^q) = ev_{\mathcal{P}}(f)$, hence we can obtain the same codes from the quotient algebra $\mathbb{F}_q[X_1, \dots, X_m]/\langle X_1^q - X_1, \dots, X_m^q - X_m\rangle$. In general, we can take an ideal $I \subset \mathbb{F}_q[X_1, \dots, X_m]$ and consider $I_q = I + \langle X_1^q - X_1, \dots, X_m^q - X_m\rangle$. Let $\mathcal{P} = \{P_1, ..., P_n\}$ be the set of all rational points in the zero set $V = V(I_q)$. The evaluation map $ev_{\mathcal{P}} : R_q = \mathbb{F}_q[X_1, \dots, X_m]/I_q \to \mathbb{F}_q^n$ is a vector space isomorphism. For any linear subspace $L \subseteq R_q$ we define the *affine variety* code $C(I, L) = ev_{\mathcal{P}}(L)$. It is known that every linear code can be obtained in this way. Also algebraic geometry codes from curves, which are the main subject of this chapter, are particular cases of this construction. Affine variety codes were introduced by Fitzgerald and Lax in [**14**], where the reader can find more details.

3.2. Weight functions and order domains. In previous examples we have seen how to construct a chain of evaluation codes from an algebra R and an ordered basis of R. The better this order, the better will be the results obtained when using the order bounds. We formalize this idea.

Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. A function $v : R \to \mathbb{N}_0 \cup \{-\infty\}$ is a *weight* on R if it verifies the following properties

(W.1) $v(f) = -\infty$ if and only if $f = 0$;
(W.2) $v(1) = 0$;
(W.3) $v(f + g) \leq \max\{v(f), v(g)\}$;
(W.4) $v(fg) = v(f) + v(g)$;
(W.5) if $v(f) = v(g)$ then there exists an element $\lambda \in \mathbb{F}_q^*$ such that $v(f - \lambda g) < v(f)$.

REMARK 3.3. Let v be a weight function on R. The following are simple consequences of properties (W.1) to (W.5).
(a) For all $\lambda \in \mathbb{F}_q^*$ we have $v(\lambda\lambda^{-1}) = v(\lambda) + v(\lambda^{-1}) = v(1) = 0$. Then $v(\lambda) = 0$. Conversely, if $v(f) = 0$ then there exists $\lambda \in \mathbb{F}_q^*$ such that $v(f - \lambda) = -\infty$ and $f = \lambda \in \mathbb{F}_q$.
(b) If $v(f) > v(g)$ then $v(f) = v(-g + (f + g)) \leq \max\{v(g), v(f + g)\} = v(f + g) \leq v(f)$, hence $v(f + g) = v(f)$.
(c) R is an integral domain. If $fg = 0$ with $g \neq 0$ then $v(1) \leq v(g)$. Thus $v(f) \leq v(fg) = -\infty$ which implies $v(f) = -\infty$ and so $f = 0$.

A $\mathbb{F}_q$-algebra R with a weight function v will be called an *order domain*. Let $H(v) = \{v(f) : f \in R^*\} = \{v_1, v_2, \dots\}$ be the increasing sequence of all integers appearing as the order of a nonzero element. For each $v_i \in H(v)$ let $f_i \in R$ be such that $v(f_i) = v_i$ and consider the ordered set $\mathcal{F} = \{f_1, f_2, \dots\}$.

PROPOSITION 3.4. *Let R be an order domain with order function v and let $\mathcal{F} = \{f_1, f_2, \dots\}$ as above. Then*

(1) *$\mathcal{F}$ is a basis of R over $\mathbb{F}_q$.*
(2) *If $f = \sum_j \lambda_j f_j$, then $v(f) = \max\{v(f_j) : \lambda_j \neq 0\}$.*

PROOF. An iterated application of property (W.5) shows that $\mathcal{F}$ is a basis of R. (2) follows from Remark 3.3 (b). □

3.3. Semigroups. A *numerical semigroup* is a set $S \subseteq \mathbb{N}_0$ such that (i) $0 \in S$ and (ii) if $a, b \in S$ then $a + b \in S$. Our interest on semigroups comes from the following fact, which is a consequence of properties (W.2) and (W.4).

PROPOSITION 3.5. *If R is an order domain and v is a weight function on R, then $H(v)$ is a numerical semigroup.*

The elements of S will be called *pole numbers* or just *poles*, while the elements in $\mathbb{N}_0 \setminus S$ will be called *gaps*. We shall denote by $\mathrm{Gaps}(S)$ the set of gaps of S. The number $g = \#\mathrm{Gaps}(S)$ is the *genus* of S. If S has finite genus then the smallest integer c such that $a \in S$ for all $a \geq c$ is the *conductor* of S. From now on, all the semigroups we consider will be of finite genus.

LEMMA 3.6. *The conductor c of a semigroup of genus g verifies $c \leq 2g$.*

PROOF. Since $c - 1$ is a gap, given a pair $(a, b) \in \mathbb{N}_0^2$ with $a + b = c - 1$, at least one of these two numbers is also a gap. There are c such pairs and g gaps so we obtain the inequality. □

When $c = 2g$ the semigroup is called *symmetric*. Note that for symmetric semigroups, given a pair $(a, b) \in \mathbb{N}_0^2$ with $a + b = c - 1$, exactly one of these two numbers is a gap and the other is a pole. Conversely, this condition ensures that $c = 2g$.

From Lemma 3.6, the interval $[0, 2g - 1]$ contains g poles and g gaps. If we write S as an increasing enumeration of its elements $S = \{v_1 = 0 < v_2 < \dots\}$, then $2g = v_{g+1}$, hence $v_{g+i} = 2g + i - 1$ for all $i = 1, 2, \dots$. The first nonzero element of S, v_2, is the *multiplicity* of S. It will play an important role in forthcoming sections of this chapter.

A set of generators of S is a set $A = \{a_1, \dots, a_r\} \subset S$ such that any $a \in S$ can be written as a linear combination $a = \lambda_1 a_1 + \cdots + \lambda_r a_r$ with nonnegative integer coefficients. In this case we write $S = \langle a_1, \dots, a_r \rangle$. All semigroups admit a finite set of generators. For example, the Apéry set

$$A(S) = \{a \in S^* : a - v_2 \notin S^*\}.$$

EXAMPLE 3.7 (Semigroups generated by two elements). Let $a, b \in \mathbb{N}$, $a < b$. Let $\delta = \gcd(a, b)$. If $\delta \neq 1$ then $S = \langle a, b \rangle \subset \delta\mathbb{N}_0$ is not of finite genus. Assume $\delta = 1$. From Bézout theorem, every integer m can be written as $m = \lambda a + \mu b$. Adding and subtracting ab to both summands if necessary, we can obtain an unique representation of this type with $0 \leq \mu < a$. Then m is a pole when $\lambda \geq 0$ and a gap when $\lambda < 0$. In particular, the largest gap is $c - 1 = -a + (a - 1)b$. Let us show that the semigroup is symmetric. Suppose the largest gap is the sum of two gaps $-a + (a - 1)b = (\lambda_1 a + \mu_1 b) + (\lambda_2 a + \mu_2 b)$ with $\lambda_1, \lambda_2 < 0$, $0 \leq \mu_1, \mu_2 < a$. Then $(-\lambda_1 - \lambda_2 - 1)a = (\mu_1 + \mu_2 - a + 1)b$. Since $-\lambda_1 - \lambda_2 - 1 > 0$ we have $a | \mu_1 + \mu_2 - a + 1 < a$, a contradiction. Then the semigroup is symmetric and hence $c = 2g$. S has genus $g = (a - 1)(b - 1)/2$.

As a consequence of this example, a semigroup S has finite genus if and only if the greatest common divisor of its nonzero elements is 1. In this case there exist $a, b \in S$ such that $\gcd(a, b) = 1$ and $\langle a, b\rangle \subseteq S$.

The following fact will be used several times in what follows.

LEMMA 3.8. *Let S be a semigroup of finite genus. If $a \in S$ then*

$$\#(S \setminus (a + S)) = a.$$

PROOF. Let c be the conductor of S and m an integer. If $m \geq a + c$ then $m \in S$ and $m \in a + S$. Thus $S \setminus (a + S) = U \setminus V$, where $U = \{m \in S : m < a + c\}$ and $V = \{a + m : m \in S, a + m < a + c\} \subseteq U$. Clearly $\#U = a + c - g$ and $\#V = \#\{m \in S : m < c\} = c - g$, where g is the genus of S. Then $\#(S \setminus (a + S)) = \#U - \#V = a$. □

3.4. Codes from weights. Let R be an order domain over $\mathbb{F}_q$ and v a weight function on R. Let $H = H(v) = \{v_1, v_2, \dots\}$ be the semigroup of v. If $\delta = \gcd\{a : a \in H(v)^*\} = 1$ then the weight v is called *normal*. Otherwise we define the normalization of v as the weight $v' = v/\delta$. From now on, all weight functions will be normal.

For each $v_i \in H$ let $f_i \in R$ be such that $v(f_i) = v_i$. The ordered set $\mathcal{F} = \{f_1, f_2, \dots\}$ is a basis of R as a vector space over $\mathbb{F}_q$. For $m = -1, 0, 1, \dots$, we consider the linear subspaces

$$L(m) = \{f \in R : v(f) \leq m\}.$$

Clearly $L(-1) = (\mathbf{0}), L(0) = \mathbb{F}_q$ and $\{f_i : v_i \leq m\}$ is a basis of $L(m)$. Then $L(m-1) \subseteq L(m)$ with equality if m is a gap of H. Since v is normal, H has a finite number of gaps, g. So equality occurs precisely g times. If m is a pole, then $\dim(L(m)) = \dim(L(m-1)) + 1$.

Let $\Phi : R \to \mathbb{F}_q^n$ be a surjective morphism of $\mathbb{F}_q$-algebras (for example, an evaluation map). Then we obtain a chain of linear codes

$$(\mathbf{0}) \subseteq C(\Phi, 0) \subseteq C(\Phi, 1) \subseteq \dots \tag{3.1}$$

where $C(\Phi, m) = \Phi(L(m))$. Since Φ is surjective, the chain contains exactly $n + 1$ distinct codes. We define the *dimension set* of this chain as

$$M = M(\Phi, v) = \{m \in \mathbb{N}_0 : C(\Phi, m-1) \neq C(\Phi, m)\}.$$

It is clear that M consists of n integers. Write $M = \{m_1 = 0, m_2, \dots, m_n\}$. The name "dimension" set of M is justified by the following fact.

PROPOSITION 3.9. *uer $\dim(C(\Phi, m_k)) = k$. If m is a nonnegative integer then $\dim(C(\Phi, m)) = \max\{r : m_r \leq m\}$.*

PROOF. The first statement is clear. For the second one, if $m_k = \max\{r : m_r \leq m\}$ then $C(\Phi, m) = C(\Phi, m_k)$. □

Let m be an integer. If $m \notin H$ then $L(m) = L(m-1)$ hence $m \notin M$. If $m \in H$, take $f \in R$ such that $v(f) = m$. Then $L(m) = L(m-1) + \langle f\rangle$ so $C(\Phi, m) = C(\Phi, m-1) + \langle \Phi(f)\rangle$. Then $m \in M$ if and only if $\Phi(f) \notin C(\Phi, m-1)$.

The conditions of being Φ a morphism and v a weight, allow us to give estimates on the parameters of $C(\Phi, m)$. The ideal (f) generated by f is a linear subspace of R, hence we can consider the quotient ring $R/(f)$ as a vector space over $\mathbb{F}_q$.

LEMMA 3.10. *Let $f \in R$ be a nonzero element. If v is a weight function on R then* $\dim(R/(f)) = v(f)$.

PROOF. The weight v maps the ideal (f) into the set $v(f)+H$. Let $f_1, f_2, \ldots \in R$ be such that $v(f_i) = v_i$ and $f_i \in (f)$ when $v_i \in v(f) + H$. Then $\{f_1, f_2, \ldots\}$ is a basis of R and $\{f_i + (f) : v_i \notin v(f) + H\}$ is a basis of $R/(f)$. Thus $\dim(R/(f)) = \#(H \setminus (v(f) + H)) = v(f)$ by Lemma 3.8. □

LEMMA 3.11. *If $m < n$ then $L(m) \cap \ker(\Phi) = (0)$.*

PROOF. Let $f \in \ker(\Phi), f \neq 0$. Then $(f) \subseteq \ker(\Phi)$ and we have a well defined, linear, surjective map $\Phi : R/(f) \to \mathbb{F}_q^n$. Thus $\dim(R/(f)) \geq n$ and Lemma 3.10 implies $v(f) \geq n$, hence $f \notin L(m)$. □

PROPOSITION 3.12. *Let $m < n$ be a nonnegative integer.*

1. *$m \in M$ if and only if $m \in H$.*
2. *The code $C(\Phi, m)$ has dimension $k = \dim(L(m)) = \max\{i : v_i \leq m\}$ and minimum distance $d \geq n - m$. If the semigroup H has genus g and $2g \leq m < n$, then $k = m + 1 - g$.*

PROOF. If $m < n$ then the map $\Phi : L(m) \to \mathbb{F}_q^n$ is injective by Lemma 3.11. Then $m \in M$ if and only if $L(m-1) \neq L(m)$ that is if and only if $m \in H$. So $k = \dim(L(m)) = \max\{i : v_i \leq m\}$. Since H has g gaps, its conductor verifies $c \leq 2g$, so when $m \geq 2g$ we have $m = v_{m+1-g}$ implying $k = m + 1 - g$. Let us prove the statement about the minimum distance d. Let $\mathbf{c} = \Phi(f)$, $f \in L(m)$, be a codeword of $C(\Phi, m)$ with weight d. Let $I = \{1, \ldots, n\} \setminus \mathrm{supp}(\mathbf{c})$ be the set of zero coordinates of $\mathbf{c}$ and $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$ be the projection on the coordinates of I. The map $\pi \circ \Phi : R \to \mathbb{F}_q^{n-d}$ is a surjective morphism of algebras. Since $f \in L(m) \cap \ker(\pi \circ \Phi)$, Lemma 3.11 implies $m \geq n - d$ or equivalently $d \geq n - m$. □

The inequality $d(C(\Phi, m)) \geq n - m$ is the *Goppa bound* on the minimum distance of $C(\Phi, m)$.

3.5. The order and dual order bounds. Besides the Goppa bound, we can apply to $C(\Phi, m)$ and its dual $C(\Phi, m)^\perp$ the bounds of Theorems 2.4 and 2.7 respect to the sequence $\mathcal{C}_0 = (\mathbf{0}) \subset \mathcal{C}_1 \subset \cdots \subset \mathcal{C}_n$, obtained from the chain of equation 3.1 after deleting repeated codes. Since $\dim(\mathcal{C}_k) = k$, the map $\rho_{\mathcal{B}}$ defined in Section 2.3 can be written as

$$\rho(\mathbf{v}) = \min\{\dim(C(\Phi, m)) : \mathbf{v} \in C(\Phi, m)\}.$$

LEMMA 3.13. *Let $f \in R^*$.*

1. *$\rho(\Phi(f)) \leq \dim C(\Phi, v(f))$ with equality if $v(f) \in M$.*
2. *If $v(f) \notin M$ then $v(fh) \notin M$ for all $h \in R^*$.*

PROOF. (1) The first statement is clear since $f \in L(v(f))$ and hence $\Phi(f) \in C(\Phi, v(f))$. If $v(f) \in M$ then $\Phi(f) \in C(\Phi, v(f)) \setminus C(\Phi, (v(f) - 1))$ and $\rho(\Phi(f)) = \dim C(\Phi, v(f))$. (2) If $v(f) \notin M$ then $\Phi(f) \in C(\Phi, v(f) - 1)$ hence there exists $\psi \in L(v(f) - 1)$ such that $\Phi(f) = \Phi(\psi)$. If $v(fh) \in M$ then $\dim C(\Phi, v(fh)) = \rho(\Phi(fh)) = \rho(\Phi(\psi h)) \leq \dim C(\Phi, v(\psi h))$. Since $v(fh) > v(\psi h)$ we get the equality $C(\Phi, v(fh)) = C(\Phi, v(\psi h))$, contradicting our assumption $v(fh) \in M$. □

The equality $\rho(\Phi(f)) = \dim C(\Phi, v(f))$ is not true in general. Let $\bar{H} = H \setminus M$. Lemma 3.13(2) implies $\bar{H} + H \subseteq \bar{H}$, or equivalently $M \subseteq H \setminus (\bar{H} + H)$.

COROLLARY 3.14. $M \subseteq H \setminus (qH^* + H)$.

PROOF. Let $m \in H$, $m \neq 0$, and let $f \in R$ be such that $v(f) = m$. Then $v(f^q) = qv(f) > v(f)$. Since Φ is a morphism, we have $\Phi(f^q) = \Phi(f) * \cdots * \Phi(f)$(q times) $= \Phi(f)$. Thus $qm \notin M$. This proves $qH^* \subseteq \bar{H}$, so $qH^* + H \subseteq \bar{H} + H$ and $M \subseteq H \setminus (\bar{H} + H) \subseteq H \setminus qH^* + H)$. □

For $i = 1, \ldots, n$, let $\phi_i \in R$ be such that $v(\phi_i) = m_i$. The set $\mathcal{B} = \{\Phi(\phi_1), \ldots, \Phi(\phi_n)\}$ is a basis of $\mathbb{F}_q^n$ and the sequence of codes $(\mathcal{C}_k)$ is given by

$$\mathcal{C}_k = \langle \Phi(\phi_1), \ldots, \Phi(\phi_k) \rangle = C(\Phi, m_k),\ k = 1, \ldots, n.$$

PROPOSITION 3.15. *If $v_r + v_s = m_t \in M$ then $v_r, v_s \in M$ and $(\Phi(f_r), \Phi(f_s))$ is a well-behaving pair with $\rho(\Phi(f_r) * \Phi(f_s)) = t$.*

PROOF. If $v_r + v_s \in M$, Lemma 3.13(2) implies $v_r, v_s \in M$. Write $v_r = m_i, v_s = m_j$, so $\phi_i = f_r$ and $\phi_j = f_s$. We have

$$\rho(\Phi(\phi_i) * \Phi(\phi_j)) = \rho(\Phi(\phi_i\phi_j)) = \dim C(\Phi, v(\phi_i\phi_j)) = \dim C(\Phi, m_i + m_j).$$

If $(a, b) \prec (i, j)$ then $v(\phi_a\phi_b) < v(\phi_i\phi_j)$ and hence $\rho(\Phi(\phi_a) * \Phi(\phi_b)) = \rho(\Phi(\phi_a\phi_b)) < \dim C(\Phi, m_i + m_j) = \rho(\Phi(\phi_i) * \Phi(\phi_j))$. □

From Proposition 3.15 we can derive a new version of the order bounds on the minimum distance of $C(\Phi, m)$ and $C(\Phi, m)^\perp$ as follows. For $r = 1, \ldots, n$, $s = 0, \ldots, n-1$, consider the sets

$$\Lambda_r^* = \{(r, j) : m_r + m_j \in M\}\ ,\ N_s^* = \{(i, j) : m_i + m_j = m_{s+1}\}$$

Define

$$\begin{aligned} d_{ORD}(k) &= \min\{\#\Lambda_r^* : r = 1, \ldots, k\} \\ d_{ORD}^\perp(k) &= \min\{\#N_s^* : s = k, \ldots, n-1\}. \end{aligned}$$

By applying the bounds of Theorems 2.4 and 2.7 with respect to the basis $\{\Phi(\phi_1), \ldots, \Phi(\phi_n)\}$, we get the following result.

THEOREM 3.16. *For a non-negative integer m, we have*

$$\begin{aligned} d(C(\Phi, m)) &\geq d_{ORD}(\dim(C(\Phi, m))) \\ d(C(\Phi, m)^\perp) &\geq d_{ORD}^\perp(\dim(C(\Phi, m))). \end{aligned}$$

The inequalities stated in this theorem are the *order* (or *Feng-Rao*) bounds on the minimum distances of the primary code $C(\Phi, m)$ and its dual $C(\Phi, m)^\perp$, respectively. They do not depend on the basis $\mathcal{B}$ but only on the dimension set M.

3.6. Bibliographical notes. Order domains and evaluation codes were introduced and studied by T. Høholdt, J.H. van Lint and R. Pellikaan, [**27**]. The purpose was to simplify the theory of algebraic geometry codes and to formulate the order bound on the minimum distance in this language. This bound was first suggested by G.L. Feng and T.N.T. Rao in [**13**] for the duals of one-point algebraic geometry codes. At the same time, R. Matsumoto and S. Miura independently developed many of the same ideas for duals of one-point codes. They also formulated the Feng-Rao bound for any linear code defined by means of its parity check matrix, [**35**]. Another generalization to all linear codes described by means of generator matrices, was given by Andersen and Geil, [**1**]. That paper is primarily devoted to linear codes, but also the cases of codes from order domains and affine variety

codes are treated. This is the bound we have stated in Theorem 2.4. Many works have been devoted to study the relations between these bounds and to generalize them, see [**21**] and the references therein.

Our presentation of order domains follows closely [**27**]. In our exposition we have limited ourselves to consider weights v whose semigroup $H(v)$ is a subsemigroup of $\mathbb{N}_0$. If more general semigroups are allowed (for example, subsemigroups of $\mathbb{N}_0^r$ for some r), then the family of obtained codes is very enlarged. See [**19, 21**].

4. Codes from Algebraic Geometry

Some of the most interesting examples of evaluation codes are obtained from algebraic curves. This section is devoted to developing a basic introduction to algebraic geometry codes.

4.1. Algebraic curves. It is not our intention here to explain the theory of algebraic curves, which can be found in many excellent books (eg. [**15, 27, 45**]). Therefore we assume a certain familiarity of the reader with algebraic geometry and we simply recall the basic ingredients we need to cook our codes.

An *algebraic curve* $\mathcal{X}$ over $\mathbb{F}_q$ is an absolutely irreducible algebraic variety of dimension one over $\mathbb{F}_q$. The set of rational points of $\mathcal{X}$ is denoted $\mathcal{X}(\mathbb{F}_q)$. Algebraic geometry codes will be obtained through evaluation of rational functions of $\mathcal{X}$ at (some) points in $\mathcal{X}(\mathbb{F}_q)$, so we always refer to curves with $\mathcal{X}(\mathbb{F}_q) \neq \emptyset$. Let $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions of $\mathcal{X}$. Among all curves having $\mathbb{F}_q(\mathcal{X})$ as a function field, there is (up to isomorphism) one nonsingular projective curve. We shall use this one for our code construction. Thus, in what follows, the word *curve* means an algebraic, projective, absolutely irreducible, nonsingular curve (although we eventually use singular plane models of such a curve for our computations).

Points on $\mathcal{X}$ correspond to valuation rings in its function field. Given a function $f \neq 0$, the *order* of f at a point P of $\mathcal{X}$ is the integer $v_P(f)$, where v_P is the discrete valuation corresponding to the valuation ring of P. If $v_P(f) < 0$ then P is a *pole* and if $v_P(f) > 0$ then P is a *zero* of f. The divisor of f is $\operatorname{div}(f) = \sum_{P \in \mathcal{X}} v_P(f) P$.

Given a rational divisor G of $\mathcal{X}$, we consider the vector space of functions having zeros and poles specified by G

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : \operatorname{div}(f) + G \geq 0\} \cup \{0\}.$$

The dimension of this space is denoted by $\ell(G)$. Riemann-Roch theorem states that there is a constant g (the *genus* of $\mathcal{X}$) such that $\ell(G) = \deg(G) + 1 - g + \ell(W - G)$, where W is a canonical divisor. Since canonical divisors have degree $2g-2$, it holds that $\ell(G) = \deg(G) + 1 - g$ when $\deg(G) > 2g - 2$.

Two divisors G and G' are *linearly equivalent*, denoted $G \sim G'$, if there is rational function ϕ with $\operatorname{div}(\phi) = G - G'$. In this case $\mathcal{L}(G)$ and $\mathcal{L}(G')$ are isomorphic via the map $f \mapsto \phi f$.

The gonality of the curve $\mathcal{X}$ over $\mathbb{F}_q$ is the smallest degree γ of a non-constant morphism from $\mathcal{X}$ to the projective line. Equivalently γ is the smallest degree of a rational divisor G such that $\ell(G) > 1$. More generally, the gonality sequence of $\mathcal{X}$, $GS(\mathcal{X}) = \{\gamma_i : i = 1, 2, \dots\}$, is defined by

$$\gamma_i = \min\{\deg(G) : \ell(G) \geq i\}.$$

Then $\gamma_1 = 0$ and γ_2 is the usual gonality. Since $\ell(G) \leq \deg(G) + 1$ when $\deg(G) \geq 0$, we have $\gamma_i \geq i - 1$. Conversely, from Riemann-Roch theorem it follows that $\gamma_i \leq i - 1 + g$ with equality for $i > g$. The gonality sequence $GS(\mathcal{X})$ verifies a symmetry property (similar to the symmetry property for semigroups): for every integer r, it holds that $r \in GS(\mathcal{X})$ if and only if $2g - 1 - r \notin GS(\mathcal{X})$, cf. [**37**]. In general, computing $GS(\mathcal{X})$ is a difficult task but for plane curves this sequence is entirely known and depends only on the degree of $\mathcal{X}$, see [**43**].

4.2. Algebraic geometry codes. Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$ and let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct rational points on $\mathcal{X}$. Let G be a rational divisor of nonnegative degree and support disjoint from $D = P_1 + \cdots + P_n$. The *algebraic geometry* code (or AG code) $C(\mathcal{X}, D, G)$ is the image of the evaluation map

$$ev_{\mathcal{P}} : \mathcal{L}(G) \to \mathbb{F}_q^n \qquad ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

$ev_{\mathcal{P}}$ is a linear map whose kernel is $\mathcal{L}(G - D)$. The dimension of this kernel $a = \ell(G - D)$ is the *abundance* of $C(\mathcal{X}, D, G)$. In particular, if $\deg(G) < n$ then $a = 0$ and hence $C(\mathcal{X}, D, G) \cong \mathcal{L}(G)$. The parameters of this code are as follows.

THEOREM 4.1. *The code $C(\mathcal{X}, D, G)$ has dimension $k = \ell(G) - \ell(G - D)$ and minimum distance $d \geq n - \deg(G) + \gamma_{a+1}$. In particular, when $2g - 2 < \deg(G) < n$, then $k = \deg(G) + 1 - g$ and $d \geq n - \deg(G)$.*

PROOF. The statements about the dimension follow from the definition of $C(\mathcal{X}, D, G)$ and the Riemann-Roch theorem. To see the bound on the minimum distance, let $\mathbf{c}$ be a codeword of weight $d > 0$. Let $D' \leq D$ be the divisor obtained as the sum of points in $\mathcal{P}$ corresponding to the $n - d$ zero coordinates of $\mathbf{c}$. There exist a function $f \in \mathcal{L}(G - D') \setminus \mathcal{L}(G - D)$ such that $\mathbf{c} = ev_{\mathcal{P}}(f)$. Then $\ell(G - D') \geq \ell(G - D) + 1 = a + 1$ hence, by definition of gonality sequence, $\gamma_{a+1} \leq \deg(G - D') = \deg(G) - (n - d)$. □

The weaker bound $d \geq d_G(C(\mathcal{X}, D, G)) = n - \deg(G)$ is often called the *Goppa bound* on the minimum distance. Note that it is similar to the bound on the minimum distance of Reed-Solomon codes seen in Example 3.2 and the Goppa bound for codes coming from order domains. The bound on d stated in Theorem 4.1, $d \geq n - \deg(G) + \gamma_{a+1}$, is sometimes referred as the *improved Goppa bound*.

PROPOSITION 4.2. *$d(C(\mathcal{X}, D, G)) = n - \deg(G)$ if an only if there exists a divisor $D', 0 \leq D' \leq D$ such that $G \sim D'$.*

PROOF. As in the proof of Theorem 4.1, $d = n - \deg(G)$ if an only if there exists a divisor $D', 0 \leq D' \leq D$ such that $\ell(G - D') > 0$. Since G and D' have the same degree, this happens if and only if $G \sim D'$. □

From Theorem 4.1, the parameters of $C(\mathcal{X}, D, G)$ verify $k + d \geq \ell(G) - \deg(G) + n$. According to Riemann-Roch theorem, a simple computation shows that this inequality implies

$$n + 1 - g \leq k + d \leq n + 1 \tag{4.1}$$

where the right-hand inequality is the Singleton bound. The number $n + 1 - k - d$ is the *Singleton defect* of $C(\mathcal{X}, D, G)$. Recall that $n + 1 - k - d \leq g$ and that codes of Singleton defect 0 are MDS.

EXAMPLE 4.3. Take $\mathcal{X} = \mathbb{P}^1$ the projective line over $\mathbb{F}_q$. Let Q be the point at infinity and $\mathcal{P}$ the set of $n = q$ affine points. Then $C(\mathbb{P}^1, D, mQ)$, $1 \leq m \leq q$, is precisely the Reed-Solomon code of dimension $k = m + 1$. Since $g = 0$, it is a MDS code.

Thus AG codes can be seen as generalizations of RS codes: instead of the projective line $\mathbb{P}^1$, consider an arbitrary curve $\mathcal{X}$ over $\mathbb{F}_q$. Note that Reed-Solomon codes have excellent parameters k and d, but too small length (consider the case $q = 2$). According to the Hasse-Weil bound, cf. [**45**], we have

$$|\#\mathcal{X}(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

hence longer codes can be obtained by using curves of higher genus, although then the Singleton defect increases. From equation 4.1, the relative parameters verify

$$\frac{k}{n} + \frac{d}{n} \geq 1 - \frac{g}{n}$$

so one way to get better codes from curves of high genus is to take n large with respect to g. This strategy requires curves with many points respect to its genus.

EXAMPLE 4.4 (Codes on the Klein Quartic). Let us consider the curve $\mathcal{X}$ defined over $\mathbb{F}_8$ by the projective equation $X^3Y + Y^3Z + Z^3X = 0$. $\mathcal{X}$ is called the *Klein quartic*. It is a nonsingular plane curve, hence its genus is 3 by Plücker's formula. A direct inspection shows that $\mathcal{X}$ has 24 rational points, which is the maximum possible number allowed by the Serre's improvement on the Hasse-Weil bound,

$$|\#\mathcal{X}(\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Consider the points $Q_0 = (1:0:0), Q_1 = (0:1:0), Q_2 = (0:0:1) \in \mathcal{X}(\mathbb{F}_8)$ and the divisor $G = m(Q_0 + Q_1 + Q_2)$, for $m = 2, \ldots, 6$. Let $\mathcal{P}$ be the set of 21 rational points different from Q_1, Q_2, Q_3 and let D be the sum of all these points. The algebraic geometry code $C(\mathcal{X}, D, G)$ was first studied in [**25**]. According to Theorem 4.1 it has dimension $k = 3m - 2$ and minimum distance $d \geq 21 - 3m$. Note that for other values of m the parameters of the obtained codes are much more difficult to estimate (try it!). For $m = 3, 4$, no codes are known improving these parameters, see [**34**]. Take, for example, $m = 4$. Then $\ell(4(Q_0 + Q_1 + Q_2)) = 10$. The following ten functions

$$\frac{X^3}{T}, \frac{X^2Y}{T}, \frac{X^2Z}{T}, \frac{XY^2}{T}, \frac{XYZ}{T}, \frac{XZ^2}{T}, \frac{Y^3}{T}, \frac{Y^2Z}{T}, \frac{YZ^2}{T}, \frac{Z^3}{T},$$

where $T = XYZ$, belong to $\mathcal{L}(4(Q_0+Q_1+Q_2))$ and are linearly independent, hence they form a basis of $\mathcal{L}(4(Q_0 + Q_1 + Q_2))$. A generator matrix of $C(\mathcal{X}, D, 4(Q_0 + Q_1 + Q_2))$ is obtained by evaluating these functions at all points of $\mathcal{P}$.

4.3. Isometric codes. An *isometry* of $\mathbb{F}_q^n$ is a linear map $l : \mathbb{F}_q^n \to \mathbb{F}_q^n$ leaving the Hamming metric invariant, $d(\mathbf{u}, \mathbf{v}) = d(l(\mathbf{u}), l(\mathbf{v}))$. Thus an isometry is an isomorphism. Two codes $\mathcal{C}, \mathcal{C}'$ of length n are *isometric* if there is an isometry l such that $l(\mathcal{C}) = \mathcal{C}'$. Clearly isometric codes have equal parameters n, k, d and similar properties.

Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a n-tuple of nonzero elements of $\mathbb{F}_q^n$ and $\sigma \in \mathcal{S}_n$, the symmetric group on n elements. The maps $\mathbf{x} : \mathbf{v} \mapsto \mathbf{x} * \mathbf{v}$ and $\sigma : \mathbf{v} \mapsto (v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ are isometries. Conversely, it can be proved (and it is left as an exercise to the reader) that any isometry l can be written as $l = \mathbf{x} \circ \sigma$, where $\mathbf{x} \in (\mathbb{F}_q^*)^n$ and $\sigma \in \mathcal{S}_n$.

PROPOSITION 4.5. *Let $\sigma \in \mathcal{S}_n$ and $D_\sigma = P_{\sigma(1)} + \cdots + P_{\sigma(n)}$. Let G, G' be two rational divisors such that $\mathrm{supp}(G) \cap \mathcal{P} = \mathrm{supp}(G') \cap \mathcal{P} = \emptyset$. If $G \sim G'$ then the codes $C(\mathcal{X}, D, G)$ and $C(\mathcal{X}, D_\sigma, G')$ are isometric.*

PROOF. If $G \sim G'$ then there exists a rational function ϕ such that $G - G' = \mathrm{div}(\phi)$ and $\mathcal{L}(G) = \{\phi f : f \in \mathcal{L}(G')\}$. Thus $C(\mathcal{X}, D, G) = ev_{\mathcal{P}}(\phi) * C(\mathcal{X}, D, G') = ev_{\mathcal{P}}(\phi) * \sigma^{-1}(C(\mathcal{X}, D_\sigma, G'))$. □

A converse of Proposition 4.5 is also true under some supplementary conditions on n, see [**36**].

4.4. Duality. The dual of an algebraic geometry code is again an AG code.

THEOREM 4.6. *There exists a differential form ω with simple poles and residue 1 at every point $P_i \in \mathcal{P}$. If W is the divisor of ω, then*

$$C(\mathcal{X}, D, G)^\perp = C(\mathcal{X}, D, D + W - G).$$

PROOF. (Sketch) The existence of such form ω is guaranteed by the independence of valuations, see [**45**], Chapter I. The map $\mathcal{L}(D + W - G) \to \Omega(G - D)$, $\phi \mapsto \phi\omega$ is a well defined isomorphism of vector spaces. Furthermore

$$\phi(P_i) = \phi(P_i)\mathrm{res}_{P_i}(\omega) = \mathrm{res}_{P_i}(\phi\omega)$$

where $\mathrm{res}_P(\eta)$ denotes the residue at P of the differential form η. Let $\mathbf{u} \in C(\mathcal{X}, D, G)$, $\mathbf{v} \in C(\mathcal{X}, D, D + W - G)$ and write $\mathbf{u} = ev_{\mathcal{P}}(f), \mathbf{v} = ev_{\mathcal{P}}(\phi)$. Then

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} f(P_i)\phi(P_i) = \sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\phi\omega) = \sum_{i=1}^{n} \mathrm{res}_{P_i}(f\phi\omega).$$

Since $\mathrm{div}(f) \geq -G$ and $\mathrm{div}(\phi\omega) \geq G - D$, we have $\mathrm{div}(f\phi\omega) \geq -D$, so $f\phi\omega$ has no poles outside $\mathrm{sop}(D)$. Then

$$\sum_{i=1}^{n} \mathrm{res}_{P_i}(f\phi\omega) = \sum_{P \in \mathcal{X}} \mathrm{res}_P(f\phi\omega) = 0$$

where the right-hand equality follows from the Residue theorem ([**45**], Corollary IV.3.3). Finally, since $\dim(C(\mathcal{X}, D, G)) + \dim(C(\mathcal{X}, D, D + W - G)) = n$, we get the result. □

4.5. One-point codes and Weierstrass semigroups. If G is a multiple of a single rational point Q of $\mathcal{X}$ and $\mathcal{P}$ is the set of rational points on $\mathcal{X}$ different from Q, then the code $C(\mathcal{X}, D, mQ)$ is called *one-point*. These codes are, in general, easier to study than the others.

The space $\mathcal{L}(mQ)$ is the set of rational functions with poles only at Q of order at most m. The set of rational functions with poles only at Q

$$\mathcal{L}(\infty Q) = \bigcup_{m=0}^{\infty} \mathcal{L}(mQ)$$

is an $\mathbb{F}_q$-algebra. The evaluation map $ev_{\mathcal{P}}$ is thus a morphism of $\mathbb{F}_q$-algebras. As the dimension of $C(\mathcal{X}, D, (n+2g-1)Q)$ is $k = l((n+2g-1)Q) - l((n+2g-1)Q - D) = n$, we have $C(\mathcal{X}, D, (n + 2g - 1)Q) = \mathbb{F}_q^n$ and $ev_{\mathcal{P}}$ is surjective. On the other hand, from the properties of valuations it follows that $-v_Q$ is a weight function on $\mathcal{L}(\infty Q)$

and this algebra becomes an order domain. So the theory developed in Section 3.4 can be applied. In particular, the chain of codes stated in equation 3.1, becomes

$$(\mathbf{0}) \subseteq C(\mathcal{X}, D, 0) \subseteq C(\mathcal{X}, D, Q) \subseteq C(\mathcal{X}, D, 2Q) \subseteq \cdots \subseteq C(\mathcal{X}, D, mQ) \subseteq \cdots$$

For simplicity we shall write v instead $-v_Q$ and ev instead $ev_{\mathcal{P}}$ whenever the point Q and the set $\mathcal{P}$ are fixed. Also in order to simplify the exposition

from now on we shall assume $n \geq 2g$

(otherwise we must distinguish several cases, which makes the exposition very cumbersome). The semigroup associated to the weight v,

$$H(v) = \{v(f) : f \in \mathcal{L}(\infty Q), f \neq 0\}$$

is now denoted $H(Q)$ and called the *Weierstrass semigroup* of Q. As it happens for general weight functions, $m \in H(Q)$ iff $l(mQ) \neq l((m-1)Q)$ (and thus $l(mQ) = l((m-1)Q)+1$). Then, when m is a gap we have $C(\mathcal{X}, D, mQ) = C(\mathcal{X}, D, (m-1)Q)$. From Riemann-Roch theorem it holds that $l(2gQ) = g+1$ hence $H(Q)$ has the same genus g as the curve $\mathcal{X}$. Since $l((2g-1)Q) = g$, then $H(Q)$ is symmetric when $l((2g-2)Q) = g$, that is when $(2g-2)Q$ is a canonical divisor.

EXAMPLE 4.7 (Hermitian curves). Consider the curve $\mathcal{H}$ defined over the field $\mathbb{F}_{q^2}$ by the affine equation

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

$\mathcal{H}$ is called the *Hermitian curve*. Codes arising from this curve are the most studied among all AG codes. $\mathcal{H}$ is a nonsingular plane curve, hence its genus is $g = q(q-1)/2$. Let us compute its rational points. $\mathcal{H}$ has exactly one point at infinity $Q = (0 : 1 : 0)$, which is the common pole of x and y. The map $\beta \mapsto \beta^q + \beta$ is the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and hence it is $\mathbb{F}_q$-linear and surjective. Let $\alpha \in \mathbb{F}_{q^2}$. Since $\alpha^{q+1} \in \mathbb{F}_q$, we deduce that the polynomial $T^q + T = \alpha^{q+1}$ has q different roots β in $\mathbb{F}_{q^2}$. Then the line $x = \alpha$ intersects $\mathcal{H}$ at q different affine points, which are rational over $\mathbb{F}_{q^2}$. In terms of divisors

$$\operatorname{div}(x-\alpha) = \sum_{\beta \in \mathbb{F}_{q^2}, \beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} - qQ$$

where $P_{\alpha,\beta} = (\alpha : \beta : 1)$. A similar reasoning proves that when $\beta^q + \beta \neq 0$, we have

$$\operatorname{div}(y-\beta) = \sum_{\alpha \in \mathbb{F}_{q^2}, \alpha^{q+1}=\beta^q+\beta} P_{\alpha,\beta} - (q+1)Q.$$

In particular, from the first equality and since we have q^2 choices for α, we deduce that $\mathcal{H}$ has q^3 rational affine points, that is q^3+1 rational points in total. Then $\mathcal{H}$ has the maximum possible number of rational points according to its genus as it achieves the Hasse-Weil upper bound. It is a *maximal* curve.

Let us compute the Weierstrass semigroup $H(Q)$. Once the divisors $\operatorname{div}(x-\alpha)$ and $\operatorname{div}(y-\beta)$ are known, we deduce that q and $q+1$ are pole numbers, hence $\langle q, q+1\rangle \subseteq H(Q)$. According to Example 3.7, the semigroup $\langle q, q+1\rangle$ has genus $g = q(q-1)/2 = g(\mathcal{H})$. Then we get equality $H(Q) = \langle q, q+1\rangle$. In particular this semigroup is symmetric.

EXAMPLE 4.8 (Hermitian codes). One-point codes over $\mathbb{F}_{q^2}$ coming from Hermitian curves are called *Hermitian codes*. Let Q be the point at infinity and $\mathcal{P}$ be the set of all $n = q^3$ affine points on $\mathcal{H}$. Hermitian codes are the AG codes

$$C(\mathcal{H}, D, mQ) = ev(\mathcal{L}(mQ))$$

$m = 0, 1, 2, \ldots$. To describe these codes explicitly we must determine the spaces of rational functions $\mathcal{L}(mQ)$ and $\mathcal{L}(\infty Q)$. The Weierstrass semigroup can be a useful tool to accomplish this task. Write $H(Q) = \{v_1 = 0, v_2 \ldots\}$ as an increasing enumeration of its elements. A basis of $\mathcal{L}(\infty Q)$ is a set of functions $\{f_i : i \in \mathbb{N}\}$ such that $v(f_i) = v_i$, see Proposition 3.4. If $m \in H(Q)$ then m can be written as a linear combination $m = \lambda q + \mu(q+1)$, where λ and μ are nonnegative integers and $\mu < q$. Then $v(x^\lambda y^\mu) = m$. It follows that a basis of $\mathcal{L}(\infty Q)$ is

$$\{x^\lambda y^\mu : 0 \leq \lambda, 0 \leq \mu < q\}$$

and a basis of $\mathcal{L}(mQ)$ is

$$\{x^\lambda y^\mu : 0 \leq \lambda, 0 \leq \mu < q, \lambda q + \mu(q+1) \leq m\}.$$

The parameters of these codes can be estimated from the arithmetic of $\mathcal{H}$. For example, let us show that for small values of $m \in H$, the minimum distance of $C(\mathcal{H}, D, mQ)$ attains the Goppa bound. Let $\alpha \in \mathbb{F}_{q^2}^*$ and let $\alpha_1, \ldots \alpha_{q+1}$ be the roots of $T^{q+1} = \alpha^{q+1}$. These roots belong to $\mathbb{F}_{q^2}$ and are pairwise distinct, so we can write $\mathbb{F}_{q^2} = \{\alpha_1, \ldots, \alpha_{q+1}, \alpha_{q+2}, \ldots, \alpha_{q^2}\}$. Let $\beta_1, \ldots, \beta_q$ be the roots of $T^q + T = \alpha^{q+1}$. Then for $i > q+1$, the affine points (α_i, β_j) are not in $\mathcal{H}(\mathbb{F}_{q^2})$. Let λ, μ be two integers such that $0 \leq \lambda < q^2 - q, 0 \leq \mu < q$ and let $m = \lambda q + \mu(q+1)$. Then $m \in H, m < n$ and the function

$$f = \prod_{i=1}^{\lambda} (x - \alpha_{q+1+i}) \prod_{j=1}^{\mu} (y - \beta_j)$$

verifies $\mathrm{div}(f) = D' - mQ$, with $0 \leq D' \leq D$. Then, according to Proposition 4.2, the code $C(\mathcal{H}, D, mQ)$ attains the Goppa bound, $d(C(\mathcal{H}, D, mQ)) = n - m$. Since all poles $m \in H$ such that $m < n - q^2$ can be written in the form $m = \lambda q + \mu(q+1)$ with $0 \leq \lambda, 0 \leq \mu < q$, we deduce that all Hermitian codes $C(\mathcal{H}, D, mQ)$ attain the Goppa bound for $m < n - q^2$. The same happens when $m < n$ is a multiple of q, $m = \lambda q$. To see that it is enough to consider the function

$$f = \prod_{i=1}^{\lambda} (x - \alpha_i).$$

We shall compute the minimum distances of all nonabundant Hermitian codes later, seeing them as particular cases of Castle codes.

The same reasoning as in the above example shows that for an arbitrary curve $\mathcal{X}$ the ring $\mathcal{L}(\infty Q)$ is a finitely generated $\mathbb{F}_q$-algebra. Take a generator set $\{a_1, \ldots, a_r\}$ of $H(Q)$ and functions $\psi_1, \ldots, \psi_r$ such that $v(\psi_i) = a_i$ for $i = 1, \ldots, r$. Then every element in $H(Q)$ is a combination of $a_1, \ldots, a_r$ with nonnegative integer coefficients, hence $\mathcal{L}(\infty Q) = \mathbb{F}_q[\psi_1, \ldots, \psi_r]$.

4.6. The dimension set and the order bound on the minimum distance. Keeping the notation of previous sections, let $\mathcal{X}$ be a curve of genus g defined over the finite field $\mathbb{F}_q$ and let $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ be the rational points in $\mathcal{X}$. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$. Consider the chain of one-point codes $(\mathbf{0}) \subseteq C(\mathcal{X}, D, 0) \subseteq \cdots \subseteq C(\mathcal{X}, D, (n+2g-1)Q) = \mathbb{F}_q^n$.

The dimensions of these codes can be obtained from the dimension set $M = \{m_1, \ldots, m_n\}$. Let $H = H(Q) = \{v_1 = 0 < v_2 < \ldots\}$ be the Weierstrass semigroup of Q and let $\mathrm{Gaps}(H) = \{l_1, \ldots, l_g\}$ be the set of gaps of H. Let us remember that

$$M = \{m \in \mathbb{N}_0 : C(\mathcal{X}, D, mQ) \neq C(\mathcal{X}, D, (m-1)Q)\}.$$

PROPOSITION 4.9. $M = \{m \in H : \ell(mQ - D) = \ell((m-1)Q - D)\}$.

PROOF. If $m \in M$ then $\ell(mQ) \neq \ell((m-1)Q)$ and $m \in H$. The kernel of the evaluation map restricted to $\mathcal{L}(mQ)$ is $\mathcal{L}(mQ - D)$, so when $m < n$ this evaluation is injective and hence $m \in M$ if and only if $m \in H$. When $m \geq n$ then $m-1, m \in H$ which implies $\ell(mQ) = \ell((m-1)Q) + 1$. Thus $C(\mathcal{X}, D, mQ) \neq C(\mathcal{X}, D, (m-1)Q)$ if and only if both kernels are equal. □

Thus, for all nonnegative integers $m < n$ we have $m \in M$ if and only if $m \in H$. Then, once H is known, the problem of calculating M is reduced to determine its last g elements. Since $C(\mathcal{X}, D, (n+2g-1)Q) = \mathbb{F}_q^n$ we deduce that g elements of $\{n, \ldots, n+2g-1\}$ belong to M while the other g elements do not.

PROPOSITION 4.10. *If the divisors D and nQ are linearly equivalent, $D \sim nQ$, then $M \cap \{n, \ldots, n+2g-1\} = \{n + l_1, \ldots, n + l_g\}$.*

PROOF. If $D \sim nQ$ then $n \notin M$ and $n + v_1, \ldots, n + v_g \notin M$ by the remark after Lemma 3.13. The statement follows by cardinality reasons. □

EXAMPLE 4.11 (Hermitian codes). As seen in Example 4.16, we have $D \sim nQ$. Then Proposition 4.10 gives M.

We can obtain estimates on the minimum distance of one-point codes by using the order bound stated in Theorem 3.16:

$$d(C(\mathcal{X}, D, mQ)) \geq d_{ORD}(\dim(C(\mathcal{X}, D, mQ))).$$

This bound improves the classical Goppa bound $d(C(\mathcal{X}, D, mQ)) \geq d_G(C(\mathcal{X}, D, mQ)) = n - m$ as the next result shows. Let π be the smallest element in $\bar{H} = H \setminus M$. Note that $\pi \geq n$. The sets Λ_i^* can be rewritten as $\Lambda_i^* = \{m_j \in M : m_i + m_j \in M\}$ or, since $\bar{H} + H \subseteq \bar{H}$ as noted after Lemma 3.13, as $\Lambda_i^* = \{m \in M : m - m_i \in H\} = (m_i + H) \cap M$.

PROPOSITION 4.12. *For all $i = 1, \ldots, n$, we have $d_{ORD}(\dim(C(\mathcal{X}, D, m_iQ))) \geq d_G(C(\mathcal{X}, D, m_iQ))$. If $m_i < \pi - l_g$ then equality holds.*

PROOF. For the first statement it suffices to show that $\#(M \setminus \Lambda_i^*) \leq m_i$ for all i. Since $\Lambda_i^* = (m_i + H) \cap M$, we have $M \setminus \Lambda_i^* \subseteq H \setminus (m_i + H)$ and this follows from the fact that $\#(H \setminus (m_i + H)) = m_i$, stated in Lemma 3.8. If $m_i + l_g < \pi$, then all elements in $H \setminus (m_i + H)$ are smaller than π and hence $M \setminus \Lambda_i^* = H \setminus (m_i + H)$. □

EXAMPLE 4.13 (Codes on the Suzuki curve). The Suzuki curve $\mathcal{S}$ is characterized as being the unique curve over $\mathbb{F}_q$, with $q = 2q_0^2$, and $q_0 = 2^r \geq 2$, of genus $g = q_0(q-1)$ having $q^2 + 1$ $\mathbb{F}_q$-rational points, see [**16**]. Without going into details, which would lead us too long, a plane singular model of $\mathcal{S}$ is given by the equation

$y^q - y = x^{q_0}(x^q - 1)$. Thus, there is just one point Q over $x = \infty$ which is $\mathbb{F}_q$-rational. The Weierstrass semigroup of Q is known to be $H(Q) = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$ (see [**26, 32**]).

Let us consider the particular case $q = 8$. In this case the Suzuki curve has genus $g = 14$ and 65 rational points. A plane model of $\mathcal{S}$ is given by the equation $y^8z^2 - yz^9 = x^2(x^8 - xz^7)$. This model is non-singular except at the point $(0 : 1 : 0)$. Being this singularity unibranched, the unique point Q lying over $(0 : 1 : 0)$ is rational. Let us consider the codes $C(\mathcal{S}, D, mQ)$, where D is the sum of all 64 rational points of $\mathcal{S}$ except Q. The Weierstrass semigroup at Q is

$$\begin{aligned} H &= \langle 8, 10, 12, 13\rangle \\ &= \{0, 8, 10, 12, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26, 28, \rightarrow\}. \end{aligned}$$

Then

$$\begin{aligned} qH^* + H &= \{qv_i + v_j : v_i, v_j \in H, v_i \neq 0\} \\ &= \{64, 72, 74, 76, 77, 80, 82, 84, 85, 86, 87, 88, 89, 90, 92, \rightarrow\}. \end{aligned}$$

By Corollary 3.14, $M \subseteq H \setminus (qH^* + H)$, so we obtain

$$\begin{aligned} M \subseteq \{&0, 8, 10, \ldots (\text{same as } H) \ldots, 63, \\ &65, 66, 67, 68, 69, 70, 71, 73, 75, 78, 79, 81, 83, 91\}. \end{aligned}$$

Since both sets have cardinality $n = 64$ we conclude that they are equal. An straightforward computation gives the sequence ($\#\Lambda_i^*$, $1 \leq i \leq 64$): (64, 56, 54, 52, 51, 48, 46, 44, 43, 42, 41, 40, 39, 38, 36, 35, 34, 33, 32, 31, 30, 29, 28, 28, 26, 25, 24, 23, 22, 21, 20, 21, 18, 19, 16, 17, 16, 13, 12, 14, 10, 13, 8, 12, 10, 9, 8, 8, 6, 8, 7, 4, 5, 4, 4, 4, 5, 4, 3, 2, 2, 2, 2, 1). We find 14 nonabundant codes ($m < 64$) for which the Goppa bound is improved (plus all the abundant ones). Specifically those corresponding to the values $m_i \in \{37, 45, 47, 49, 50, 53, 55, 57, 58, 59, 60, 61, 62, 63\}$. In particular we find four codes $[64, 37, \geq 16]$, $[64, 58, \geq 4]$, $[64, 62, \geq 2]$ and $[64, 63, \geq 2]$ achieving the best known parameters, see [**34**].

4.7. Duals of one-point codes. The dual of an one-point code is not one-point in general. According to Proposition 4.6 we have $C(\mathcal{X}, D, mQ)^\perp = C(\mathcal{X}, D, D + W - mQ)$, where W is the divisor of a differential form ω with simple poles and residue 1 at all points $P_i \in \mathcal{P}$. Then we have the following result.

PROPOSITION 4.14. *If there exist a differential form ω with simple poles and residue 1 at all points $P_i \in \mathcal{P}$, such that* $\operatorname{div}(\omega) = (n + 2g - 2)Q - D$ *then* $C(\mathcal{X}, D, mQ)^\perp = C(\mathcal{X}, D, (n + 2g - 2 - m)Q)$.

In this case, the dual of an one-point code $C(\mathcal{X}, D, mQ)$ is again an one-point code, $C(\mathcal{X}, D, mQ)^\perp = C(\mathcal{X}, D, (n + 2g - 2 - m)Q)$. Thus we get two order bounds on the minimum distance of this code, namely $d_{ORD}(\dim C(\mathcal{X}, D, mQ))$ and $d^\perp_{ORD}(\dim C(\mathcal{X}, D, (n + 2g - 2 - m)Q))$. Both bounds give the same result.

PROPOSITION 4.15. *If there exist a differential form ω with simple poles and residue 1 at all points $P_i \in \mathcal{P}$, such that* $\operatorname{div}(\omega) = (n + 2g - 2)Q - D$, *then* $d_{ORD}(\dim C(\mathcal{X}, D, mQ)) = d^\perp_{ORD}(\dim C(\mathcal{X}, D, (n + 2g - 2 - m)Q))$.

The proof of this result can be found in [**22**].

EXAMPLE 4.16 (Duals of Hermitian and Suzuki codes). Consider the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$. The function

$$f = \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha)$$

has divisor $\operatorname{div}(f) = D - q^3 Q$, where D is the sum of all $n = q^3$ rational affine points on $\mathcal{H}$. Then $\operatorname{div}(f) = D - nQ$. It can be proved (see [**44**]) that $\operatorname{div}(df/f) = (n+2g-2)Q - D$. Thus $C(\mathcal{H}, D, mQ)^{\perp} = C(\mathcal{H}, D, (n+2g-2-m)Q)$. Analogously, for the Suzuki curve $\mathcal{S}$ over $\mathbb{F}_q$, the function

$$f = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

verifies $\operatorname{div}(f) = D - nQ$ and $\operatorname{div}(df/f) = (n + 2g - 2)Q - D$. Then the dual of an one-point Suzuki code is one-point too.

4.8. Improved codes. By choosing suitable functions f to be evaluated, in some cases we can slightly change one-point codes improving their parameters. Let δ be an integer, $0 < \delta \leq n$. Let $\mathcal{X}, \mathcal{P}, Q$ as in the previous sections. Given functions $\phi_1, \ldots, \phi_n$ such that $\phi_i \in \mathcal{L}(\infty Q)$ and $v(\phi_i) = m_i$, we define the *improved code*

$$C(D, Q, \delta) = \langle \{ ev(\phi_i) : \#\Lambda_i^* \geq \delta \} \rangle.$$

From Proposition 2.3 it is clear that the minimum distance of $C(D, Q, \delta)$ is at least δ. The sequence (Λ_i^*) is said to be *monotone* for δ if for every i, j such that $\#\Lambda_i^* \geq \delta$ and $\#\Lambda_j^* < \delta$ we have that $i < j$. If (Λ_i^*) is monotone for δ then $C(D, Q, \delta)$ is an usual one-point code, so improved codes only improve one-point codes for those δ for which the sequence is not monotone. In this case the code $C(D, Q, \delta)$ depends on the choice of $\phi_1, \ldots, \phi_n$. In fact, if $\#\Lambda_i^* = \delta$ and $\#\Lambda_j^* < \delta$ for some $j < i$, then $v(\phi_i + \phi_j) = v(\phi_i)$ but in general $ev(\phi_j) \notin C(D, Q, \delta)$, hence $ev(\phi_i + \phi_j) \notin C(D, Q, \delta)$. Thus we have a collection of improved codes with designed distance δ, depending on the collection of sets $\{\phi_1, \ldots, \phi_n\}$.

EXAMPLE 4.17 (Improved Suzuki codes). Let us consider the Suzuki curve $\mathcal{S}$ over $\mathbb{F}_8$ of Example 4.13. In that example we computed the sequence $(\#\Lambda_i^*)$. This sequence is monotone for $\delta = 3, 5, 6, 9, 13, 14, 18, 20, 21$. For example the one-point code $C(\mathcal{S}, D, 70Q)$ has dimension 55 and distance at least 4 (that is $d_{ORD}(55) = 4$), whereas $C(D, Q, 4)$ has the same distance and dimension 57.

4.9. Bibliographical notes. Algebraic geometry codes (also called geometric Goppa codes) were introduced by V.D. Goppa in in the seventies, [**23, 24**], as a generalization of another family of codes previously invented by himself, that of classical Goppa codes. AG codes became famous when M. Tsfasman, S.G. Vladuts and T. Zink showed in the early eighties, that there exist infinite families of these codes exceeding the Gilbert-Varshamov bound, [**46**]. The enormous interest aroused by these codes has encouraged the study of the theoretical tools supporting them, mainly algebraic geometry over finite fields.

Codes coming from many interesting curves have been studied in detail. For what it is referring to the two main examples discussed in this chapter, Hermitian codes were first studied by Stichtenoth, [**44**], and later by many authors. Their minimum distances were computed in [**47**] and their complete weight hierarchies in [**2**]. Suzuki codes were introduced by J. P. Hansen and H. Stichtenoth, [**26**]. The

true minimum distances of codes on this curve are known in many cases, but not always.

Besides one-point codes, which are the ones mainly discussed in this chapter, codes over more than one point (two, three or more) have been also studied, [**7, 28, 33**]. The interested reader can find multiple-point codes on the Hermitian curve [**31**], the Suzuki curve [**32**], or the Norm-Trace curve [**41**].

Many works have been devoted to the study of the order bound for AG codes. In its original formulation this bound applies to the duals of one-point codes. A nice generalization to arbitrary AG codes was given by P. Beelen [**3**] and later improved by I. Duursma, R. Kirov and S. Park in a sequence of articles [**9, 10, 11**]. The application of Andersen-Geil bound to one-point codes treated in this chapter is due to O. Geil, C. Munuera, D. Ruano and F. Torres, [**22**].

5. Castle curves and Castle codes

As seen above, curves with many points with respect to its genus provide codes with good parameters. This observation has led in recent years to an intensive research in order to determine good bounds on the number of rational points of a curve and to find curves with many points. For our purposes in this chapter is relevant one of these bounds, due to Lewittes. This bound has the particularity of being proved by using one-point codes. It links the number of points on the curve to the Weierstrass semigroup of one of them. This fact makes the bound particularly interesting for coding theory because the properties of this semigroup strongly affect the parameters of the obtained codes.

5.1. The Lewittes bound on the number of rational points of an algebraic curve. Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$ and write $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \dots, P_n\}$, $\mathcal{P} = \{P_1, \dots, P_n\}$. Consider the one-point codes $C(\mathcal{X}, D, mQ)$. Let $H = \{v_1 = 0, v_2, \dots\}$ be the Weierstrass semigroup of Q and v_2 its multiplicity.

THEOREM 5.1 (Lewittes-Geil-Matsumoto bound). *Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$, Q a rational point and H be the Weierstrass semigroup of Q. Then*

$$\#\mathcal{X}(\mathbb{F}_q) \leq \#(H \setminus (qH^* + H)) + 1 \leq qv_2 + 1$$

where v_2 is the multiplicity of H.

PROOF. Let $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \dots, P_n\}$, $\mathcal{P} = \{P_1, \dots, P_n\}$, and consider the one-point codes $C(\mathcal{X}, D, mQ)$. Then $\#\mathcal{X}(\mathbb{F}_q) = n = \#M$. By Corollary 3.14, $M \subseteq H \setminus (qH^* + H)$. Taking cardinalities we obtain the first inequality. To see the second one, note that $qv_2 + H \subseteq qH^* + H$ and according to Lemma 3.8 we have $\#(H \setminus (qv_2 + H)) = qv_2$. □

The bound $\#\mathcal{X}(\mathbb{F}_q) \leq \#(H \setminus (qH^* + H)) + 1$ was stated by Geil and Matsumoto, [**20**], improving the previous result $\#\mathcal{X}(\mathbb{F}_q) \leq qv_2 + 1$ obtained by Lewittes, [**29**].

5.2. Castle curves. Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$. $\mathcal{X}$ is called *Castle* is there exists a rational point $Q \in \mathcal{X}(\mathbb{F}_q)$ such that:

(1) the Weierstrass semigroup of Q, $H(Q)$ is symmetric; and
(2) the number of rational points on $\mathcal{X}$ reaches the Lewittes bound $\#\mathcal{X}(\mathbb{F}_q) = qv_2(Q) + 1$

where $v_2(Q)$ is the multiplicity of $H(Q)$.

EXAMPLE 5.2. Some of the curves previously discussed in this chapter are Castle.
(1) A rational curve is clearly a Castle curve.
(2) The Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$ is a Castle curve. Let Q be the point at infinity. The Weierstrass semigroup $H = \langle q, q+1 \rangle$ is symmetric of multiplicity $v_2 = q$ and $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^3 + 1$.
(3) The Suzuki curve $\mathcal{S}$ is Castle. Let Q be the point over $x = \infty$. The Weierstrass semigroup of Q, $H(Q) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$ is telescopic (see [**27**]), hence symmetric of multiplicity $v_2 = q$. Since $\mathcal{S}$ has $q^2 + 1$ rational points, it is a Castle curve.

Many of the most interesting curves for Coding Theory purposes are Castle. Let us see other examples.

EXAMPLE 5.3. Let $\mathcal{X}$ be a hyperelliptic curve and Q a hyperelliptic rational point. $\mathcal{X}$ is Castle if and only if Q is the only rational hyperelliptic point on $\mathcal{X}$ and $\mathcal{X}$ attains equality in the hyperelliptic bound $\#\{\text{rational nonhyperelliptic points}\} + 2\#\{\text{rational hyperelliptic points}\} \leq 2q + 2$.

EXAMPLE 5.4 (The Norm-Trace curve). Let us consider the curve defined over $\mathbb{F}_{q^r}$ by the affine equation

$$x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y$$

or equivalently by $N_{\mathbb{F}_{q^r}|\mathbb{F}_q}(x) = T_{\mathbb{F}_{q^r}|\mathbb{F}_q}(y)$, where the maps N and T are respectively the norm and trace from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. This curve has $2^{2r-1} + 1$ rational points and the Weierstrass semigroup at the unique pole Q of x is given by

$$H(Q) = \langle q^{r-1}, (q^r - 1)/(q-1) \rangle .$$

Since every semigroup generated by two elements is symmetric, this is a Castle curve. Codes on these curves have been studied by Geil in [**18**], where the reader can find proofs and details.

EXAMPLE 5.5 (Generalized Hermitian curves). For $r \geq 2$ let us consider the curve $\mathcal{X}_r$ over $\mathbb{F}_{q^r}$ defined by the affine equation

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

or equivalently by $s_{r,1}(y, y^q, \ldots, y^{q^{r-1}}) = s_{r,2}(x, x^q, \ldots, x^{q^{r-1}})$, where $s_{r,1}$ and $s_{r,2}$ are respectively the first and second symmetric polynomials in r variables. Note that $\mathcal{X}_2$ is the Hermitian curve. These curves were introduced by Garcia and Stichtenoth in [**17**]. They have $q^{2r-1} + 1$ rational points. Let Q be the only pole of x. Then $H(Q) = \langle q^{r-1}, q^{r-1} + q^{r-2}, q^r + 1 \rangle$. This semigroup is telescopic and hence symmetric (see e.g. [**27**]). Therefore, $\mathcal{X}_r$ is a Castle curve. AG-codes based on these curves were studied in [**6**] (binary case) and [**40**] (general case).

The next proposition states a fundamental property of Castle curves.

PROPOSITION 5.6. *Let $\mathcal{X}$ be a Castle curve with respect to a point $Q \in \mathcal{X}(\mathbb{F}_q)$. Write $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ and let $D = P_1 + \cdots + P_n$.*

(1) *Let $f \in \mathcal{L}(\infty Q)$ be such that $v(f) = v_2$. For every $a \in \mathbb{F}_q$ we have $\operatorname{div}(f - a) = D_a - v_2 Q$ with $0 \leq D_a \leq D$.*
(2) *$D \sim nQ$.*

PROOF. (1) The morphism $f : \mathcal{X} \to \mathbb{P}^1$ has degree v_2 hence $\#f^{-1}(a) \leq v_2$ for all $a \in \mathbb{F}_q$. Since $\#\mathcal{X}(\mathbb{F}_q) = qv_2$ we conclude that $\#f^{-1}(a) = v_2$. Then there exist exactly v_2 points $P \in \mathcal{X}(\mathbb{F}_q)$ such that $f(P) = a$. (2) Consider the one-point codes $C(\mathcal{X}, D, mQ)$ and the function $\phi = f^q - f$. $v(\phi) = qv_2 = n$ and $\phi(P_i) = 0$ for all P_i. Then $\phi \in \mathcal{L}(nQ - D)$ hence $D \sim nQ$. □

COROLLARY 5.7. *Let $\mathcal{X}$ be a Castle curve of genus g with respect to a point $Q \in \mathcal{X}(\mathbb{F}_q)$. Let $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, \ldots, P_n\}$ and $D = P_1 + \cdots + P_n$. Then $(n+2g-2)Q - D$ is a canonical divisor.*

PROOF. $(n+2g-2)Q - D \sim (2g-2)Q$. Since H is symmetric this is a canonical divisor. □

REMARK 5.8. Let ϕ be the function defined in the proof of Proposition 5.6. It can be proved that the differential form $\omega = d\phi/\phi$ has simple poles and residue 1 at all points P_i. So ω is the differential form for which we asked in Proposition 4.6.

Let us remember that by γ_r we denote the r-th gonality of $\mathcal{X}$ over $\mathbb{F}_q$.

PROPOSITION 5.9. *Let $\mathcal{X}$ be a Castle curve with respect to a point $Q \in \mathcal{X}(\mathbb{F}_q)$ with Weierstrass semigroup $H = \{v_1 = 0, v_2, \ldots\}$. If the multiplicity at Q satisfies $v_2 \leq q + 1$, then*

1. *$\gamma_i \leq v_i$ for all $i = 1, 2, \ldots$.*
2. *$\gamma_2 = v_2$.*
3. *$\gamma_i = v_i$ for $i \geq g - \gamma_2 + 2$.*

PROOF. (1) Follows from the definition of gonality. (2) There is a non-constant morphism of degree γ_2 from $\mathcal{X}$ to the projective line. Then $qv_2 + 1 = \#\mathcal{X}(\mathbb{F}_q) \leq \gamma_2(q+1)$, so $(qv_2 + 1)/(q+1) = v_2 - (v_2 - 1)/(q+1) \leq \gamma \leq v_2$. By our hypothesis $v_2 \leq q + 1$, it holds that $(v_2 - 1)/(q + 1) < 1$ and we get the equality. (3) The statement about the gonalities of high order follows from the fact that both, the semigroup H and the set of gonalities $GS(\mathcal{X}) = (\gamma_r)_{r \geq 1}$ verify the same symmetry property: for every integer t, it holds that $t \in H$ (resp. $t \in GS(\mathcal{X})$) if and only if $2g - 1 - t \notin H$ (resp. $2g - 1 - t \notin GS(\mathcal{X})$). □

5.3. Codes on Castle curves. Let $\mathcal{X}$ be a Castle curve of genus g over $\mathbb{F}_q$ with $(n + 1)$ $\mathbb{F}_q$-rational points, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$. A *Castle code* is a one-point code $C(\mathcal{X}, D, mQ)$ constructed from $\mathcal{X}$ and $\mathcal{P} = \{P_1, \ldots, P_n\}$. Let $H = H(Q) = \{0 = v_1 < v_2 < \ldots\}$ be the Weierstrass semigroup of Q. The dimension set M can be easily obtained: by Propositions 4.10 and 5.6, $M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H)$. Define the function $\iota = \iota_Q : \mathbb{N}_0 \to \mathbb{N}$ by $\iota(m) = \max\{i : v_i \leq m\}$. Note that $\iota(m) = \ell(mQ)$.

PROPOSITION 5.10. *Let m be a nonnegative integer. The Castle code $C(\mathcal{X}, D, mQ)$ has dimension $k = \iota(m) - \iota(m - n)$ and abundance $\iota(m - n)$.*

We now turn to the minimum distance.

PROPOSITION 5.11. *Let $C(\mathcal{X}, D, mQ)$ be a Castle code. Then*

1. *for $1 \leq m < n$, $C(\mathcal{X}, D, mQ)$ reaches Goppa bound if and only if $C(\mathcal{X}, D, (n - m)Q)$ does.*
2. *For $1 \leq r \leq q - 1$, $d(C(\mathcal{X}, D, rv_2Q) = n - rv_2$.*
3. *For $n - v_2 \leq m \leq n$, $d(C(\mathcal{X}, D, mQ) = v_2$.*

PROOF. (1) As seen in Proposition 4.2, $C(\mathcal{X}, D, mQ)$ reaches equality in the Goppa bound if and only if then there exists $D', 0 \leq D' \leq D$ such that $mQ \sim D'$. Let $D'' = D - D'$. Thus $mQ \sim D - D'' \sim nQ - D''$, hence $(n-m)Q \sim D''$ and the code $C(\mathcal{X}, D, (n-m)Q)$ also reaches equality in the Goppa bound. (2) Follows from Propositions 4.2 and 5.6(1). (3) $v_2 = d(C(\mathcal{X}, D, (n-v_2)Q) \geq d(C(\mathcal{X}, D, mQ) \geq d(C(\mathcal{X}, D, nQ) \geq v_2$. The first equality comes from item (2) of this proposition and the last inequality is the improved Goppa bound on the minimum distance. □

EXAMPLE 5.12. The bound d_{ORD} was computed for codes on the Suzuki curve over $\mathbb{F}_8$ in Example 4.13. In particular we found the result $d(C(\mathcal{S}, D, 62Q)) \geq d(C(\mathcal{S}, D, 63Q)) \geq 6$. By using Proposition 5.11 we get now $d(C(\mathcal{S}, D, 62Q)) = d(C(\mathcal{S}, D, 63Q)) = 8$. So this last one is a $[64, 50, 8]$ code and again we the get a code with the best known parameters according to [**34**]. Furthermore this fact shows that the bound d_{ORD} does not always improve on the improved Goppa bound $d(C(\mathcal{X}, D, mQ)) \geq n - \deg(G) + \gamma_{a+1}$.

The cardinalities $\#\Lambda^*$ can be now computed in a simple way.

LEMMA 5.13. *For Castle codes it holds that* $M = \{m \in H : n+2g-1-m \in H\}$. *As a consequence,* $m_{n-r+1} = n + 2g - 1 - m_r$ *for* $r = 1, \ldots, n$.

PROOF. Let $m \in H$. From Riemann-Roch theorem, $\ell(mQ-D) = m-n+1-g+\ell((n+2g-2-m)Q)$, hence $\ell(mQ) = \ell((m-1)Q)$ if and only if $\ell((n+2g-2-m)Q) = \ell((n+2g-1-m)Q)$, that is if and only if $n + 2g - 1 - m \in H$. The conclusion $m_{n+1-r} = n + 2g - 1 - m_r$ is clear. □

For $i = 1, \ldots, n$, let $L_i = m_i + \text{Gaps}(H) = \{m_i + l_1, \ldots, m_i + l_g\}$.

PROPOSITION 5.14. *For Castle codes,* $\#\Lambda_i^* = n - i + 1 - \#(L_i \cap M)$.

PROOF. Since $M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H)$ and H is symmetric, we have $M = \{0, \ldots, n + 2g - 1\} \setminus L$, where $L = \{l_1, \ldots, l_g, n + 2g - l_g - 1, \ldots, n + 2g - l_1 - 1\}$. For $i = 1, \ldots, n$, let

$$\begin{aligned} U_i &= \{m_j \in M : m_i + m_j < n + 2g, m_i + m_j \notin M\}, \\ V_i &= \{m_j \in M : m_i + m_j \geq n + 2g\}. \end{aligned}$$

Clearly $\#\Lambda_i^* = \#\{m_j : m_i + m_j \in M\} = \#(M \setminus (U_i \cup V_i)) = n - \#U_i - \#V_i$. Since $M \subset H$, we have $U_i = \{m_j \in M : m_i + m_j \in L\} = \{n + 2g - 1 - l_g - m_i, \ldots, n + 2g - 1 - l_1 - m_i\} \cap M$. According to Lemma 5.13, $\#U_i = \#(L_i \cap M)$. Besides $\#V_i = i - 1$. In fact, if $m_i + m_j \geq n + 2g$, from Lemma 5.13, we can write $m_j = n + 2g - 1 - m_t$ with $t = n - j + 1$. Then $n + 2g - 1 + m_i - m_t > n + 2g - 1$ if and only if $m_i > m_t$ and there exists $i - 1$ such choices for m_t. □

Then for Castle codes we have

$$d(C(\mathcal{X}, D, m_k Q)) \geq d_{ORD}(k) = \min\{n - r + 1 - \#(L_r \cap M) : r \leq k\}.$$

EXAMPLE 5.15 (Hermitian codes). The minimum distances of Hermitian codes $C(\mathcal{H}, D, mQ)$ were computed in Example 4.8 for m in the range $0 \leq m \leq n - q^2$. We shall study now the case $n - q^2 < m < n$. Note that all m in this range are pole numbers and $n - m \leq n - q^2$. Write $m = n - aq - b$ with $0 \leq a, b < q$. If $b \leq a$ then $n - m \in H$ hence Proposition 5.11(1) and Example 4.8 ensure that $C(\mathcal{H}, D, mQ)$

reaches the Goppa bound, $d(C(\mathcal{H}, D, mQ)) = d_G(C(\mathcal{H}, D, mQ)) = n - m = aq + b$. If $b > a$, then

$$\begin{aligned} d(C(\mathcal{H}, D, (n - aq - a - 1)Q)) &\leq d(C(\mathcal{H}, D, (n - aq - b)Q) \\ &\leq d(C(\mathcal{H}, D, (n - (a+1)q)Q)) = (a+1)q. \end{aligned}$$

A straightforward computation using Proposition 5.14 shows that

$$d_{ORD}(C(\mathcal{H}, D, (n - aq - a - 1)Q)) = (a+1)q$$

so we get equality, $d(C(\mathcal{H}, D, (n - aq - b)Q)) = (a+1)q$.

Finally we sate a duality property of Castle codes. As a consequence of Propositions 4.5, 4.14 and Corollary 5.7, we have the following.

PROPOSITION 5.16. *For Castle codes, there exist* $\mathbf{x} \in (\mathbb{F}_q^*)^n$ *such that* $C(\mathcal{X}, D, m_k Q)^\perp = \mathbf{x} * C(\mathcal{X}, D, (n + 2g - 2 - m_k)Q)$ *for all* $k = 1, \ldots, n$.

Codes verifying the duality relation of the above proposition are called *isometry dual*. Let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a basis of $\mathbb{F}_q^n$ such that $C(\mathcal{X}, D, m_r Q) = \langle \mathbf{b}_1, \ldots, \mathbf{b}_r \rangle$, $r = 1, \ldots, n$. A vector $\mathbf{x} \in (\mathbb{F}_q^*)^n$ providing the isometries stated in the proposition can be explicitly obtained from the duality relations, which lead to the system of linear equations $(\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{x} = 0$, $i + j \leq n$.

Since isometric codes have equal minimum distance, we can obtain estimates on the minimum distance of Castle codes by using both the order and dual order bounds. It can be proved that both bounds give the same result.

PROPOSITION 5.17. *For Castle codes we have* $\#N^*_{n-r} = \#\Lambda^*_r$, $r = 1, \ldots, n$. *As a consequence*

$$d_{ORD}(C(\mathcal{X}, D, m_k Q)) = \min\{\#N^*_r : r = n - k, \ldots, n - 1\}.$$

PROOF. According to Lemma 5.13, for Castle codes it holds that $m_{n+1-r} = n + 2g - 1 - m_r$. Then

$$\begin{aligned} \#N^*_{n-r} &= \#\{(i,j) : m_i + m_j = m_{n-r+1}\} \\ &= \#\{(i,j) : m_r + m_j = m_{n-i+1}\} \\ &= \#\{(r,j) : m_r + m_j \in M\} \\ &= \#\Lambda^*_r. \end{aligned}$$

The conclusion is clear. □

5.4. Bibliographical notes. Castle curves and codes were introduced in [**38**] and generalized in [**39**]. The computation of d_{ORD} for some Castle codes (including all Hermitian and Suzuki codes) can be found in the article [**42**]. For Hermitian codes this bound provides the true minimum distance of $C(\mathcal{H}, D, mQ)$ for all m, see [**27**]. Such distances were first computed by K. Yang and P.V. Kumar in [**47**] (without using order bounds).

6. Feng-Rao decoding

In this section we show a very general decoding method for codes $\mathcal{C}_k$ belonging to chains, as those treated in Section 2. Keeping the notations used in that section, let $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ be a basis of $\mathbb{F}_q^n$ and $\mathcal{C}_r = \langle \mathbf{b}_1, \ldots, \mathbf{b}_r \rangle$, $r = 1, \ldots, n$. By using the information given by the whole chain $\mathcal{C}_0 = (\mathbf{0}) \subset \mathcal{C}_1 \subset \cdots \subset \mathcal{C}_n = \mathbb{F}_q^n$ we can decode $\mathcal{C}_k$.

If these codes are one-point AG codes, $\mathcal{C}_r = C(\mathcal{X}, D, m_r Q)$, then we take the basis vectors $\mathbf{b}_1 = ev(\phi_1), \ldots, \mathbf{b}_n = ev(\phi_n)$, where $v(\phi_r) = m_r$, as treated in previous sections.

6.1. Preparation step. Our decoding algorithm works for dual codes. hence we first consider a dual basis $\mathcal{D} = \{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ of $\mathbb{F}_q^n$ verifying

$$\mathbf{b}_i \cdot \mathbf{h}_j = \begin{cases} 0 & \text{if } i+j < n+1 \\ \neq 0 & \text{if } i+j = n+1 \end{cases}$$

where $\cdot$ stands for the usual inner product in $\mathbb{F}_q^n$. These conditions imply the duality relations

$$\langle \mathbf{h}_1, \ldots, \mathbf{h}_{n-r} \rangle = \mathcal{C}_r^{\perp} = \langle \mathbf{b}_1, \ldots, \mathbf{b}_r \rangle^{\perp}$$

or equivalently $\langle \mathbf{h}_1, \ldots, \mathbf{h}_r \rangle^{\perp} = \mathcal{C}_{n-r}$ for all $r = 1, \ldots, n$. If the chain $\mathcal{C}_0 = (\mathbf{0}) \subset \mathcal{C}_1 \subset \cdots \subset \mathcal{C}_n = \mathbb{F}_q^n$ verifies a duality relation $\mathcal{C}_r^{\perp} = \mathcal{C}_{n-r}$, $r = 0, \ldots, n$, then we take $\mathbf{h}_i = \mathbf{b}_i$. If the chain verifies an isometry-dual relation $\mathcal{C}_r^{\perp} = \mathbf{x} * \mathcal{C}_{n-r}$, $r = 0, \ldots, n$ (the case of Castle codes), then we take $\mathbf{h}_i = \mathbf{x} * \mathbf{b}_i$, $i = 1, \ldots, n$.

Once the basis $\mathcal{D}$ has been fixed, we consider the dual chain

$$\mathcal{C}_n^{\perp} = (\mathbf{0}) \subset \mathcal{C}_{n-1}^{\perp} \subset \cdots \subset \mathcal{C}_{k+1}^{\perp} \subset \mathcal{C}_k^{\perp} \subset \cdots \subset \mathcal{C}_0^{\perp} = \mathbb{F}_q^n$$

and let $\rho_{\mathcal{D}} : \mathbb{F}_q^n \to \{0, \ldots, n\}$ be the sorting map relative to the basis $\mathcal{D}$, defined by $\rho_{\mathcal{D}}(\mathbf{v}) = \min\{i : \mathbf{v} \in \langle \mathbf{h}_1, \ldots, \mathbf{h}_i \rangle\}$ if $\mathbf{v} \neq \mathbf{0}$. A pair of basis vectors $(\mathbf{h}_r, \mathbf{h}_s)$ is well-behaving with respect to $\mathcal{D}$ if for all $(i,j) \prec (r,s)$ we have $\rho_{\mathcal{D}}(\mathbf{h}_i * \mathbf{h}_j) < \rho_{\mathcal{D}}(\mathbf{h}_r * \mathbf{h}_s)$. Remember that for $r = 0, 1, \ldots, n-1$, we define the sets

$$N_r = \{(i,j) : \ (\mathbf{h}_i, \mathbf{h}_j) \text{ is well-behaving with respect to } \mathcal{D} \text{ and } \rho_{\mathcal{D}}(\mathbf{h}_i * \mathbf{h}_j) = r+1\}.$$

All these sets are precomputed in the preparation step. The dual order bound with respect to $\mathcal{D}$, stated in Theorem 2.7, ensures that the minimum distance of $\mathcal{C}_k = \langle \mathbf{h}_1, \ldots, \mathbf{h}_{n-k} \rangle^{\perp}$ satisfies $d(\mathcal{C}_k) \geq \delta = \min\{\#N_r : r = n-k, \ldots, n-1\}$. We can decode $\mathcal{C}_k$ up to $(\delta - 1)/2$ errors by using majority voting.

When we consider one-point AG codes then we can manage the sets N_r^* instead of N_r. If these codes are Castle, Proposition 5.17 implies that the Feng-Rao algorithm corrects errors of weight up to one half the order bound.

6.2. Syndromes. Let $\mathbf{u} = \mathbf{c} + \mathbf{e}$ be a received word, where $\mathbf{c} \in \mathcal{C}_k$ and $\mathbf{e}$ is the error vector. Assume $wt(\mathbf{e}) \leq (\delta - 1)/2$. To decode $\mathbf{u}$ we shall compute the syndromes

$$s_1 = \mathbf{h}_1 \cdot \mathbf{e}, \ldots, s_n = \mathbf{h}_n \cdot \mathbf{e}.$$

Consider the matrix $\mathbf{H}$ whose rows are the vectors $\mathbf{h}_1, \ldots, \mathbf{h}_n$. $\mathbf{H}$ has full rank n and $\mathbf{H}\mathbf{e}^T = \mathbf{s}^T$, where $\mathbf{s} = (s_1, \ldots, s_n)$. Once all one-dimensional syndromes s_i are known we can deduce the error vector by solving a system of linear equations. Note that $s_1, \ldots, s_{n-k}$ can be derived from $\mathbf{u}$: as $\mathcal{C}_k^{\perp} = \langle \mathbf{h}_1, \ldots, \mathbf{h}_{n-k} \rangle$, for $i = 1, \ldots, n-k$, we have

$$\mathbf{h}_i \cdot \mathbf{u} = \mathbf{h}_i \cdot (\mathbf{c} + \mathbf{e}) = \mathbf{h}_i \cdot \mathbf{e} = s_i.$$

In order to compute $s_{n-k+1}, \ldots, s_n$, we shall use two-dimensional syndromes

$$s_{rt} = (\mathbf{h}_r * \mathbf{h}_t) \cdot \mathbf{e}, \ 1 \leq r, t \leq n.$$

Let $\mathbf{S}$ be the matrix $\mathbf{S} = (s_{rt})$, $1 \leq r, t \leq n$. As seen in Section 2.4, this matrix can be written also as $\mathbf{S} = \mathbf{H}\mathbf{D}(\mathbf{e})\mathbf{H}^T$, where $\mathbf{D}(\mathbf{e})$ is the diagonal matrix with $\mathbf{e}$

in its diagonal. Since $\mathbf{H}$ has full rank, we have $\mathrm{rank}(\mathbf{S}) = \mathrm{rank}(\mathbf{D}(\mathbf{e})) = wt(\mathbf{e})$. For $1 \leq i, j \leq n$ let us consider the submatrix of $\mathbf{S}$

$$\mathbf{S}(i,j) = (s_{rt}),\ 1 \leq r \leq i, 1 \leq t \leq j.$$

An entry (i,j) is a *discrepancy* of $\mathbf{S}$ if $\mathrm{rank}(\mathbf{S}(i-1,j-1)) = \mathrm{rank}(\mathbf{S}(i-1,j)) = \mathrm{rank}(\mathbf{S}(i,j-1))$ and $\mathrm{rank}(\mathbf{S}(i-1,j-1)) \neq \mathrm{rank}(\mathbf{S}(i,j))$. Clearly the total amount of discrepancies in $\mathbf{S}$ is $\mathrm{rank}(\mathbf{S}) = wt(\mathbf{e})$.

6.3. Computing unknown syndromes. Assume that $s_1, \ldots, s_l$ are known and s_{l+1} is the smallest unknown syndrome. Let $(i,j) \in N_l$. The well-behaving property implies that for each $(r,t) \prec (i,j)$ we have $\rho_{\mathcal{D}}(\mathbf{h}_r * \mathbf{h}_t) < \rho_{\mathcal{D}}(\mathbf{h}_i * \mathbf{h}_j) = l+1$. Then there exist $\lambda_1, \ldots, \lambda_l$ such that $\mathbf{h}_r * \mathbf{h}_t = \lambda_1 \mathbf{h}_1 + \cdots + \lambda_l \mathbf{h}_l$ and $s_{rt} = \lambda_1 s_1 + \cdots + \lambda_l s_l$. Thus the matrices $\mathbf{S}(i-1,j-1), \mathbf{S}(i-1,j)$ and $\mathbf{S}(i-1,j-1)$ are known. If these three matrices have equal rank, then (i,j) is called a *candidate*. Let K be the number of discrepancies in the known part of $\mathbf{S}$. If (r,t) is a known discrepancy, then all entries (r,t') and (r',t) with $r' > r, t' > t$ are noncandidates. Conversely, if $(i,j) \in N_l$ is not a candidate then there exists a known discrepancy in its same row or column. Thus the number of pairs $(i,j) \in N_l$ which are not candidates is at most $2K$. If $wt(\mathbf{e}) \leq (\#N_l - 1)/2$, then

$$\text{number of candidates} \geq \#N_l - 2K \geq \#N_l - 2wt(\mathbf{e}) > 0$$

and there always exist candidates. Let (i,j) be one of them. There is a unique value s'_{ij} of entry (i,j) such that $\mathrm{rank}(\mathbf{S}(i-1,j-1)) = \mathrm{rank}(\mathbf{S}(i,j))$. The candidate (i,j) is called *true* if $s'_{ij} = s_{ij}$ and *false* if $s'_{ij} \neq s_{ij}$. Since s_{l+1} is unknown, then so is s_{ij} and we cannot check in advance whether a candidate is true or false. However, a candidate (i,j) is false if and only if it is a discrepancy, hence there are at most $wt(\mathbf{e})$ false candidates in $\mathbf{S}$. As $wt(\mathbf{e})$ is 'small', most candidates will be true. Let us formalize this idea.

Let T and F be respectively the number of true and false candidates in N_l. Since a false candidate is a discrepancy and the total number of discrepancies is $wt(\mathbf{e})$, we have $K + F \leq wt(\mathbf{e}) \leq (\#N_l - 1)/2$. Combining this inequality with

$$\#N_l = \#\text{candidates} + \#\text{noncandidates} \leq (T+F) + 2K$$

we obtain $F < T$ and the majority of candidates are true.

For each candidate (i,j), compute s'_{ij} and suppose $s_{ij} = s'_{ij}$. This assumption leads to a predicted value s'_{l+1} of s_{l+1} as above: since $\rho_{\mathcal{D}}(\mathbf{h}_i * \mathbf{h}_j) = l+1$, we can write $\mathbf{h}_i * \mathbf{h}_j = \lambda_1 \mathbf{h}_1 + \cdots + \lambda_{l+1} \mathbf{h}_{l+1}$ with $\lambda_{l+1} \neq 0$. Then $s_{ij} = \lambda_1 s_1 + \cdots + \lambda_{l+1} s_{l+1}$. Define the *vote* of (i,j) as $s'_{l+1} = \lambda_{l+1}^{-1}(s'_{ij} - \lambda_1 s_1 - \cdots - \lambda_l s_l)$.

Compute the votes of all candidates $(i,j) \in N_l$. Since the majority of candidates are true, we can derive the correct value of s_{l+1} as the most voted among all candidates.

Once this value is known we proceed to the next unknown syndrome. If $wt(\mathbf{e}) \leq (\delta - 1)/2$ then $wt(\mathbf{e}) \leq (\#N_l - 1)/2$ for all $l = n-k, \ldots, n-1$ and all syndromes $s_{n-k+1}, \ldots, s_n$ can be computed. Assuming that all these sets N_l have been precomputed, the complexity of this algorithm is that of solving a linear system of n equations in n unknowns, that is $O(n^3)$.

6.4. Bibliographical notes. The idea of using majority voting for unknown syndromes is due to G.L. Feng and T.N.T. Rao [**12**] and I. Duursma, [**8**]. The original algorithm was designed for duals of primary AG codes. A full and nice

description for duals of codes coming from order domains can be found in [**27**]. A generalization to a broad class of codes, including primary codes, was done in [**21**]. Our presentation is a mixture of these two works.

Decoding AG codes is a very active area of research today. General AG codes $C(\mathcal{X}, D, G)$ can be decoded by several methods. Here we just cite the nice report [**4**] by Beelen and Høholdt, which is close to the ideas presented in this chapter.

6.5. An example. Let us consider the Hermitian curve $\mathcal{H} : y^2 + y = x^3$ defined over the field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $1 + \alpha = \alpha^2$. $\mathcal{H}$ has genus 1 and nine rational points, namely $Q = (0 : 1 : 0)$ and the eight affine points

$$\begin{array}{llll} P_1 = (0,0), & P_3 = (1,\alpha), & P_5 = (\alpha,\alpha), & P_7 = (\alpha^2,\alpha), \\ P_2 = (0,1), & P_4 = (1,\alpha^2), & P_6 = (\alpha,\alpha^2), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let $\mathcal{P} = \{P_1, \ldots, P_8\}$ and consider the codes $C(\mathcal{H}, D, mQ)$, $m = 0, \ldots, 9$. The Weierstrass semigroup of Q is $H = \langle 2, 3\rangle = \{0, 2, 3, \rightarrow\}$, and the dimension set is $M = \{0, 2, 3, 4, 5, 6, 7, 9\}$. Then, a basis $\mathcal{B}$ of $\mathbb{F}_4^8$ is then given by the vectors

$$\begin{array}{lcccccccccc} \mathbf{b}_1 & = & ev_{\mathcal{P}}(1) & = & (1, & 1, & 1, & 1, & 1, & 1, & 1) \\ \mathbf{b}_2 & = & ev_{\mathcal{P}}(x) & = & (0, & 0, & 1, & 1, & \alpha, & \alpha, & \alpha^2, & \alpha^2) \\ \mathbf{b}_3 & = & ev_{\mathcal{P}}(y) & = & (0, & 1, & \alpha, & \alpha^2, & \alpha, & \alpha^2, & \alpha, & \alpha^2) \\ \mathbf{b}_4 & = & ev_{\mathcal{P}}(x^2) & = & (0, & 0, & 1, & 1, & \alpha^2, & \alpha^2, & \alpha, & \alpha) \\ \mathbf{b}_5 & = & ev_{\mathcal{P}}(xy) & = & (0, & 0, & \alpha, & \alpha^2, & \alpha^2, & 1, & 1, & \alpha) \\ \mathbf{b}_6 & = & ev_{\mathcal{P}}(x^3) & = & (0, & 0, & 1, & 1, & 1, & 1, & 1, & 1) \\ \mathbf{b}_7 & = & ev_{\mathcal{P}}(x^2y) & = & (0, & 0, & \alpha, & \alpha^2, & 1, & \alpha, & \alpha^2, & 1) \\ \mathbf{b}_8 & = & ev_{\mathcal{P}}(x^3y) & = & (0, & 0, & \alpha, & \alpha^2, & \alpha, & \alpha^2, & \alpha, & \alpha^2) \end{array}$$

In view of the duality property of Hermitian codes we can take $\mathcal{D} = \mathcal{B}$. Consider the code $\mathcal{C} = C(\mathcal{H}, D, 3Q)$ of dimension 3. A direct computation gives

$$\begin{aligned} \Lambda_1^* &= \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(1,7),(1,8)\} \\ \Lambda_2^* &= \{(2,1),(2,2),(2,3),(2,4),(2,5),(2,7)\} \\ \Lambda_3^* &= \{(3,1),(3,2),(3,3),(3,4),(3,6)\} \\ N_5^* &= \{(1,6),(2,4),(3,3),(4,2),(6,1)\} \\ N_6^* &= \{(1,7),(2,5),(3,4),(4,3),(5,2),(7,1)\} \\ N_7^* &= \{(1,8),(2,7),(3,6),(4,5),(5,4),(6,3),(7,2),(8,1)\} \end{aligned}$$

hence both, the order and dual order bounds, ensure $d(\mathcal{C}) \geq 5$, which is the true minimum distance of $\mathcal{C}$ according to Example 4.8. Then it can correct up to 2 errors.

Since $k = 3$, the code $\mathcal{C}$ allows us to encode 3-tuples $\mathbf{z} \in \mathbb{F}_4^3$ by 8-tuples $\mathbf{c} \in \mathcal{C}$. Suppose we want to transmit the message $\mathbf{z} = (1, 1, 1)$. It is encoded as $\mathbf{c} = 1\mathbf{b}_1 + 1\mathbf{b}_2 + 1\mathbf{b}_3 = (1, 0, \alpha, \alpha^2, 1, 0, 0, 1)$. Suppose we receive the word $\mathbf{u} = (0, 0, \alpha, 1, 1, 0, 0, 1)$ with error $\mathbf{e} = (1, 0, 0, \alpha, 0, 0, 0, 0)$. To decode $\mathbf{c}$ we first compute the known one-dimensional syndromes of $\mathbf{e}$

$$s_1 = \mathbf{b}_1 \cdot \mathbf{e} = \alpha^2,\ s_2 = \mathbf{b}_2 \cdot \mathbf{e} = \alpha,\ s_3 = \mathbf{b}_3 \cdot \mathbf{e} = 1,\ s_4 = \mathbf{b}_4 \cdot \mathbf{e} = \alpha,\ s_5 = \mathbf{b}_5 \cdot \mathbf{e} = 1.$$

The smallest unknown syndrome is s_6. Using the information given by $s_1, \ldots, s_5$ and N_5^*, the known part of $\mathbf{S}$ is

$$\mathbf{S} = \begin{bmatrix} \alpha^2 & \alpha & 1 & \alpha & 1 & * \\ \alpha & \alpha & 1 & * & & \\ 1 & 1 & * & & & \\ \alpha & * & & & & \\ 1 & & & & & \\ * & & & & & \\ & & & & & \\ & & & & & \end{bmatrix}$$

where the entries in N_5^* are marked with $*$. Since $\operatorname{rank}(\mathbf{S}(2,2)) = 2$ there is a unique candidate: $(3,3)$. As $s'_{3,3} = \alpha^2$ and $\mathbf{b}_3 * \mathbf{b}_3 = \mathbf{b}_3 + \mathbf{b}_6$, it votes for $s_6 = s'_{3,3} - s_3 = \alpha^2 + 1 = \alpha$.

Once this syndrome is known let us compute s_7. We first update the matrix

$$\mathbf{S} = \begin{bmatrix} \alpha^2 & \alpha & 1 & \alpha & 1 & \alpha & * \\ \alpha & \alpha & 1 & \alpha & * & & \\ 1 & 1 & \alpha^2 & * & & & \\ \alpha & \alpha & * & & & & \\ 1 & * & & & & & \\ \alpha & & & & & & \\ * & & & & & & \\ & & & & & & \end{bmatrix}.$$

As above, the entries in N_6^* are marked with $*$. Candidates are $(3,4)$ and $(4,3)$. A simple computation gives $s'_{3,4} = 1, s'_{4,3} = 1$, and both vote for $s_7 = 1$. Let us compute s_8. The current form of $\mathbf{S}$ is

$$\mathbf{S} = \begin{bmatrix} \alpha^2 & \alpha & 1 & \alpha & 1 & \alpha & 1 & * \\ \alpha & \alpha & 1 & \alpha & 1 & \alpha & * & \\ 1 & 1 & \alpha^2 & 1 & \alpha^2 & * & & \\ \alpha & \alpha & 1 & \alpha & * & & & \\ 1 & 1 & \alpha^2 & * & & & & \\ \alpha & \alpha & * & & & & & \\ 1 & * & & & & & & \\ * & & & & & & & \end{bmatrix}.$$

Candidates are $(3,6), (4,5), (5,4)$ and $(6,3)$. We get $s'_{3,6} = 1, s'_{4,5} = 1, s'_{5,4} = 1, s'_{6,3} = 1$. All of them vote for $s_8 = 1$.

Once all one-dimensional syndromes are known, we deduce the error vector $\mathbf{e}$ by solving the system $s_1 = \mathbf{b}_1 \cdot \mathbf{e}, \ldots, s_n = \mathbf{b}_n \cdot \mathbf{e}$. In our case, as expected, $\mathbf{e} = (1,0,0,\alpha,0,0,0,0)$, hence $\mathbf{c} = \mathbf{u} - \mathbf{e} = (0,0,\alpha,1,1,0,0,1) - (1,0,0,\alpha,0,0,0,0) = (1,0,\alpha,\alpha^2,1,0,0,1)$. Finally we write $\mathbf{c}$ as a linear combination of $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$, obtaining $\mathbf{c} = \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3$. The original message was $\mathbf{z} = (1,1,1)$.

References

1. H. Andersen and O. Geil, *Evaluation codes from order domain theory*, Finite Fields and their Applications **14** (2008), pp. 92–123.
2. A. Barbero, C. Munuera, *The Weight Hierarchy of Hermitian Codes*, SIAM Journal on Discrete Mathematics **13** (2000), pp. 79-104.

3. P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields and Application **13** (2007), pp. 665–680.
4. P. Beelen and T. Høholdt, *The decoding of algebraic geometry codes*. In E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, World Scientific, Singapore, 2008, pp. 49–98.
5. E.R. Berlekamp, R.J. McEliece and H. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Transactions on Information Theory **24(3)** (1978), pp. 384–386.
6. S. V. Bulygin, *Generalized Hermitian codes over $GF(2^r)$*, IEEE Transactions on Information Theory **52** (2006), pp. 4664–4669.
7. C. Carvalho and Fernando Torres, *On Goppa codes and Weierstrass gaps at several points*, Designs, Codes and Cryptography **35** (2005), pp. 211–225.
8. I.M. Duursma, *Majority coset decoding*, IEEE Transactions on Information Theory **39** (1993), pp. 1067–1071.
9. I. Duursma and R. Kirov *An extension of the order bound for AG codes*. In Applied Algebra, Algebraic algorithms and error-correcting codes, pp. 11-22, LNCS 5527, Springer, 2009.
10. I. Duursma and S. Park, Coset bounds for algebraic geometric codes, Finite Fields Applications **16** (2010), pp. 36–55.
11. I. Duursma, R. Kirov and S. Park, *Distance bounds for algebraic geometric codes*, J. Pure and Applied Algebra **215** (2011), pp. 18631878. arXiv1001.1374, 2010.
12. G.L. Feng and T.R.N. Rao, *Decoding of algebraic geometric codes up to the designed minimum distance*, IEEE Transactions on Information Theory **39** (1993), pp. 37–45.
13. G.L. Feng and T.N.T. Rao, *Improved geometric Goppa codes. Part I: Basic Theory*, IEEE Transactions on Information Theory **41** (1995), pp. 1678–1693.
14. J. Fitzgerald and R.F. Lax, *Decoding affine variety codes using Gröbner basis*, Designs, Codes and Cryptography **13(2)** (1998), pp. 147–158.
15. W. Fulton, *Algebraic Curves*. Benjamin, New York, 1969.
16. R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Suplemento ai Rendiconti del Circolo Matematico di Palermo **51** (1998), pp. 25–46.
17. A. Garcia and H. Stichtenoth, A class of polynomials over finite fields, Finite Fields and Applications **5** (1999), pp. 424–435.
18. O. Geil, *On codes from norm-trace curves*, Finite Fields and Their Applications **9(3)** (2003), pp. 351–371.
19. O. Geil, *Evaluation codes from an affine variety code perspective*. In E. Martínez-Moro, C. Munuera, D. Ruano (Eds.), Advances in algebraic geometry codes, World Scientific, Singapore, 2008, pp. 153–180.
20. O. Geil and R. Matsumoto, *Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups*, J. Pure and Applied Algebra **213(6)** (2009), pp. 1152–1156.
21. O. Geil, R. Matsumoto and D. Ruano, *Feng-Rao decoding of primary codes*, Finite Fields and their Applications **23** (2013), pp. 35–52.
22. O. Geil, C. Munuera, D. Ruano and F. Torres, *On the order bounds for one-point AG codes*, Advances in Mathematics of Communications **3** (2011), pp. 489–504.
23. V.D. Goppa, *Codes Associated with Divisors*, Problemy Peredachi Informatsii **13(1)** (1977), pp. 33–39.
24. V.D. Goppa, *Algebraico-Geometric Codes*, Mathematics of the USSR-Izvestiya **21** (1983), pp. 75–91.
25. J.P. Hansen, *Codes on the Klein Quartic, Ideals and Decoding*, IEEE Transactions on Information Theory **33(6)** (1987), pp. 923–925.
26. J. P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, Applicable Algebra in Engineering, Communication and Computing **1** (1990), pp. 67–77.
27. T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic-Geometry codes*. In V.S. Pless and W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998. Corrected version available online at http://www.tue.nl/∼ruudp/paper/31.pdf
28. M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure and Applied Algebra **162** (2001), pp. 273–290.
29. J. Lewittes, *Places of degree one in function fields over finite fields* J. Pure and Applied Algebra **69** (1990), pp. 177-183–1156.

30. F.J. MacWilliams and N. Sloane, *The theory of error-correcting codes*. North-Holland, Amsterdam, 1977.
31. G.L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography **22** (2001), pp. 107–121.
32. G.L. Matthews, *Codes from the Suzuki Function Field*, IEEE Transactions on Information Theory **50(12)** (2004), pp. 3298–3302.
33. G.L. Matthews and T. Michel, *One-point codes using places of higher degree*, IEEE Transactions on Information Theory **51** (2005), pp. 1590–1593.
34. MinT. *Online database for optimal parameters of* (t, m, s)*-nets,* (t, s)*-sequences, orthogonal arrays, linear codes, and OOAs*. Available at http://mint.sbg.ac.at/
35. R. Matsumoto and S. Miura, *On the Feng-Rao bound for the L-construction of Algebraic-Geometry codes*. IEICE Transactions on Fundamentals, **5** (2000), pp. 923-927.
36. C. Munuera and R. Pellikaan, *Equality of geometric Goppa codes and equivalence of divisors*, Journal of Pure and Applied Algebra **90** (1993), pp. 229–252.
37. C. Munuera and F. Torres, *Bounding the trellis state complexity of algebraic geometric codes*, Applicable Algebra in Engineering, Communication and Computing **15** (2004), pp. 81–100.
38. C. Munuera, A. Sepúlveda and F. Torres, *Algebraic Geometry codes from Castle curves*, In Coding Theory and Applications, LNCS 5228, pp. 117–127, Springer-Verlag, Berlin, 2008.
39. C. Munuera, A. Sepúlveda and F. Torres, *Castle curves and codes*, Advances in Mathematics of Communication **3** (2009), pp. 399–408.
40. C. Munuera, A. Sepúlveda and F. Torres, *Generalized Hermitian codes*, Designs, Codes and Cryptography **69** (2013), pp. 123–130.
41. C. Munuera, G. Tizziotti and F. Torres, *Two-point codes on Norm-Trace curves*. In Coding Theory and Applications, LNCS 5228, pp. 128–136, Springer-Verlag, Berlin, 2008.
42. W. Olaya-León and C. Munuera, *On the minimum distance of Castle codes*, Finite Fields and Applications **20** (2013), pp. 55–63.
43. R. Pellikaan, *On special divisors and the two variable zeta function of algebraic curves over finite fields*. In Arithmetic, geometry and coding theory, pp. 175-184, de Gruyter, Berlin, 1996.
44. H. Stichtenoth, *A note on Hermitian codes over* $\mathbb{F}_{q^2}$, IEEE Transactions on Information Theory **34(5)** (1988), pp. 1346–1348.
45. H. Stichtenoth, *Algebraic Functions Fields and Codes*. Springer-Verlag, Berlin, 1993.
46. M.A. Tsfasman, S.G. Vladuts and T. Zink, *Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound*, Mathematische Nachrichten **109** (1982), pp. 21–28.
47. K. Yang and P.V. Kumar, *On the true minimum distances of Hermitian codes*. In Coding Theory and Algebraic Geometry, LNCS 1518, pp. 99-107, Springer-Verlag, Berlin, 1992.

University of Valladolid
Current address: Avda Salamanca SN, 47014 Valladolid, Castilla, Spain
E-mail address: cmunuera@arq.uva.es

Universidad Industrial de Santander
Current address: Cra 27, Cll 9, AA 678 Bucaramanga, Santander, Colombia.
E-mail address: wolaya@uis.edu.co