Contemporary Mathematics

Evaluation Codes and Plane Valuations

J. I. Farrán and C. Galindo

Abstract. Evaluation codes are a particular construction of error-correcting codes, consisting of evaluating functions at rational places of certain geometric objects. Classical examples are Reed-Muller or Reed-Solomon codes. In recent years many other constructions have arisen, like algebraic geometry codes (AG codes in short), toric codes or complete intersection codes. This paper is addressed to survey the above mentioned cases, together with evaluation codes coming from order functions, with a special emphasis on a recent construction of codes obtained from plane valuations.

Contents

1. Introduction

Evaluation codes are error-correcting codes constructed by evaluating functions from some suitable vector space at rational places of some geometric object. Very important families of error-correcting codes, as Reed-Muller, Reed-Solomon and AG codes, can be regarded as families of evaluation codes. Facts as the usefulness of Reed-Solomon codes or the existence of AG codes attaining the Varshamov-Gilbert bound [**51**] explain the importance of these codes. We devote this paper to review some of the most interesting evaluation codes, laying special emphasis on those obtained with plane valuations.

The introductory part of Section 2 defines this class of codes, explains the main problems which appear for constructing them, and presents their most known and

Key words and phrases. Evaluation codes, plane valuations, Hamburger-Noether expansions, semigroups at infinity, resolution of singularities.

Farrán is partially supported by Spain Ministry of Economy: MTM2012-36917-C03-01 and Galindo by MTM2012-36917-C03-03 and Universitat Jaume I: P1-1B2012-04.

classical examples. Afterwards in successive subsections, we define and provide the main properties and results on the parameters of AG codes, codes defined over higher dimensional varieties, toric and differential codes, and codes determined by order functions. We do not show proofs of the results, but give references where the reader can check the details about our statements. AG codes are surely the most studied among the codes that we present here. They enjoy the advantages of being supported in deep theorems of algebraic geometry, and having efficient decoding algorithms. Indeed, the so-called Berlekamp-Massey-Sakata algorithm [**5, 37, 42**] has been used to get fast implementations of both, the modified algorithm given in [**32, 45**] (see also [**33, 30**]), and the majority voting scheme for unknown syndromes of Feng and Rao [**16**], [**47**] (see also [**43, 44**]). Codes given by order functions were introduced in [**29**] to simplify AG codes given by divisors defined with a unique point. However, if one allows semigroups to be different from that of positive integers, then the family of obtained codes is very enlarged. These new codes admit similar decoding methods as the above mentioned for AG codes, and Feng-Rao type bounds for their minimum distances can be given. In addition, Section 2 devotes a subsection to codes defined by varieties different from curves and to toric codes introduced by Hansen and studied, among others, by Ruano. We also consider the so-called differential codes. Although, there is no known procedure for decoding them, they admit good estimates of their parameters thanks to Cayley-Bacharach Theorem.

In all the above cases, one needs to solve some computational problems for constructing evaluation codes. For the case of AG codes, computations related to algebraic curves are required and Section 3 is addressed to analyze such computations for the special case of having plane curves. Thus, we study first the resolution of singularities of plane curves and how to use it to construct codes using the desingularized curves. We introduce the Hamburger-Noether expansions, which provide both the desingularization at a singular point and natural parameterizations of the corresponding *branches*. We also remark that it is possible to compute a vector basis of the so-called Riemann-Roch spaces by means of the Brill-Noether algorithm. This is the crucial step of the construction of AG codes, although this method only applies for plane curves, since it is based on the adjunction theory. Furthermore, in this section we study the particular situation of curves with only one point at infinity. That is a very common case in coding theory examples, for which we show an alternative way to construct the Weierstrass semigroups with the aid of the Abhyankar-Moh algorithm. Finally, the use of order functions as an elementary approach to AG codes is treated.

Order functions and, especially, those named weight functions were defined over the semigroup of nonnegative integers with the aim of doing understandable one point AG codes for non expert in algebraic geometry people. However, the families of the obtained codes are much increased simply by extending their value semigroups. We know few things about these order functions, but this is not the case for some similar objects as valuations. They have been studied because of their relation with singularity theory in algebraic geometry, and plane valuations are classified in [**46**] (see also [**52**]). As a consequence, valuations seem to be one of the best sources for obtaining weight functions. In [**20**, Proposition 2.2], one can see how to get weight functions from valuations and, in [**21**], a class of plane valuations that is well-adapted to these purposes, namely plane valuations

at infinity, is introduced. Semigroups of weight functions defined by them are easy to handle, because they are generated by the so-called (generalized) δ-sequences. The corresponding valuations are related to curves with only one place at infinity, which have useful properties for coding theory as one can see in [**8**]. To construct the above mentioned weight functions, one only needs certain sequences of values in $\mathbb{Z}^2$, $\mathbb{Q}$ or $\mathbb{R}$, which are the mentioned δ-sequences. Order bounds for the codes of the corresponding dual families and some well-behaved examples can be seen in [**21**].

The previous paragraph has introduced the objects we will study in Sections 4 and 5. In Section 4, we recall the concept of valuation. Unfortunately, a complete classification is only available for the planar case, and this is the reason for using plane valuations. We recall this classification and afterwards introduce a subclass of the set of plane valuations, the so-called plane valuations at infinity, which is suitable for coding purposes. Valuations in this subclass intersect all the types of valuations of the mentioned classification of valuations. A remarkable result by Matsumoto [**38**] asserts that order domains corresponding to one-point AG codes are affine coordinate rings of algebraic curves with exactly only one place at infinity. Our subclass of plane valuations is closely related to such algebraic curves, and the corresponding valuations determine weight functions whose attached value semigroup is spanned by δ-sequences. To get our codes, we only need a δ-sequence and a family of points to be evaluated. Since our codes are given by order functions, they admit Feng-Rao type bounds and have efficient decoding algorithms. A detailed explanation of the above facts and some explanatory examples are given in Section 4 and in the first subsection of Section 5.

The mentioned codes, over a finite field $\mathbb{F}_q$, have length at most q^2, but codes given by weight functions (an important property due to their advantages for the decoding procedure) of arbitrary length can be also made if one considers a number of plane valuations at infinity, which depends on the length of the code one desires. We explain this fact, developed in [**22**], in the second subsection of Section 5, where some examples are added to make easier its reading.

2. Evaluation codes

Evaluation codes are a very common type of error-correcting codes. The general idea of their construction is quite simple:

(1) Take a geometric object χ defined over a finite field $\mathbb{F}_q$.
(2) Take a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ with n rational places in χ, i.e. defined over the base field $\mathbb{F}_q$.
(3) Consider a (finite dimensional) vector space L with rational functions on χ which are well-defined over the points in $\mathcal{P}$.
(4) Evaluate the functions of L at the points in $\mathcal{P}$

$$\begin{array}{rccc} \varphi : & L & \to & \mathbb{F}_q^n \\ & f & \mapsto & f(P_1, \ldots, P_n) \end{array}$$

obtaining the code $C := \operatorname{Im} \varphi$ as the image of this linear map.

This construction is general, but in order to construct good codes in this way one needs to choose suitable χ, $\mathcal{P}$ and L so that the construction of such codes is computationally effective, coding and decoding are efficient tasks, and good estimates for the parameters can be given from the mathematical properties of the

involved geometric objects. To this end, the main practical problems to solve, depending on the nature of χ, are the following:

(A): Find sufficiently many places $\mathcal{P}$ in χ, if we want the length n to be sufficiently large.

(B): Compute a basis of the vector space L.

(C): Evaluate functions in L at points of $\mathcal{P}$. This is usually an easy task, but not always (see Section 3).

(D): Obtain the generator matrix of the code in order to compute the coding map. This follows immediately from tasks **(B)** and **(C)**.

(E): Get good estimates for the dimension and the minimum distance of the code.

(F): Design efficient decoding procedures, for both error-detection and error-correction. Tasks **(E)** and **(F)** strongly rely on special geometrical properties of the chosen object χ.

Practical efficiency of these codes is usually achieved by dividing all the coding and decoding tasks into two parts:

- **Preprocessing**, where we group the hard tasks of the coding and decoding algorithms. These computations are to be performed only once from the geometric data of the construction, and they can be time consuming since they are done before the real-time applications (namely, encoding information and correcting errors from a received transmission).
- **Coding and Decoding** algorithms themselves must be fast for real applications, once all the preprocessing is previously performed (efficiency means polynomial time, and real time applications require complexity at most $\mathcal{O}(n^3)$).

In this section, we will introduce the following constructions of evaluation codes: AG codes (where algebraic curves are used as the geometric object χ), variety codes (using higher dimensional varieties instead of curves, including complete intersection varieties), toric codes (using toric varieties), differential codes (using the singular locus of a differential form), and codes given by order functions. Beforehand, we present two very classical examples which are in fact evaluation codes.

Example 2.1 (Reed-Solomon codes). Reed-Solomon codes can be defined as primitive BCH codes over $\mathbb{F}_q$ with $n = q - 1$ (see [**36**]). BCH codes are a very interesting family of codes where the minimum distance can be estimated just by imposing conditions on the involved polynomials (designed minimum distance). The advantage of Reed-Solomon codes is that the n-th root of unity used, α, is in the base field, so that all the computations with the code are performed inside $\mathbb{F}_q$ and no field extension is needed. Nevertheless, the main disadvantage is that the length is bounded to be $q - 1$, so that when the finite field is fixed we cannot get codes with arbitrarily large length n and, in particular, there is no Reed-Solomon code over the binary field $\mathbb{F}_2$.

Anyway, Reed-Solomon codes are widely used in real life over extensions $\mathbb{F}_{2^m}$ of $\mathbb{F}_2$. For example, concatenated Reed-Solomon codes over $\mathbb{F}_{256}$ are used to correct both random errors (inner code) and burst codes (outer code) in the CD and DVD players. On the other hand, Reed-Solomon codes are MDS, meaning that they satisfy the equality $k + d = n + 1$, k and d being respectively the dimension and the minimum distance of the code. Notice that the previous equality means that

Reed-Solomon codes attain the Singleton bound (see [**36**]). Finally, Reed-Solomon codes can be efficiently decoded, so that they are suitable for real life applications.

Reed-Solomon codes were originally defined as evaluation codes by evaluating polynomials f of degree at most $k-1$ at all the nonzero points of $\mathbb{F}_q$. Thus, their words have the form $(f(1), f(\alpha), \ldots, f(\alpha^{q-2}))$. This way is more convenient for encoding k information symbols (in fact, the coefficients of such a polynomial are precisely the information symbols). The reader can check for example in [**36**] that both definitions of Reed-Solomon codes are equivalent. Note also that the dual of a Reed-Solomon code is again a Reed-Solomon code.

EXAMPLE 2.2 (Reed-Muller codes). Let $\chi = \mathbb{F}_q^m$ be the affine space over the finite field $\mathbb{F}_q$, and take all rational points $\mathcal{P} = \mathbb{F}_q^m$ for evaluation. Consider the polynomial space $V = \mathbb{F}_q[X_1, \ldots, X_m]$ with infinite dimension, and evaluate such polynomials at $\mathcal{P}$

$$\varphi : \mathbb{F}_q[X_1, \ldots, X_m] \to \mathbb{F}_q^n,$$

where $n := q^m$ is the number of all affine points (i.e., we consider polynomial functions). One can easily check that the map φ is surjective. Note that for $q = 2$ such polynomial functions look like *truth tables*.

The q-ary Reed-Muller code of order r and length $n = q^m$ is denoted by $\mathcal{RM}_q(r, m)$, and it is defined as the image by the above evaluation map of the space of polynomials with degree at most r, that is $L := \mathbb{F}_q[X_1, \ldots, X_m]_{(r)}$. Notice that when evaluating in $\mathbb{F}_q$ we have $X_i^q \equiv X_i$, so that we can actually work in the ring

$$\mathbb{F}_q[X_1, \ldots, X_m]/\langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$$

of the so-called *reduced polynomials*. For $q = 2$, reduced polynomials are called *Boolean functions*.

One easily checks that for $r > m(q-1)$, $\mathcal{RM}_q(r, m) = \mathbb{F}_q^n$ holds, since reduced polynomials have degree at most $m(q-1)$ and the evaluation map is surjective. Computing parameters of Reed-Muller codes is just a combinatorial problem (see [**36**] for the details). In fact, the dimension of $\mathcal{RM}_q(r, m)$ is just

$$k = \sum_{t=0}^{r} \sum_{i=0}^{m} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} \begin{pmatrix} t - iq + m + 1 \\ t - iq \end{pmatrix}.$$

For $q = 2$, it happens that the dimension of $\mathcal{RM}_2(r, m)$ is

$$k = \sum_{t=0}^{r} \begin{pmatrix} m \\ t \end{pmatrix}.$$

In addition, the minimum distance of $\mathcal{RM}_q(r, m)$ for $0 \leq r \leq m(q-1)$ is $d = (q-s)q^{m-\nu-1}$, provided $r = \nu(q-1) + s$ with $0 \leq s < q-1$. Finally, we remark that Reed-Muller codes are efficiently decoded by using majority logic.

2.1. AG codes.

Algebraic Geometry codes (AG codes in short) can be considered as a generalization of Reed-Solomon codes. In fact, Reed-Solomon codes can be constructed from the projective line, whereas AG codes come from any arbitrary projective curve. To define an AG code, we take as geometric object an absolutely irreducible projective smooth algebraic curve χ over $\mathbb{F}_q$, consider a set $\mathcal{P}$ of rational points in χ as places to evaluate at, and the Riemann-Roch space $\mathcal{L}(G)$ will be the set of functions to be evaluated, choosing the divisor G so that these functions are

well-defined at the points in $\mathcal{P}$. Although the details are referred to [**29**], we are going to give some basic information about these codes.

Let $\mathbb{F}_q(\chi)$ be the function field of χ over $\mathbb{F}_q$, and denote by $\Omega(\chi)$ the space of differential forms over $\mathbb{F}_q$. One can consider three families of points on χ:

Rational points: Those with coordinates in the base field $\mathbb{F}_q$.
Geometric points: Those with coordinates in the algebraic closure $\overline{\mathbb{F}}_q$.
Closed points: Conjugation classes of geometric points under the Frobenius map.

A (rational) divisor of χ is any formal linear combination of closed points with integer coefficients. For any divisor H one considers the function space

$$\mathcal{L}(H) := \{\varphi \in \mathbb{F}_q(\chi) \mid (\varphi) + H \geq 0\} \cup \{0\}$$

where (φ) denotes the divisor of zeros and poles of the function φ, and ≥ 0 means to be effective (that is, every nonzero coefficient of the divisor is positive).

Now one takes two divisors $D = P_1 + \ldots + P_n$ and $G = \sum_P n_P P$ such that $\mathrm{supp}\,(G) \cap \mathrm{supp}\,(D) = \emptyset$ and consider the $\mathbb{F}_q$-linear evaluation map

$$\begin{array}{rccc} ev_D \ : & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & \varphi & \mapsto & (\varphi(P_1), \ldots, \varphi(P_n)) \end{array}$$

so that the (evaluation) AG code is defined by the image

$$C_L = C_L(D, G) := \mathrm{im}\,(ev_D).$$

The dual of C_L is

$$C_\Omega = C_\Omega(D, G) := C_L(D, G)^\perp,$$

which can be regarded either as a code obtained by evaluating residues of certain differential forms in $\Omega(\chi)$ or, again, as an evaluation AG code for a suitable divisor (see [**29**]). Estimates of the parameters of AG codes can be obtained by using the Riemann-Roch Theorem in the following way:

THEOREM 2.3 (Goppa). *Assume that $2g - 2 < deg\, G < n$, then the map ev_D is injective, and one has*

$$k(C_L) = \deg\, G + 1 - g \quad \text{and} \quad d(C_L) \geq n - \deg\, G := d^*(C_L).$$
$$k(C_\Omega) = n - deg\, G + 1 - g \quad \text{and} \quad d(C_\Omega) \geq deg\, G + 2 - 2g := d^*(C_\Omega).$$

The numbers d^* in the above result are called the (corresponding) *Goppa distances*, and they play the same role as the designed minimum distances in BCH codes.

On one hand, a generator matrix for $C_L(D, G)$ is

$$\begin{pmatrix} \varphi_1(P_1) & \ldots & \varphi_1(P_n) \\ \ldots & \ldots & \ldots \\ \varphi_k(P_1) & \ldots & \varphi_k(P_n) \end{pmatrix},$$

where $\{\varphi_1, \ldots, \varphi_k\}$ is a basis of $\mathcal{L}(G)$ over $\mathbb{F}_q$. By "duality", the above matrix is also a parity-check matrix for $C_\Omega(D, G)$.

On the other hand, it is possible to prove that $C_\Omega(D, G) = C_L(D, W + D - G)$ for a suitable canonical divisor W (see [**29**]). Thus, just by using linear algebra, we can easily compute a generator matrix for $C_\Omega(D, G)$ and a parity-check matrix for $C_L(D, G)$. This efficiently solves the problem of encoding and error-detection,

assumed that we are able to compute bases for the corresponding *Riemann-Roch spaces*.

EXAMPLE 2.4 ([**29**]). Consider the plane curve χ over $\mathbb{F}_4$ given by the equation

$$X^3 + Y^3 + Z^3 = 0.$$

Since the cube of any element in $\mathbb{F}_4$ is 0 or 1, then all the rational points in χ have a projective coordinate equal to 0, so that we may take one of the other coordinates equal to 1. Thus, it is easy to list the 9 rational points of this curve (see below).

Now take $Q = (0 : 1 : 1)$. By the Riemann-Roch theorem we get that the dimension of $\mathcal{L}(3Q)$ equals 3 (note that the curve is nonsingular and its genus is $g = 1$). In fact, a basis of this Riemann-Roch space is

$$\{1, \frac{X}{Y+Z}, \frac{Y}{Y+Z}\}.$$

Thus, by using the remaining $n = 8$ rational points for evaluation, and denoting by α the primitive element of $\mathbb{F}_4$, we may compute a generator matrix for the corresponding AG code as

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2 & 1 & \alpha & \alpha^2 \\ \alpha^2 & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

where the list of points is

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

Finally, note that Goppa theorem implies that $d \geq 5$, and looking at G the minimum distance is exactly $d = 5$.

Dual codes given by $G = mP_\infty$, being $m > 0$ and P_∞ an "extra" rational place (i.e. a rational point not used for evaluation), are called *one-point (AG) codes*. Their Goppa distances can be improved by the so-called *Feng-Rao distances*, defined on the Weierstrass semigroup of χ at P_∞. Such semigroup is nothing but the complementary in $\mathbb{N}$ of the (finite) set of *Weierstrass gaps* of χ at P, where a positive integer m is called a gap if and only if $\mathcal{L}(mP) = \mathcal{L}((m-1)P)$ (see [**18**] for further details).

In fact, let $G = mP_\infty$ and $\Gamma_P = \{\rho_i \mid i \in \mathbb{N}\}$ be an increasing enumeration of the elements in the Weierstrass semigroup of χ at P_∞ (i.e., $0 = \rho_1 < \rho_2 < \rho_3 \cdots$). Denote $C_r := C(\rho_r)$, where $C(m) := C_\Omega(D, mP_\infty)$. If we fix a function g_i with only one pole at P_∞ of order ρ_i, then $\{g_1, \ldots, g_r\}$ is a basis of $\mathcal{L}(\rho_r P_\infty)$. Thus, the matrix H_r with rows $\mathbf{h}_i := ev_D(g_i)$, $1 \leq i \leq r$, is a parity-check matrix for C_r. The *dimension* of these codes is given by $n - k_r$ where $k_r = \text{card}\,(\Gamma_P \cap [0, \rho_r])$, and the *minimum distance* satisfies $d_r \geq \delta_{FR}(\rho_{r+1}) \geq d_r^*$, where

$$\delta_{FR}(\rho_r) := \min\{n_s \mid s \geq r\},$$

being $n_r := \text{card}\,\mathcal{N}_r$ and $\mathcal{N}_r := \{(i,j) \in \mathbb{N}^2 \mid \rho_i + \rho_j = \rho_{r+1}\}$.

The integer $\delta_{FR}(\rho_r)$ is called the Feng-Rao distance of the code C_r. This estimate for the minimum distance is usually better than the Goppa distance. The main interest of these codes comes from the fact that they have a very fast decoding procedure by means of the so-called Feng-Rao (majority) decoding algorithm (see

[**29**]). In general, AG codes can be decoded efficiently with *preprocessing*. The main computational problems involved in this preprocessing are the following:

(1) Find curves with sufficiently many rational places, (so that n is large enough), and compute explicitly such points with the aid of Groebner bases tools.

(2) Compute Weierstrass semigroups and their associated functions or, in general, compute bases for the Riemann-Roch spaces $\mathcal{L}(G)$. This can be done with the aid of the Brill-Noether algorithm, when plane curves are used (see [**9**]).

(3) Compute pole orders, and evaluate functions at rational places.

(4) Compute the Feng-Rao distance (this can be easily done with numerical semigroup techniques, see [**8**]).

We will provide more details about some of these problems in Section 3.

2.2. Codes on varieties.

We outline here two different approaches in order to generalize AG codes to higher-dimensional varieties. The first one is more algebraic, and the second one has a more geometric nature.

The algebraic approach is referred to [**24**]. Consider an ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$, define

$$I_q := I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle \text{ and } R_q := \mathbb{F}_q[X_1, \ldots, X_m]/I_q$$

and consider $V = \mathcal{V}_{\mathbb{F}_q}(I_q) = \mathcal{V}_{\overline{\mathbb{F}}_q}(I_q) = \{P_1, \ldots, P_n\}$ the variety of I_q over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Define an evaluation $\mathbb{F}_q$-linear map $ev : R_q \to \mathbb{F}_q^n$ given by

$$ev(F + I_q) = (F(P_1), \ldots, F(P_n)).$$

Notice that this map is surjective. Finally, for a linear subspace $L \subseteq R_q$ of finite dimension, we get the code $C(I, L) = ev(L)$ and its orthogonal code $C(I, L)^\perp$.

Groebner bases theory is the main tool to work with these codes. We state here the main properties of these codes (see [**24**] for further details):

(1) The points P_i of the variety V are computed with a combination of Groebner basis calculations and triangulation procedures.

(2) The length of the codes is given by the cardinality of the so-called *footprint* $\Delta(I_q)$ of the ideal I_q, where the footprint of an ideal $J \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$, for a fixed monomial ordering, is defined as the set of monomials in $\mathbb{F}_q[X_1, \ldots, X_m]$ which are not the leading monomial of any polynomial in J.

(3) Since the evaluation map is injective, the dimensions of the mentioned codes are

$$\dim C(I, L) = \dim(L),$$
$$\dim C(I, L)^\perp = n - \dim(L).$$

(4) The minimum distance of the code $C(I, L)$ can also be estimated by means of footprints and well-behaving bases.

(5) Finally, the minimum distance of the code $C(I, L)^\perp$ can be estimated by an analogous of the Feng-Rao bound, also in terms of footprints and well-behaving bases. For the special case when R_q is an order domain, one retrieves the classical Feng-Rao distance in terms of some numerical semigroups (see [**29**]).

We finish this section summarizing the geometric approach for constructing evaluation codes from higher dimensional varieties given in [**34**]. Let $\chi \subseteq \mathbb{F}_q^m$ be an algebraic variety and $\mathcal{S} = \{P_1, \ldots, P_n\}$ a finite set of rational points of χ. Consider

$\mathcal{F}$ an $\mathbb{F}_q$-vector space (with finite dimension) of rational functions on χ, so that these functions are well-defined on $\mathcal{S}$. Then, the corresponding evaluation code is defined as the image of the linear map

$$\begin{array}{rccl} ev_{\mathcal{S}} & : & \mathcal{F} & \to & \mathbb{F}_q^n \\ & & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

and the corresponding dual code is obtained by orthogonality. Now the problem for constructing these codes is far more complicated and strongly depends on the nature of the variety χ. Even though there are general bounds for the parameters, the best results can be obtained by considering special varieties like quadrics, Hermitian hypersurfaces, Grassmannians and flag varieties, ruled surfaces or Deligne-Lusztig varieties.

2.3. Toric codes.

Toric codes are constructed from the so-called toric varieties. In fact, computations with this kind of varieties are reduced to combinatorics, so that toric codes are suitable for explicit and effective constructions. Indeed, as we will see later, the construction of toric codes is reduced to evaluate monomials inside a *polytope* at points of the *algebraic torus* (i.e., points with nonzero coordinates). The details of this section are referred to [**39**].

The construction of toric codes is as follows: Consider a (rational) polytope P over $\mathbb{F}_q$, with dimension $r \geq 2$, let X_P be the associated toric variety (which is a regular variety) and D_P the corresponding *Cartier divisor* over X_P. For any $t \in T = (\mathbb{F}_q^*)^r$ in the algebraic torus T, the rational functions in $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ can be evaluated at t and we define the toric codes by evaluating the rational functions of $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ at the $(q-1)^r$ points of the torus $T = (\mathbb{F}_q^*)^r$, namely

$$\begin{array}{rccl} ev_T : \mathrm{H}^0(X_P, \mathcal{O}(D_P)) & \to & (\mathbb{F}_q)^{\mathrm{card}\ T} \\ f & \mapsto & (f(t))_{t \in T}, \end{array}$$

obtaining the *toric code* $\mathcal{C}_P$ associated to the polytope P as the image of the above linear map. The length of $\mathcal{C}_P$ is obviously $\mathrm{card}\ T = (q-1)^r$.

Note that $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ is a $\mathbb{F}_q$-vector space of finite dimension, with basis $\{\chi^u \mid u \in P \cap M\}$, M being a lattice isomorphic to $\mathbb{Z}^r$ for some r, and where χ^u denotes a Laurent monomial $X_1^{u_1} \cdots X_r^{u_r}$ (see [**39**] for further details). Basically, up to an isomorphism, M consists of the of integer points in the corresponding ambient affine space where the polytope is embedded. In other words, this basis consists of those monomials whose (integer) exponents are inside the polytope P. In particular, the computation of integer points inside polytopes involves algorithms of combinatorial geometry.

Thus, a generator system for the code $\mathcal{C}_P$ is just $\{(\chi^u(t))_{t \in T} \mid u \in P \cap M\}$, and this becomes a basis if and only if the evaluation map is *injective*. In other words, encoding procedures are described in terms of combinatorics.

We will explicitly show how to get such a basis, even without the *injectivity condition*. Let P be a polytope and $\mathcal{C}_P$ the associated toric code. For every $u \in P \cap M$, write $u = c_u + b_u$ with $c_u \in H = \{0, \ldots, q-2\}^r \subset M$ and $b_u \in ((q-1)\mathbb{Z})^r$ and denote $\overline{u} = c_u$ and $\overline{P} = \{c_u \mid u \in P\} \subset P \cap M$. The kernel of the evaluation map is generated by

$$\{\chi^u - \chi^{u'} \mid u, u' \in P \cap M,\ c_u = c_{u'}\},$$

so that a basis of $\mathcal{C}_P$ is just $\{(\chi^{c_u}(t))_{t\in T} \mid u \in P \cap M\}$. As a consequence, the dimension of $\mathcal{C}_P$ is precisely

$$k = \text{card } \{\overline{u} \mid u \in P \cap M\} = \text{card } \overline{P}.$$

The polytope P satisfies the injectivity condition when for all $u, u' \in P \cap M$, one has that $u \neq u'$ implies $c_u \neq c_{u'}$ (i.e. the evaluation map ev_T is injective). In such case, the code $\mathcal{C}_P$ has dimension $k = \text{card } (P \cap M)$, that is precisely the number of integer points inside the polytope P. Notice that there exist polynomial algorithms to count integer (lattice) points inside a polytope (see [**12**]). Moreover, for plane polytopes, Pick's formula [**3**] holds, namely

$$\text{card } (P \cap M) = \text{vol}_2(P) + \frac{\text{per}(P)}{2} + 1,$$

where vol_2 is the planar Lebesgue volume, and $\text{per}(P)$ the number of lattice points in the border of the polytope. Notice that the above formula is true whenever all the vertices of the polytope P are in the lattice M.

EXAMPLE 2.5 ([**41**]). Consider the plane polytope with vertices $(0,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b,2b)$ and $(0,b)$ with $b < q-1$. The length of the corresponding toric code is $n = (q-1)^2$ and the evaluation map is injective because of the assumption $b < q-1$. On the other hand, by applying Pick's formula one gets that the dimension equals to

$$k = \text{vol}_2(P) + \frac{\text{per}(P)}{2} + 1 = 3b^2 + 3b + 1.$$

EXAMPLE 2.6. Consider $\mathbb{F}_7$ and the plane polytope with vertices $(0,0)$, $(4,1)$ and $(1,4)$. In this case, the length of the toric code is $n = 36$ and we may list all the monomials:

$$\{1, XY, XY^2, XY^3, XY^4, X^2Y, X^2Y^2, X^2Y^3, X^3Y, X^3Y^2, X^4Y\}$$

Finally, we have to evaluate to obtain a generator matrix of such code.

We add that, in the literature, one can found several ways to estimate the minimum distance of these codes, namely using combinatorics and elementary computations (see [**31**]), mixed volumes of polytopes (see [**41**]), Intersection Theory (see [**28**] and [**41**]), Minkowsky sums (see [**35**]), and the Minkowsky length (see [**49**]).

As an example, we briefly show how to bound the minimum distance with the aid of Minkowsky sums. The Minkowsky sum of two polytopes P and Q is the set containing the pointwise sums of their points $P+Q := \{p+q \mid p \in P,\ q \in Q\}$. Let P be a polytope with $P \cap M \subseteq \{0, \ldots, q-2\}^r$, and take $q \gg 0$ a large enough positive integer. Consider the largest positive integer l such that there exists a polytope $Q \subset P$ which is the Minkowsky sum of l non-trivial polytopes $Q = P_1 + \cdots + P_l$, non-trivial meaning that all the polytopes have positive dimension. Then, there actually exists such a polytope $Q \subset P$ satisfying

$$d(\mathcal{C}_P) \geq \sum_{i=1}^{l} d(\mathcal{C}_{P_i}) - (l-1)(q-1)^2.$$

We also notice that an upper bound can be obtained in a similar way (see [**35**] for the details).

As a final remark, we note that a decoding procedure for these codes is feasible and efficient. This procedure makes use of order functions (described later in this

paper) and the Feng-Rao majority decoding algorithm (see the details in [**4**] and [**29**]).

2.4. Differential codes.

We devote this section to describe a recent construction of evaluation codes from a completely new point of view. Here, we evaluate polynomials up to a certain degree at some singular points of an algebraic differential equation over a finite field (the details are referred to [**10**]). In this case, the decoding problem is not yet solved, although the construction provides good estimates for the parameters via cohomology theory and the Cayley-Bacharach Theorem.

More precisely, take $P_1, \ldots, P_n$ points in the affine plane $\mathbb{A}^2$ which are rational over $\mathbb{F}_q$. For an integer $m > 0$, denote by $\mathbb{F}_q[x,y]_{\leq m}$ the set of polynomials with degree at most m, and consider the (linear) evaluation map given by

$$\begin{array}{rccc} \mathcal{E} : \mathbb{F}_q[x,y]_{\leq m} & \longrightarrow & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

In general, it is not easy to estimate the parameters of the code $E_m := \mathrm{Im}(\mathcal{E})$. Nevertheless, we will consider the special case where the points $P_1, \ldots, P_n$ lie in the singular locus of a foliation.

In fact, let $(X : Y : Z)$ be homogeneous coordinates on the projective plane over $\mathbb{F}_q$, $\mathbb{P}^2 := \mathbb{P}^2_{\mathbb{F}_q}$. A *foliation* $\mathcal{F}$ of degree $r \geq 0$ on $\mathbb{P}^2$ can be given by a differential form $\Omega = AdX + BdY + CdZ$, where A, B, C are homogeneous polynomials of degree $r+1$ with no common factor and satisfying the Euler condition $XA + YB + ZC = 0$. Notice that it corresponds locally to an algebraic differential equation.

The *singular scheme* of $\mathcal{F}$ is the zero-dimensional closed subscheme of $\mathbb{P}^2$ given by the indeterminacy ideal $\mathcal{I}$ of the polarity map Φ, i.e. the ideal $\mathcal{I} = (A, B, C)$. In such points, the gradient of the differential form is not well-defined. This singular locus is computed in practice from Ω by means of Groebner basis computations.

The following result, proved in [**11**], shows that we do not actually need the foliation, but just a set of points satisfying some geometric conditions. In fact, a set of points $\mathcal{Z} = Z(\mathcal{I})$ is the singular locus of a foliation in $\mathbb{P}^2$ with degree $r \geq 2$ if and only if the following conditions hold:

(1) There are at least 3 independent divisors of degree $r+1$ passing through all the points of $\mathcal{Z}$.
(2) For each $1 \leq j \leq r-2$ there is no subset with $(r-j)(r+1)$ points of $\mathcal{Z}$ lying on a divisor of degree $r-j$.
(3) There is no subset of $r+2$ points of $\mathcal{Z}$ lying on a (projective) line.

Now, let $\mathcal{F}$ be a (projective) foliation of degree $r \geq 2$ over $\mathbb{F}_q$, and assume that the singularities of $\mathcal{F}$ are reduced and rational over $\mathbb{F}_q$. Thus, the support of $Z(\mathcal{I})$ consists of $r^2 + r + 1$ different rational points of $\mathbb{P}^2$, r being the degree of the foliation. This implies $r \leq q$, since the number of rational points of $\mathbb{P}^2$ is precisely $q^2 + q + 1$.

Denote by $P_1, ..., P_n$ the points in $Z(\mathcal{I}) \cap \mathbb{A}^2$, and by l the cardinality of $Z(\mathcal{I}) \cap H$, H being the line at infinity given by $Z = 0$. One obviously has

$$r^2 + r + 1 = n + l.$$

Let m be an integer such that $1 \leq m \leq 2r-2$, and denote by $E_m = E_m(\mathcal{F}, H)$ the code defined by evaluation of the functions of $\mathcal{L}(mH) = \mathbb{F}_q[x,y]_{\leq m}$, $x = X/Z, y =$

Y/Z, at the rational points $P_1, ..., P_n$. In other words E_m is the image of the linear map

$$\mathcal{E} : \mathbb{F}_q[x, y]_{\leq m} \longrightarrow F_q^n$$

given by $f \to (f(P_1), ..., f(P_n))$.

By construction, the length of such codes is $n = r^2 + r + 1 - l$. The geometric properties of the singular locus of $\mathcal{F}$ provide a formula for the dimension and a bound for the minimum distance. In fact, if for every non negative integer s we denote by N_s the number of monomials of degree s in three variables, that is $N_s = (s + 1)(s + 2)/2$, we have the following result:

THEOREM 2.7 ([**10**]). *Under the above conditions, we have:*

(1) *A formula for the dimension:*
   - $k(E_m) = N_m$ *for* $1 \leq m \leq r - 1$.
   - $k(E_m) = N_m - (m - r)(m - r + 2) - \max(0, l + m + 1 - 2r)$ *for* $r \leq m \leq 2r - 2$.

(2) *An estimate for the minimum distance:*
   - $d(E_1) \geq r^2 - l$.
   - $d(E_m) \geq (r + 1)(r - m) - l + 2$ *for* $2 \leq m \leq r - 1$.
   - $d(E_m) \geq 2r - m - l$ *for* $r \leq m \leq 2r - 2$ *, if* $l < 2r - m - 1$.
   - $d(E_m) \geq 2r - m - 1$ *for* $r \leq m \leq 2r - 2$ *, if* $l \geq 2r - m - 1$.

EXAMPLE 2.8. For $q = 3$, consider the foliation given by the forms $A = X(Z^2 - Y^2)$, $B = Y(X^2 - Z^2)$ and $C = Z(Y^2 - X^2)$, with degree $r = 2$ and $q - 1 = 2$ points at infinity (i.e. $n = 5$ and $l = 2$). Notice that A, B and C satisfy the Euler equation and have no common factor. The singular points in the affine chart $Z \neq 0$ are

$$P_1 = (0, 0),\ P_2 = (1, 1),\ P_3 = (1, 2),\ P_4 = (2, 1),\ P_5 = (2, 2)$$

and the singular points at infinity are $Q_1 = (1 : 0 : 0)$ and $Q_2 = (0 : 1 : 0)$. Thus, by taking $m = 1$ one obtains a code with parameters $n = 5$, $k = 3$ and $d = 2$.

EXAMPLE 2.9. In the same way, for $q = 3$, take now the foliation given by $A = (Y + Z)(YZ - X^2)$, $B = X(X^2 - Z^2)$ and $C = X(X^2 - Y^2)$ with degree $r = 2$, but now with just one point at infinity (i.e. $n = 6$ and $l = 1$). The affine singular points are:

$$P_1 = (0, 0),\ P_2 = (0, 2),\ P_3 = (1, 1),\ P_4 = (1, 2),\ P_5 = (2, 1),\ P_6 = (2, 2)$$

and the singular point at infinity is $Q = (0 : 1 : 0)$. If $m = 1$, one gets a code with parameters $n = 6$, $k = 3$ and $d = 3$, which is optimum in the sense that any other code with the same parameters n and k over the finite field with q elements cannot have a larger minimum distance (one can check it by using the Main Conjecture MDS, on *maximum distance separable* codes, see [**36**]).

REMARK 2.10 (Complete Intersection Codes). The construction of differential codes can be generalized to complete intersection varieties in any dimension. In this case, we also evaluate multivariate polynomials up to a certain degree at points of general complete intersection varieties. The construction works since the parameters of the codes can also be estimated with the Cayley-Bacharach Theorem [**27**], even though the decoding problem is not solved yet. This construction can also be regarded as a particular case of the constructions in Section 2.2.

2.5. Codes given by order functions.

We conclude this Section 2 by introducing a large class of codes containing interesting particular cases which will be described later. Consider a commutative semigroup with zero Γ, which admits an ordering $\leq$. The ordering $\leq$ is said to be *admissible* if $0 \leq \gamma$, together with $\alpha \leq \beta$, implies $\alpha + \gamma \leq \beta + \gamma$, where α, β, γ are arbitrary elements in Γ. In addition, Γ is called *cancellative* whenever from the equality $\alpha + \beta = \alpha + \gamma$ one can conclude $\beta = \gamma$. Finally, $\Gamma \cup \{-\infty\}$ will denote the above semigroup together with a new minimal element, denoted by $-\infty$, which satisfies $\alpha + (-\infty) = -\infty$ for all $\alpha \in \Gamma \cup \{-\infty\}$.

DEFINITION 2.11. An *order function* from a $\mathbb{F}_q$-algebra A onto $\Gamma \cup \{-\infty\}$, where Γ is a cancellative well-ordered commutative with zero and with admissible ordering semigroup, is a mapping $w : A \longrightarrow \Gamma \cup \{-\infty\}$ such that, for $p, q \in A$, the following statements are satisfied:

(1) $w(p) = -\infty$ if and only if $p = 0$;
(2) $w(ap) = w(p)$ for all nonzero element $a \in \mathbb{F}_q$;
(3) $w(p + q) \leq \max\{w(p), w(q)\}$;
(4) If $w(p) = w(q)$, then there exists a nonzero element $a \in \mathbb{F}_q^*$ such that $w(p - aq) < w(q)$.

In this case, the triple (A, w, Γ) is called an order domain over $\mathbb{F}_q$ (see for instance [**25**]). When adding the condition $w(pq) = w(p) + w(q)$, one gets the definition of *weight function*.

Order and weight functions for coding purposes were introduced in [**29**] with $\Gamma = \mathbb{N}$ as semigroup. The main advantage of using order functions is that one can consider the filtration of vector spaces $O_\alpha := \{p \in A \mid w(p) \leq \alpha\}$, where α runs over the semigroup Γ. Then, the properties of order function prove that if we set $O_{\alpha^-} := \{p \in A \mid w(p) < \alpha\}$, then the dimension of the quotient vector space O_α / O_{α^-} equals 1. This fact is very useful in coding theory. The purpose of the paper [**29**] was to explain how one point AG codes can be constructed and studied in a simple manner, avoiding the use of algebraic geometry. Indeed, the corresponding order (in fact, weight) function is $-v_{\chi,P}$, where $v_{\chi,P}$ is the valuation given by the curve χ that defines the code at the point $P = P_\infty$.

Notwithstanding, the ideas in [**29**] can be extended to more general codes only by considering different semigroups Γ instead of $\mathbb{N}$. Let us summarize it. Let w be as above and set $ev : A \to \mathbb{F}_q^n$, for some fixed positive integer n, an epimorphism of $\mathbb{F}_q$-algebras. Then, one can construct the family of evaluation codes defined by w and ev as $\{E_\alpha := ev(O_\alpha)\}_{\alpha \in \Gamma}$. We are even more interested, for decoding purposes, in the family of dual codes, which are denoted by $\{C_\alpha := E_\alpha^\perp\}_{\alpha \in \Gamma}$. It is not difficult to prove that there is a positive integer Ω_n such that the vector spaces C_α vanish (and therefore $E_\alpha = \mathbb{F}_q^n$) if and only if $\alpha \geq \Omega_n$.

In order to get bounds on the minimum distance, set

$$\omega_\beta := \mathrm{card}\{(\beta_1, \beta_2) \in \Gamma^2 \ \mid \ \beta_1 + \beta_2 = \beta\},$$

β being any element in Γ. Following the ideas in Section 2.1, the values

$$d(\alpha) := \min\{\omega_\beta \,|\, \alpha < \beta \in \Gamma\}$$

and

$$d_{ev}(\alpha) := \min\{\omega_\beta \,|\, \alpha < \beta \in \Gamma \text{ and } C_\beta \neq C_{\beta^+} \},$$

where $\beta^+ := \min\{\gamma \in \Gamma | \gamma > \beta\}$ are called the *Feng-Rao distances* of C_α. They satisfy $d(C_\alpha) \geq d_{ev}(\alpha) \geq d(\alpha)$, $d(C_\alpha)$ being the minimum distance of the code C_α.

There is also a very related bound for the set of primal codes $\{E_\alpha\}_{\alpha\in\Gamma}$, called the Andersen-Geil bound (see [**2**]).

Concerning a decoding procedure of this class of codes, one can use the methods described in [**29**] for decoding the dual codes: the basic algorithm, which works when w is a weight function, and the extended algorithm, that uses majority voting on unknown syndromes, and which can be used for any order function. Berlekamp-Massey-Sakata algorithm also helps to decode these codes (see for instance [**48**]). In the case of order functions, this algorithm decodes up to half the Feng-Rao distance. Recently, in [**26**], has been proved that the primal codes can also be decoded by a similar procedure up to half of the mentioned Andersen-Geil bound, which in [**26**] is called the Feng-Rao bound for primal codes.

3. Plane curve tools

In this section, we will study some of the computational problems related to plane curves that appear in the effective construction and practical implementation of AG codes. Some of the technical tools and geometric concepts that are needed for these tasks will be useful for the construction of evaluation codes from plane valuations which will be developed in the last part of this paper.

Thus, consider a smooth absolutely irreducible curve χ over $\mathbb{F}_q$, and take its function field $\mathbb{F}_q(\chi)$. If the curve χ is smooth and it is embedded in $\mathbb{P}^n$, one easily evaluates rational functions at rational points, just by substituting variables by the corresponding values. However, we do not have a general method to compute a basis of $\mathcal{L}(H)$ for a divisor H, that is the crucial point of the construction of AG codes.

There exists a general algorithm to compute such a basis for plane curves. However, note that if a curve is plane and non-singular, then the number of rational points is upper bounded by $q^2 + q + 1$, so that we cannot have arbitrarily many rational points for a fixed finite field $\mathbb{F}_q$, whereas if we allow singular points we can have arbitrarily many rational branches, corresponding to rational places in the function field $\mathbb{F}_q(\chi)$. Thus, we may construct AG codes from singular plane curves, just by substituting "points" by "branches", but in this case evaluation of functions at branches is not so evident.

Thus, considering plane curves for constructing AG codes leads to the problem of effective resolution of singularities. In fact, AG codes are constructed just from the algebraic function field and the rational places of the corresponding curve (see [**50**]). If we consider an (absolutely irreducible) plane curve χ over $\mathbb{F}_q$, then the code can be constructed just from the normalization $\tilde{\chi}$, by using the same algebraic function field, and taking into account that rational places correspond to "rational branches". For example, a singular point with two branches corresponds to two places in the normalization.

Therefore, some computational problems arise for plane curves: compute the singular points, the resolution of the singularities (and the genus, as a consequence) together with parameterizations for the rational branches at the singular points, evaluate rational functions at rational branches, and finally compute a basis of the Riemann-Roch spaces $\mathcal{L}(H)$. For the case of one-point AG codes, we need furthermore to calculate the pole order of a rational function at a rational branch,

find the functions achieving the pole orders of the Weierstrass semigroup, and compute the Weierstrass semigroup itself, together with the Feng-Rao distances (this last thing is just a problem in numerical semigroups, that can be solved by means of Apéry sets, see [**8**]).

3.1. Resolution of singularities of plane curves.

Concerning the resolution of singularities, singular points are found by a combination of Groebner bases techniques, triangulation procedures and factorization algorithms for polynomials over finite fields. This task is feasible, since the Jacobian of the curve is a zero-dimensional ideal. In the same way, we find all the points (singular or not) over extensions of $\mathbb{F}_q$, just by adding the equations $X_i^q - X_i = 0$, obtaining again a zero-dimensional ideal.

Once the singular points are found, one has to perform the sequence of blowing-ups to solve each singularity. In positive characteristic, an effective way to solve a singularity is to compute the so-called symbolic Hamburger-Noether expansions (see [**9**]). This procedure is faster than the usual blowing-up sequence, since groups of several blowing-ups are performed in a single step and, furthermore, local parameterizations of the branches together with the local invariants of the singularities are obtained.

Assume that we have a local parametrization of the place (branch) P, namely, with a change of variables so that the base point of P is at the origin of coordinates. Note that such a parametrization can have infinitely many terms, so that we actually use a "lazy" parametrization, which means that we compute as many terms as we need for a concrete calculation. Later, we will see how to obtain parameterizations from the symbolic Hamburger-Noether expressions by lazy computations.

Finally, we wish to evaluate a rational function $\phi = G/H$ at P, where G, H are homogeneous polynomials of the same degree in three variables. To that end, set $(X(t) : Y(t) : Z(t))$ the local parametrization obtained from the symbolic Hamburger-Noether expressions for the branch given by P, substitute

$$\phi(t) = \frac{G(X(t), Y(t), Z(t))}{h(X(t), Y(t), Z(t))} = \frac{a_r t^r + \dots}{b_s t^s + \dots}$$

and then we get the order of ϕ at P as $\nu = r - s$ (note that P corresponds to $t = 0$). In particular, when the order is $\nu \geq 0$, the function is well-defined at P and the evaluation is

$$\phi(P) = a_s/b_s.$$

Clearly $\phi(P) = 0$ if $\nu > 0$. In case $\nu < 0$, ϕ has at P a pole of order $-\nu$. Thus, computing the order of a function at a place can be done by lazy parameterizations of the corresponding branch, that is, by computing as many terms as we need to find r and s in the above formula.

3.2. Symbolic Hamburger-Noether expressions.

We devote this section to introduce the concept of Hamburger-Noether expansion (HNE) for a branch of a plane curve χ with local equation $f = 0$. We may assume in general that the base field is a perfect field $\mathbb{F}$ (a finite field, in particular). Further details about calculations can be found in [**9**]. Assume that we have chosen a suitable affine chart and the corresponding equation so that the point P of the curve χ is at the origin of coordinates.

DEFINITION 3.1. *A branch of χ at P is given by an equivalence class of parameterizations*

$$\rho \, : \, K[[x,y]] \to F[[t]],$$

i.e. formal series $x(t), y(t) \in F[[t]]$ with at least one of them non identically zero, such that $f(x(t), y(t)) \equiv 0$, where K and F are suitable extensions of the base field $\mathbb{F}$.

DEFINITION 3.2. *The Hamburger-Noether expansion (HNE in short) of χ at P for the rational branch given by ρ is a finite sequence $\mathbb{D}$ of expressions, in some new variables $Z_{-1}, Z_0, \ldots, Z_r$, of the form*

$$Z_{-1} = a_{0,1}Z_0 + a_{0,2}Z_0^2 + \ldots + a_{0,h_0}Z_0^{h_0} + Z_0^{h_0}Z_1$$

$$Z_0 = a_{1,2}Z_1^2 + a_{1,3}Z_1^3 + \ldots + a_{1,h_1}Z_1^{h_1} + Z_1^{h_1}Z_2$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Z_{r-2} = a_{r-1,2}Z_{r-1}^2 + a_{r-1,3}Z_{r-1}^3 + \ldots + a_{r-1,h_{r-1}}Z_{r-1}^{h_{r-1}} + Z_{r-1}^{h_{r-1}}Z_r$$

$$Z_{r-1} = \sum_{i \geq 1} a_{r,i}Z_r^i,$$

where r is a non-negative integer, $a_{j,i} \in F$, $a_{k,1} = 0$ if $k > 0$, h_j are positive integers and moreover

$$\varphi(Z_0(Z_r), Z_{-1}(Z_r)) = 0 \quad \text{in} \quad F[[Z_r]]$$

if $\varphi \in K[[x,y]]$ is a generator of the prime ideal $\ker(\rho)$.

If we substitute the last (possibly infinite) line by an implicit equation

$$g(Z_r, Z_{r-1}) = 0$$

we get a symbolic Hamburger-Noether expression.

Notice that such a symbolic Hamburger-Noether expression allows us to compute a rational parameterizations equivalent to ρ, by considering $x \equiv \mathrm{Z}_0$ and $y \equiv \mathrm{Z}_{-1}$ as a function of the local parameter $t = Z_r$ after successive backward substitutions. In fact, by lazy computation, we can add as many terms to the parametrization as we need, that is, by substituting more terms in the above expressions (see [**9**]). The symbolic Hamburger-Noether expressions, together with lazy parameterizations, are implemented in SINGULAR [**13**] with the `hnoether.lib` library.

Moreover, the Hamburger-Noether expansion $\mathbb{D}$ (or the symbolic version) depends only on the branch given by ρ and the choice of the parameters $x(t), y(t)$ in $\mathcal{O}_{\chi,P}$ given by the images of x, y under ρ. The role played by the HNE's in arbitrary characteristic is just the same as that classically played by the Puiseux expansions in characteristic 0. Notice that these ones do not always exist in positive characteristic. Moreover, even when such expansions exist, the problem of making them *primitive* is hard (see [**7**]), and the parameter t is not (in general) a rational function over the given curve. Thus, Hamburger-Noether expansions provide natural parameterizations in positive characteristic.

The HNE can be computed from the Newton diagram of the local equation of χ at P, together with the coefficients of such a local equation (see [**9**]). The process is equivalent to the desingularization of the branch, but several blowing-ups are frequently performed in a single step, saving time in the resolution process.

EXAMPLE 3.3. Let χ be the projective plane curve over $\mathbb{F}_2$ given by

$$F(\mathrm{X},\mathrm{Y},\mathrm{Z}) = \mathrm{X}^{10} + \mathrm{Y}^8\mathrm{Z}^2 + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Y}\mathrm{Z}^9 = 0$$

with only one singular point $P = (0:1:0)$ which is rational over $\mathbb{F}_2$. Take the local equation

$$f(x,z) = x^{10} + x^3z^7 + z^9 + z^2$$

of χ where P is the origin. By applying the Hamburger-Noether algorithm, the symbolic Hamburger-Noether expression of χ at P is

$$\left\{\begin{array}{rcl} Z_{-1} & = & Z_0^5 + Z_0^{19} + Z_0^{22}Z_1 \\ g(Z_1,Z_0) & = & Z_1^9Z_0^{154} + Z_1^8Z_0^{151} + Z_1^8Z_0^{137} + Z_1Z_0^{130} + Z_0^{127} + Z_1^7Z_0^{113} + \\ & + & Z_1^6Z_0^{110} + Z_0^{113} + Z_1^5Z_0^{107} + Z_1^4Z_0^{104} + Z_1^3Z_0^{101} + Z_1^6Z_0^{96} + \\ & + & Z_1^2Z_0^{98} + Z_1Z_0^{95} + Z_1^4Z_0^{90} + Z_0^{92} + Z_1^2Z_0^{84} + Z_1^5Z_0^{79} + \\ & + & Z_1^4Z_0^{76} + Z_0^{78} + Z_1Z_0^{67} + Z_1^4Z_0^{62} + Z_0^{64} + Z_0^{50} + \\ & + & Z_1^3Z_0^{45} + Z_1^2Z_0^{42} + Z_1Z_0^{39} + Z_0^{36} + Z_1^2Z_0^{28} + Z_0^{22} + \\ & + & Z_1Z_0^{18} + Z_0^{15} + Z_1Z_0^{11} + Z_0^8 + Z_1^2 + Z_0 \end{array}\right.$$

(see the details in [**9**]).

REMARK 3.4 (The Brill-Noether algorithm). We remark that, with the aid of the Brill-Noether algorithm, it is possible to compute a basis for a Riemann-Roch space if the underlying curve is plane, singular or not (see [**9**] for further details). This method relies on the adjunction theory, that only works properly for the case of plane curves. Thus, it is not possible to use this algorithm for curves embedded in a higher dimensional space, and hence there is no general method to do this task.

In the same way, by combining the Brill-Noether algorithm for the case $G = mP$ and a triangulation procedure, one gets an effective method to compute the Weierstrass semigroup Γ_P of χ at P up to an element m, together with a function f_l for each non-gap $l \leq m$ (see again [**9**] for further details). This method is implemented in SINGULAR [**13**] with the `brnoeth.lib` library [**15**].

Finally, if P is the only place at infinity of χ, the Weierstrass semigroup can also be computed by a combination of the algorithm of approximate roots (see next paragraph) and the integral basis algorithm (see [**8**]).

3.3. Semigroups at infinity.

Many examples of plane curves that are used in coding theory have the special property of having only one point at infinity. This paragraph is addressed to study this particular situation. Let $\tilde{\chi}$ be a (non-singular and absolutely irreducible) projective algebraic curve defined over a perfect field $\mathbb{F}$. Consider a plane model χ for $\tilde{\chi}$, i.e. a birational morphism

$$\mathbf{n} \ : \ \tilde{\chi} \to \chi \subseteq \mathbb{P}^2.$$

Let $L \subseteq \mathbb{P}^2$ be a projective line defined over $\mathbb{F}$ so that $L \cap \chi = \{P\}$ and $\mathbf{n}^{-1} = \{\overline{P}\}$. Define

$$\tilde{C} = \tilde{\chi} \setminus \{\overline{P}\} \qquad \text{and} \qquad C = \chi \setminus \{P\}.$$

Note that if we take L as the line at infinity, then we have a plane model with only one branch at infinity. The affine equation of C can be given by

$$f(x,y) = y^m + a_1(x)\, y^{m-1} + \ldots + a_m(x) \in \mathbb{F}[x][y].$$

Consider also the following additive subsemigroups of the semigroup of nonnegative integers $\mathbb{N}$:

$$\Gamma_P := \{-\upsilon_{\overline{P}}(f) \mid f \in \mathcal{O}_{\tilde{\chi}}(\tilde{C})\},$$
$$S_{\chi,\infty} := \{-\upsilon_{\overline{P}}(f) \mid f \in \mathcal{O}_{\chi}(C)\},$$

where $\mathcal{O}_{\tilde{\chi}}(\tilde{C})$ and $\mathcal{O}_{\chi}(C)$ denote the respective affine coordinate rings. Then, the following formula holds:

$$\text{card}\,(\Gamma_P \setminus S_{\chi,\infty}) = \dim_{\mathbb{F}}(\mathcal{O}_{\tilde{\chi}}(\tilde{C})/\mathcal{O}_{\chi}(C)),$$

so that both semigroups, the *semigroup at infinity* $S_{\chi,\infty}$, and the *Weierstrass semigroup* Γ_P, coincide if and only if there is no affine singular point in the plane model.

The description of the semigroup $S_{\chi,\infty}$ and the construction of the associated functions (those whose poles span the semigroup) can be done with the so-called Abhyankar-Moh theorem and the algorithm of approximate roots. Semigroups at infinity will be of importance in this paper. So, we are going to give some more information (the classical reference is [**1**]).

First, we introduce the definition of approximate root. Let S be a ring, $g \in S[y]$ a monic polynomial of degree e, and $f \in S[y]$ a monic polynomial of degree m with $e|m$. If we write $m = ed$, then g is called an approximate d-th root of f if $\deg(f - g^d) < m - e = e\,(d-1)$. In other words, $f - g^d$ has a small enough degree, so that one can consider g^d as a good enough approximation of f. The main remark is that if d is a unit in the ring S, then there exists a unique approximate d-th root of f, which will be denoted $\text{app}(d, f)$. In the sequel, we will work with $S = \mathbb{F}[x]$ as the coefficient ring.

Now, consider the affine plane model χ, having only one point at infinity, given by the equation

$$f = f(x, y) = y^m + a_1(x)\, y^{m-1} + \ldots + a_m(x),$$

where m is actually the total degree of the polynomial f, and set $n := \deg_x f$. Assume moreover that the following condition holds:

(*) $\text{char}\,\mathbb{F}$ does not divide either $\deg\,\chi$ or $e_P(\chi)$.

It happens that $m = \deg\,\chi$ and $n = \deg\,\chi - e_P(\chi)$, and the above Condition (*) is equivalent to say that $p = \text{char}\,\mathbb{F}$ does not divide either m or n, that is, $p = \text{char}\,\mathbb{F}$ does not divide both $\deg_x f$ and $\deg_y f$.

We may assume that p does not divide $m = \deg\,\chi$. In fact, if m is a multiple of p but n is not, we choose k not divisible by p such that $nk > m$, and by doing a change of variables of the form $x' = x + y^k$, $y' = y$ we get a new (but isomorphic) affine curve whose degree is not divisible by p.

Next, we will use resultants of polynomials, denoted by Res, and agree to set

$$\deg_x \text{Res}_y(g, h) = -\infty \;\text{ if }\; \text{Res}_y(g, h) = 0$$

for any couple of polynomials $g, h \in \mathbb{F}[x, y]$, and

$$\gcd\,(\delta_0, \delta_1, \ldots, \delta_i) = \gcd\,(\delta_0, \delta_1, \ldots, \delta_j)$$

if $\delta_0, \delta_1, \ldots, \delta_j$ are integers, $j < i$ and $\delta_{j+1} = \delta_{j+2} = \ldots = \delta_i = -\infty$.

Then, the *algorithm of approximate roots* works as follows from an *input* f as above (the case when y divides f is trivial, so we assume the opposite):

Algorithm 3.5.

Input: f

Set $d_0 = 0$, $F_0 = x$, $\delta_0 = d_1 = m$, $F_1 = y$ *and* $\delta_1 = \deg_x \mathrm{Res}_y(f, F_1)$.
For i *from* 2 *do*
$d_i = \gcd(d_{i-1}, \delta_{i-1})$.
If $d_i = d_{i-1}$ *then* $g = i - 2$ *and STOP else*
$F_i = \mathrm{app}(d_i, f)$
$\delta_i = \deg_x \mathrm{Res}_y(f, F_i)$.
Output: g, $(\delta_0, \ldots, \delta_g)$ *and* $(F_0, \ldots, F_g)$.

Note that, since the sequence $\{d_i\}_{i\geq 1}$ is a decreasing one of positive integers, there exists a unique positive integer g such that $d_1 > \ldots > d_{g+1} = d_{g+2}$, and hence the algorithm terminates.

Our first application for this algorithm is the following criterion for a curve with only one (rational) point at infinity to have only one (rational) branch at this point (and to be absolutely irreducible, as a consequence).

THEOREM 3.6 (Criterion for one branch at infinity). *Let* f *be a polynomial giving the equation of a plane model with only one point at infinity as above, and assume that* $\mathrm{char}\,\mathbb{F}$ *does not divide* $m = \deg f$. *Let* g, d_i *and* δ_i *the integers computed by the algorithm of approximate roots. Then, the curve has only one (rational) branch at infinity if and only if* $d_{g+1} = 1$, $\delta_1 d_1 > \delta_2 d_2 > \ldots > \delta_g d_g$ *and* $n_i\delta_i$ *is in the semigroup generated by* $\delta_0, \delta_1, \ldots, \delta_{i-1}$ *for* $1 \leq i \leq g$, *where* $n_i := d_i/d_{i+1}$ *also for* $1 \leq i \leq g$.

A second application of the algorithm of approximate roots is just the computation of $S_{\chi,\infty}$ and the above mentioned associated functions by means of the following

THEOREM 3.7 (Abhyankar-Moh, [**1**]). *Let* χ *be a plane model with only one branch at infinity and assume that* $\mathrm{char}\,\mathbb{F}$ *does not divide* $\deg \chi$. *Then, there exist a positive integer* g *and a sequence of positive integers* $\delta_0, \ldots, \delta_g \in S_{\chi,\infty}$ *generating* $S_{\chi,\infty}$ *such that*

(I): $d_{g+1} = 1$ *and* $n_i > 1$ *for* $2 \leq i \leq g$, *where* $d_i := \gcd(\delta_0, \ldots, \delta_{i-1})$ *for* $1 \leq i \leq g+1$, *and* $n_i := d_i/d_{i+1}$ *for* $1 \leq i \leq g$.
(II): $n_i\delta_i$ *is in the semigroup generated by* $\delta_0, \ldots, \delta_{i-1}$, *for* $1 \leq i \leq g$.
(III): $n_i\delta_i > \delta_{i+1}$ *for* $1 \leq i \leq g-1$.

Moreover, up to a change of affine coordinates, one can assume that $\delta_0 = \deg \chi$.

The above set of numbers $\{\delta_i\}_{0\leq i\leq g}$ is called the *δ-sequence* of the branch at infinity. Later on, we will introduce generalized δ-sequences included in semigroups which are different from the nonnegative integers. Thus, in order to avoid confusion, the above δ-sequences will be called δ-sequences in $\mathbb{N}_{>0}$. Without loss of generality and for our convenience, we will assume along this paper that $\delta_0 > \delta_1$.

EXAMPLE 3.8. Consider the affine plane curve $y^8 + y^2 + x^3 = 0$ defined over $\mathbb{F}_2$, with only one point at infinity $P = (1 : 0 : 0)$. The degree of the curve is multiple of the characteristic, but with the change of variables $x = x + y^3$ and $y = y$, one gets the plane model $f(x, y) = y^9 + y^8 + xy^6 + x^2y^3 + y^2 + x^3$, and the algorithm of approximate roots can be applied to f:

$$F_0 = x\,,\ \delta_0 = d_1 = 9\,,\ F_1 = y,$$

$$\delta_1 = \deg_x \mathrm{Res}_y(f, y) = 3,\ d_2 = \gcd(9, 3) = 3,$$

$$F_2 = \mathrm{app}(3, f) = y^3 + y^2 + y + x + 1,$$
$$\delta_2 = \deg_x \mathrm{Res}_y(f, F_2) = 8 \text{ and } d_3 = \gcd(9, 3, 8) = 1.$$

Thus $g = 2$ and $S_{\chi,\infty} = \langle 9, 3, 8\rangle$. As a consequence, there is only one branch at infinity, since properties **(I)**, **(II)** and **(III)** from the Abhyankar-Moh Theorem are satisfied.

3.4. Dual graph and δ-sequences.

As in the previous section, fix homogeneous coordinates $(X : Y : Z)$ on $\mathbb{P}^2$. Here, $Z = 0$ will be the line L at infinity and $P = (1 : 0 : 0)$. Set (x, y) coordinates in the chart $Z \neq 0$, and $(u = y/x, v = 1/x)$ coordinates around the point at infinity. Consider a projective plane model χ with only one branch at infinity. As we have said, the curve χ is defined by a monic polynomial $f(x, y)$ in the indeterminate y with coefficients in $\mathbb{F}[x]$.

Consider the infinite sequence of morphisms

$$\cdots \to X_{i+1} \to X_i \to \cdots \to X_1 \to X_0 := \mathbb{P}^2, \tag{3.1}$$

where $X_1 \to X_0$ is the blowing-up at $p_0 := P$ (the point at infinity) and, for each $i \geq 1$, $X_{i+1} \to X_i$ denotes the blowing-up of X_i at the unique point p_i which lies on both the strict transform of χ and the exceptional divisor created by the preceding blowing-up. Notice that p_i is defined over $\mathbb{F}$, since the branch of χ at P is rational. It is well-known that there exists a minimum integer n such that, if $\pi : X_n \to \mathbb{P}^2$ denotes the composition of the first n blowing-ups, then the germ of the strict transform of χ by π at p_n becomes regular and transversal to the exceptional divisor. This gives the (minimal embedded) resolution of the germ of χ at P. The essential information, that is, the (topological) equisingularity class of the germ, can be given either in terms of its sequence of *Newton polygons* [**6**, III.4], or by means of its *dual graph* (see [**14**] within a more general setting, or [**17**] for a slightly different version). This information basically provides the number and the position of the blowing-up centers of π, which can be placed either on a free point (not an intersection of two exceptional divisors) or on a satellite point. In this last case, it is also important to know whether, or not, the blowing-up center belongs to the last but one created exceptional divisor. Thinking of blowing-up centers, we will say that a center p_i is proximate to other p_j whenever p_i is on any strict transform of the divisor created after the blowing-up at p_j.

After a suitable choice $\{u', v'\}$ of local coordinates of the local ring $\mathcal{O}_{\chi,P}$, it happens that the HNE of χ at P has the form

$$\begin{array}{rcl}
v' & = & a_{01}u' + a_{02}u'^2 + \cdots + a_{0h_0}u'^{h_0} + u'^{h_0}w_1 \\
u' & = & w_1^{h_1}w_2 \\
\vdots & & \vdots \\
w_{s_1-2} & = & w_{s_1-1}^{h_{s_1-1}}w_{s_1} \\
w_{s_1-1} & = & a_{s_1k_1}w_{s_1}^{k_1} + \cdots + a_{s_1h_{s_1}}w_{s_1}^{h_{s_1}} + w_{s_1}^{h_{s_1}}w_{s_1+1} \\
\vdots & & \vdots \\
w_{s_g-1} & = & a_{s_gk_g}w_{s_g}^{k_g} + \cdots,
\end{array}$$

where the family $\{s_i\}_{i=0}^{g}$, $s_0 = 0$, of nonnegative integers, is the set of indices corresponding to the free rows of the expression, that is, those rows that express the blowing-ups at free points (they are those that have some nonzero $a_{jl} \in \mathbb{F}$) and

one of the main goals (of the HNE) is that it gives local coordinates of the transform of the germ of χ at P in each center of blowing-up. The local coordinates after $\{u', v'\}$ are $\{u', (v'/u') - a_{01}\}$, and so on.

The *dual graph* Γ associated to the above germ of curve is a tree such that each vertex represents an exceptional divisor of the sequence π, and two vertices are connected by an edge whenever the corresponding divisors intersect. Additionally, we label each vertex with the minimal number of blowing-ups needed to create its corresponding exceptional divisor. The dual graph can be done by gluing up, by their vertices st_i, subgraphs Γ_i $(1 \leq i \leq g)$ corresponding to blocks of data $B_i = \{h_{s_{i-1}} - k_{i-1} + 1, h_{s_{i-1}+1}, h_{s_{i-1}+2}, \ldots, h_{s_i-1}, k_i\}$ (with $k_0 = 0$), which represent the divisors involved in the part of the HNE of the germ between two free rows. In other words, Γ_i contains the divisors corresponding to $h_{s_{i-1}} - k_{i-1} + 1$ free points, and to sets of h_j $(s_{i-1} + 1 \leq j \leq s_i - 1)$ and k_i proximate points to satellite ones. Each subgraph Γ_i starts in the vertex st_{i-1} and ends in st_i containing, among others, the vertex ρ_i. So, the dual graph has the shape depicted in Figure 1.

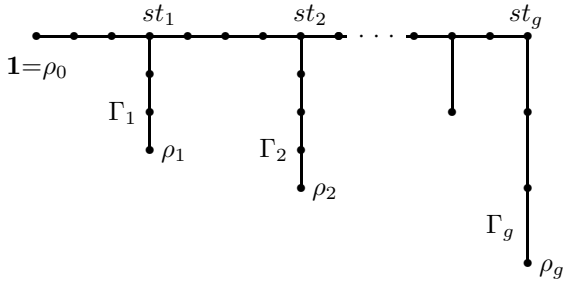

FIGURE 1. The dual graph of a germ of curve

Set E_{s_i} $(1 \leq i \leq g)$ the exceptional divisor obtained after blowing-up the last free point corresponding to the subgraph Γ_i. It corresponds to the vertex ρ_i in the dual graph. An irreducible germ of curve ψ at P, is said to *have maximal contact of genus* i with the germ of χ at P, if the strict transform of ψ in the (corresponding germ of the) surface containing E_{s_i} is not singular, and meets transversely E_{s_i} and no other exceptional curves.

The sequence of Newton polygons and the dual graph of the germ of a curve χ with only one branch at infinity can be recovered from a δ-sequence in $\mathbb{N}_{>0}$, $\Delta = \{\delta_0, \delta_1, \ldots, \delta_s\}$, associated with it. We assume that the Newton polygons are given by segments P_i $(0 \leq i \leq g-1)$ joining the points $(0, e_i)$ and $(m_i, 0)$, $e_i, m_i \in \mathbb{N}_{>0}$. If $\delta_0 - \delta_1$ does not divide δ_0 then $s = g$ and

$$e_0 = \delta_0 - \delta_1, \quad e_i = d_{i+1} \tag{3.2}$$

$$m_0 = \delta_0, \quad m_i = n_i\delta_i - \delta_{i+1}$$

for $1 \leq i \leq s-1$. Otherwise, $s = g+1$ and

$$e_0 = d_2 = \delta_0 - \delta_1, \quad e_i = d_{i+2}$$

$$m_0 = \delta_0 + n_1\delta_1 - \delta_2, \quad m_i = n_{i+1}\delta_{i+1} - \delta_{i+2}$$

for $1 \leq i \leq s-2$. These formulae can be deduced from results in [**6**, IV.3].

Concerning the dual graph or the blocks in the HNE of the germ, one gets

$$\frac{m_{j-1}}{e_{j-1}} + k_{j-1} = h_{s_{j-1}} + \cfrac{1}{h_{s_{j-1}+1} + \ddots + \cfrac{1}{h_{s_j-1} + \cfrac{1}{k_j}}}, \tag{3.3}$$

for $j = 1, 2, \ldots, g$, where $s_0 = k_0 = 0$ (see [**6**, III.4]).

Next, we define a useful concept for us.

Definition 3.9. A sequence of polynomials in $\mathbb{F}[x, y]$

$$q_0^*(x, y), q_1^*(x, y), \ldots, q_g^*(x, y)$$

is a *family of approximates* for the above given curve χ given by $f(x, y)$ if the following conditions hold:

(1) $q_0^*(x, y) = x$, $q_1^*(x, y) = y$, $\delta_0^* := -v_{\chi,p}(q_0^*) = \deg_y(f)$ and $\delta_1^* := -v_{\chi,p}(q_1^*)$.
(2) $q_i^*(x, y)$ $(1 < i \leq g)$ has degree δ_0^*/d_i and it is monic in the indeterminate y, where $d_i = \gcd(\delta_0^*, \delta_1^*, \ldots, \delta_{i-1}^*)$, being $\delta_i^* := -v_{\chi,p}(q_i^*)$.
(3) The germ of curve at P given by the local expression of $q_i^*(x, y)$ $(1 < i \leq g)$ in the coordinates (u, v) has maximal contact with the germ of χ at P, of genus i when $\delta_0^* - \delta_1^*$ does not divide δ_0^*, and of genus $i - 1$ otherwise.

By an abuse of notation, when we set $-v_{\chi,p}(q_i^*)$, q_i^* stands for the element in the fraction field of $\mathcal{O}_{\chi,p}$ that it defines. On the other hand, under the conditions of Abhyankar-Moh Theorem, that is, the characteristic of $\mathbb{F}$ does not divide the degree of the curve χ, approximate roots are a family of approximates for χ.

Now, let $\Delta = \{\delta_i\}_{i=0}^g$ be a δ-sequence in $\mathbb{N}_{>0}$, and set S_Δ the semigroup in $\mathbb{N}_{>0}$ that it generates. It is well-known the existence of a unique expression of the form

$$n_i\delta_i = \sum_{j=0}^{i-1} a_{ij}\delta_j, \tag{3.4}$$

where $a_{i0} \geq 0$ and $0 \leq a_{ij} < n_j$, for $1 \leq j \leq i - 1$. Set $q_0 := x$ $q_1 := y$ and, for $1 \leq i \leq g$,

$$q_{i+1} := q_i^{n_i} - t_i \prod_{j=0}^{i-1} q_j^{a_{ij}}, \tag{3.5}$$

where $t_i \in \mathbb{F} \setminus \{0\}$ are arbitrary. Although the results in this paper concerning these polynomials hold for any family of parameters $\{0 \neq t_i\}_{i=1}^g$, we fix for convenience $t_i = 1$ for all i. Then, by applying the algorithms relative to Newton polygons of a germ of curve given by Campillo in [**6**, III.4] to the germ given by q_{g+1}, it holds the following result (see [**40**, Section 4] for more details), where we notice that there is no restriction for the characteristic of the field $\mathbb{F}$.

Proposition 3.10. *The equality $q_{g+1} = 0$ defines a plane curve χ with only one branch at infinity such that $S_{\chi,\infty} = S_\Delta$, and the set $\{q_i\}_{i=0}^g$ is a family of approximates for χ such that $-v_{\chi,p}(q_i) = \delta_i$, for all $i = 0, 1, \ldots, g$.*

4. Plane valuations

We start by recalling the concept of *valuation*.

DEFINITION 4.1. A *valuation* of a field K is a mapping

$$\nu : K^*(:= K \setminus \{0\}) \to G,$$

where G is a totally ordered group, such that it satisfies

- $\nu(f+g) \geq \min\{\nu(f), \nu(g)\}$ and
- $\nu(fg) = \nu(f) + \nu(g)$,

f, g being elements in K^*. The subring of K, $R_\nu := \{f \in K^* | \nu(f) \geq 0\} \cup \{0\}$, is called the *valuation ring* of ν. R_ν is a local ring whose maximal ideal is $m_\nu := \{f \in K^* | \nu(f) > 0\} \cup \{0\}$.

Given a local regular domain (R, m), we will say that a valuation ν of the quotient field of R *is centered* at R if $R \subseteq R_\nu$ and $R \cap m_\nu = m$. The subset of G given by $S_\nu := \nu(R \setminus \{0\})$ is called the *semigroup* of the valuation ν (relative to R). We will only consider *plane valuations*, that is, valuations of the quotient field of a local regular domain (R, m) of dimension two which are centered at R. Assume for a while that the field $\mathbb{F} := R/m$ is algebraically closed. In this case, a plane valuation is the algebraic version of a simple sequence of blowing-ups at closed points, starting with the blowing-up at m (see [**46**] for the details). In fact, attached to a plane valuation ν, there is a unique sequence of point blowing-ups

$$\cdots \longrightarrow X_{N+1} \stackrel{\pi_{N+1}}{\longrightarrow} X_N \longrightarrow \cdots \longrightarrow X_1 \stackrel{\pi_1}{\longrightarrow} X_0 = \text{Spec } R, \tag{4.1}$$

where π_1 is the blowing-up of X_0 centered at its closed point p_0 and, for each $i \geq 1$, π_{i+1} is the blowing-up of X_i at the unique closed point p_i of the exceptional divisor E_i (obtained after the blowing-up π_i) satisfying that ν is centered at the local ring $\mathcal{O}_{X_i,p_i}$ $(:= R_i)$. Conversely, each sequence as in (4.1) provides a unique plane valuation. We will denote by $\mathcal{C}_\nu = \{p_i\}_{i\geq 0}$ the sequence (finite or infinite) of closed points involved in the blowing-ups of (4.1). When $\mathcal{C}_\nu$ is finite, ν is called the *divisorial valuation* corresponding to the last exceptional divisor obtained in (4.1); this is so since if π_{N+1} is the last blowing-up in the sequence (4.1) given by ν, then ν is the m_N-adic valuation, m_N being the maximal ideal of the ring R_N. Otherwise (when $\mathcal{C}_\nu$ is not finite), the plane valuation ν can be regarded as the limit of the sequence of divisorial valuations $\{\nu_i\}_{i\geq 0}$, ν_i being the divisorial valuation corresponding to the divisor E_i.

With the above notation, let p_i and p_j be points in $\mathcal{C}_\nu = \{p_i\}_{i\geq 0}$. We will say that p_i *is proximate* to p_j (and it will be denoted by $p_i \to p_j$) if $i > j$ and p_i belongs to the strict transform (by the corresponding sequence of blowing-ups given in (4.1)) of E_{j+1}. This binary relation among the points of $\mathcal{C}_\nu$ will be called *proximity relation* and it induces a binary relation $\mathcal{P}_\nu$ in the set of natural numbers ($i \to j$ if $p_i \to p_j$). Also, the point p_i is said to be *satellite* if there exists $j < i-1$ such that $p_i \to p_j$ (in other words, if p_i belongs to the intersection of the strict transforms of two exceptional divisors); otherwise, p_i is said to be a *free* point. Notice that these definitions extend those we mentioned for plane curves in the previous section. It is worth pointing out that the semigroup S_ν of a plane valuation depends only on the relation $\mathcal{P}_\nu$. According with this relation, a plane valuation ν (with associated sequence $\mathcal{C}_\nu = \{p_i\}_{i\geq 0}$) belongs to one of the following five types (see [**46**] and [**19**]):

– **TYPE A** (or divisorial): if $\mathcal{C}_\nu$ is finite.
– **TYPE B**: if there exists $i_0 \in \mathbb{N}_{>0}$ such that the point p_i is free for all $i > i_0$.
– **TYPE C**: if there exists $i_0 \in \mathbb{N}_{>0}$ such that $p_i \to p_{i_0}$ for all $i > i_0$.
– **TYPE D**: if there exists $i_0 \in \mathbb{N}_{>0}$ such that p_i is a satellite point for all $i > i_0$ but ν is not a type C valuation. This means that the sequence (4.1) ends with infinitely many blowing-ups at satellite points, but they are not ever centered at some point of the strict transforms of the same divisor.
– **TYPE E**: if the sequence $\mathcal{C}_\nu$ alternates indefinitely blocks of free and satellite points.

As in the case of germs of curves, a plane valuation ν admits also a Hamburger-Noether expansion (HNE), which for a regular system of parameters of the ring R, $\{u, v\}$, has the shape showed in Figure 2.

$$
\begin{array}{rcl}
v & = & a_{01}u + a_{02}u^2 + \cdots + a_{0h_0}u^{h_0} + u^{h_0}w_1 \\
u & = & w_1^{h_1}w_2 \\
\vdots & & \vdots \\
w_{s_1-2} & = & w_{s_1-1}^{h_{s_1-1}}w_{s_1} \\
w_{s_1-1} & = & a_{s_1k_1}w_{s_1}^{k_1} + \cdots + a_{s_1h_{s_1}}w_{s_1}^{h_{s_1}} + w_{s_1}^{h_{s_1}}w_{s_1+1} \\
\vdots & & \vdots \\
w_{s_g-1} & = & a_{s_gk_g}w_{s_g}^{k_g} + \cdots + a_{s_gh_{s_g}}w_{s_g}^{h_{s_g}} + w_{s_g}^{h_{s_g}}w_{s_g+1} \\
\vdots & & \vdots \\
w_{i-1} & = & w_i^{h_i}w_{i+1} \\
\vdots & & \vdots \\
(w_{z-1} & = & w_z^{\infty}).
\end{array}
\tag{3}
$$

FIGURE 2. HNE of a plane valuation

When ν is of type A, the last row has the form

$$w_{s_g-1} = a_{s_gk_g}w_{s_g}^{k_g} + \cdots + a_{s_gh_{s_g}}w_{s_g}^{h_{s_g}} + w_{s_g}^{h_{s_g}}w_{s_g+1},$$

here $w_{s_g+1} \in R_\nu$ and $\nu(w_{s_g+1}) = 0$.

In case ν is of type B, its corresponding HNE has a last equality associated with an infinite sum like this

$$w_{s_g-1} = \sum_{j=k_g}^{\infty} a_{s_gj}w_{s_g}^{j}.$$

Notice that, in this case, the shape of the HNE is the same as that for a germ of a curve around the point defined by m.

If ν is of type C, its HNE has a last free row like this

$$w_{s_g-1} = a_{s_gk_g}w_{s_g}^{k_g} + \cdots + a_{s_gh_{s_g}}w_{s_g}^{h_{s_g}} + w_{s_g}^{h_{s_g}}w_{s_g+1}$$

and, after, finitely many non-free rows with the shape

$$\begin{array}{ccc} w_{s_g} & = & w_{s_g+1}^{h_{s_g+1}} w_{s_g+2} \\ \vdots & & \vdots \\ w_{z-1} & = & w_z^{\infty}. \end{array}$$

With respect to the case ν of type D, the HNE has a last free row like this

$$w_{s_g-1} = a_{s_g k_g} w_{s_g}^{k_g} + \cdots + a_{s_g h_{s_g}} w_{s_g}^{h_{s_g}} + w_{s_g}^{h_{s_g}} w_{s_g+1}$$

followed by infinitely many rows as follows

$$w_{i-1} = w_i^{h_i} w_{i+1},$$

$(i > s_g)$. Clearly, $g < \infty$ and $z = \infty$.

Finally, the HNE of a valuation of type E satisfies that there exist infinitely many ordered sets of equalities with the shape

$$\begin{array}{ccc} w_{s_i-1} & = & a_{s_i k_i} w_{s_i}^{k_i} + \cdots + a_{s_i h_{s_i}} w_{s_i}^{h_{s_i}} + w_{s_i}^{h_{s_i}} w_{s_i+1} \\ \vdots & & \vdots \\ w_{s_{i+1}-2} & = & w_{s_{i+1}-1}^{h_{s_{i+1}-1}} w_{s_{i+1}}. \end{array}$$

Here $g = z = \infty$.

4.1. Plane valuations at infinity.

Next, we introduce a particular type of plane valuations: *plane valuations at infinity*. We do not actually need that the ground field is algebraically closed. This is because the procedure and concepts above explained will work similarly, due to the special nature of the valuations that we will consider, and the centers of the associated blowing-ups will be defined over $\mathbb{F}$. We recall that the field $\mathbb{F}$ has to be a perfect field.

We start by stating the concept of general element of a divisorial valuation.

Definition 4.2. Let ν be a divisorial valuation. An element f in the maximal ideal of R is said to be a *general element of* ν if the germ of curve given by f is analytically irreducible, its strict transform in the last variety X_{N+1} obtained by the sequence (4.1) attached to ν is smooth, and meets E_{N+1} transversely at a non-singular point of the exceptional divisor of the sequence (4.1).

Remark 4.3. General elements are useful to compute plane divisorial valuations. Indeed, if $f \in R$, then

$$\nu(f) = \min \{(f, g) | g \text{ is a general element of } \nu\},$$

where (f, g) stands for the intersection multiplicity of the germs of curve given by f and g.

Let $P := p_0$ be a closed point of $\mathbb{P}^2$ on the line of infinity and assume, from now on, that $R = \mathcal{O}_{\mathbb{P}^2, P}$ and K is the quotient field of R.

Definition 4.4. A *plane divisorial valuation at infinity* is a plane divisorial valuation of K centered at R that admits, as a general element, an element in R providing the germ at P of some curve with only one branch at infinity (P being its point at infinity).

DEFINITION 4.5. A plane valuation ν of K centered at R is said to be *at infinity* whenever it is a limit of plane divisorial valuations at infinity. More explicitly, ν will be at infinity if there exists a sequence of divisorial valuations at infinity $\{\nu_i\}_{i=1}^{\infty}$ such that $\mathcal{C}_{\nu_i} \subseteq \mathcal{C}_{\nu_{i+1}}$ for all $i \in \mathbb{N}_{>0}$, and $\mathcal{C}_{\nu} = \bigcup_{i\geq 1} \mathcal{C}_{\nu_i}$.

There exist plane valuations at infinity of all types above described. The concept of valuation at infinity of type A is equivalent to the one of plane divisorial valuation at infinity; such a valuation is obtained whenever the sequence $\{\nu_i\}_{i=1}^{\infty}$ given in the above definition satisfies that $\nu_i = \nu_{i+1}$ for every index larger than or equal to a fixed index $i_0 \in \mathbb{N}_{>0}$ (in fact, it can be taken constant for all i). It is obtained a valuation at infinity of type B if there exists $i_0 \in \mathbb{N}_{>0}$ such that $\mathcal{C}_{\nu_{i_0}}$ is the set of centers of the blowing-ups corresponding with the minimal embedded resolution of the germ at p of a curve having only one branch at infinity and, for all $i \geq i_0$, the strict transform of this germ meets transversely the exceptional divisor associated with ν_i. Explicit constructions of plane valuations at infinity of types C, D, and E are described in [**21**].

The concept of approximate can be extended to valuations at infinity as we show in the following definition.

DEFINITION 4.6. Let ν be a plane valuation at infinity. A sequence of polynomials $P = \{q_i(x,y)\}_{i\geq 0}$ in $\mathbb{F}[x,y]$ is a *family of approximates* for ν whenever each plane curve C with only one branch at infinity providing a general element of some of the plane divisorial valuations at infinity converging to ν admits some subset of P as a family of approximates, and P is minimal with this property.

4.2. Generalized δ-sequences.

For a starting point, we introduce the concept of semigroup at infinity of a plane valuation at infinity. Recall that $\{x, y\}$ are coordinates in the chart $Z \neq 0$.

DEFINITION 4.7. Let $\nu : K^* \to G$ be a plane valuation at infinity. The *semigroup at infinity* of ν is defined to be the following sub-semigroup of G:

$$S_{\nu,\infty} := \{-\nu(f) \mid f \in k[x,y] \setminus \{0\}\}.$$

A *normalized δ-sequence in* $\mathbb{N}_{>0}$ will be an ordered finite set of rational numbers $\overline{\Delta} = \{\overline{\delta}_0, \overline{\delta}_1, \ldots, \overline{\delta}_g\}$ such that there is a δ-sequence in $\mathbb{N}_{>0}$, $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g\}$, satisfying $\overline{\delta}_i = \delta_i/\delta_1$ for $0 \leq i \leq g$. As we have said, we will consider δ-sequences for the different types of plane valuations at infinity:

DEFINITION 4.8. A *δ-sequence of* **TYPE A** (respectively, **B**, **C**, **D**, **E**) is a sequence $\Delta = \{\delta_0, \delta_1, \ldots, \delta_i, \ldots\}$ of elements in $\mathbb{Z}$ (respectively, $\mathbb{Z}^2$, $\mathbb{Z}^2$, $\mathbb{R}$, $\mathbb{Q}$) such that

- **TYPE A:** $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g, \delta_{g+1}\} \subset \mathbb{Z}$ is finite, the elements of the set $\{\delta_0, \ldots, \delta_g\}$ satisfy the conditions (I), (II) and (III) of the Theorem 3.7 and $\delta_{g+1} \leq n_g \delta_g$.
- **TYPE B:** There exists a δ-sequence in $\mathbb{N}_{>0}$, $\Delta^* = \{\delta_0^*, \delta_1^*, \ldots, \delta_g^*\}$, such that $\Delta = \{(0, \delta_0^*), (0, \delta_1^*), \ldots, (0, \delta_g^*), (-1, (\delta_0^*)^2)\}$.
- **TYPE C:** $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g\} \subset \mathbb{Z}^2$ is finite, $g \geq 2$ (respectively, ≥ 3) and there exists a δ-sequence in $\mathbb{N}_{>0}$, $\Delta^* = \{\delta_0^*, \delta_1^*, \ldots, \delta_g^*\}$, such that $\delta_0^* - \delta_1^*$ does not divide (respectively, divides) δ_0^* and

$$\delta_i = \frac{\delta_i^*}{Aa_t + B}(A, B) \quad (0 \leq i \leq g-1) \quad \text{and}$$

$$\delta_g = \frac{\delta_g^* + A'a_t + B'}{Aa_t + B}(A,B) - (A',B'),$$

where $\langle a_1; a_2, \ldots, a_t\rangle$, $a_t \geq 2$, is the continued fraction expansion of the quotient m_{g-1}/e_{g-1} (respectively, m_{g-2}/e_{g-2}) given by Δ^* and, considering the finite recurrence relation $\underline{y}_i = a_{t-i}\underline{y}_{i-1} + \underline{y}_{i-2}$, $\underline{y}_{-1} = (0,1)$, $\underline{y}_0 = (1,0)$, then $(A,B) := \underline{y}_{t-2}$ and $(A',B') := \underline{y}_{t-3}$. We complete this definition by adding that $\Delta = \{\delta_0, \delta_1\}$ (respectively, $\Delta = \{\delta_0, \delta_1, \delta_2\}$) is a δ-sequence of type C whenever $\delta_0 = \underline{y}_{t-1}$ and $\delta_0 - \delta_1 = \underline{y}_{t-2}$ (respectively, $\delta_0 = j\underline{y}_{t-2}$, $\delta_0 - \delta_1 = \underline{y}_{t-2}$ and $\delta_0 + n_1\delta_1 - \delta_2 = \underline{y}_{t-1}$) for the above recurrence attached to a δ-sequence in $\mathbb{N}_{>0}$, $\Delta^* = \{\delta_0^*, \delta_1^*\}$ (respectively, $\Delta^* = \{\delta_0^*, \delta_1^*, \delta_2^*\}$, such that $j := \delta_0^*/(\delta_0^* - \delta_1^*) \in \mathbb{N}_{\geq 0}$ and $n_1 := \delta_0^*/\gcd(\delta_0^*, \delta_1^*)$).

TYPE D: $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g\} \subset \mathbb{R}$ is finite, $g \geq 2$, δ_i is a positive rational number for $0 \leq i \leq g-1$, δ_g is non-rational, and there exists a sequence

$$\left\{\overline{\Delta}_j = \{\delta_0^j, \delta_1^j, \ldots, \delta_g^j\}\right\}_{j\geq 1}$$

of normalized δ-sequences in $\mathbb{N}_{>0}$ such that $\delta_i^j = \delta_i$ for $0 \leq i \leq g-1$ and any j and $\delta_g = \lim_{j\to\infty} \delta_g^j$. We complete this definition by adding that $\Delta = \{\tau, 1\}$, $\tau > 1$ being a non-rational number, is also a δ-sequence of type D.

TYPE E: $\Delta = \{\delta_0, \delta_1, \ldots, \delta_i, \ldots\} \subset \mathbb{Q}$ is infinite and any ordered subset $\Delta_j = \{\delta_0, \delta_1, \ldots, \delta_j\}$ is a normalized δ-sequence in $\mathbb{N}_{>0}$.

Example 4.9. We show some examples of δ-sequences of types from A to E: $\{18, 12, 33, 4, -5\}$ is of type A, $\{(0,18), (0,12), (0,33), (0,4), (-1,18^2)\}$ of type B, $\{(6,6), (4,4), (11,11), (1,2)\}$ of type C, $\{3/2, 1, 33/12, 4/12, (75+32\sqrt{2})/12(7+3\sqrt{2})\}$ of type D and the first terms of a δ-sequence of type E are

$$\{3/2, 1, 33/12, 1/3, 15/4, \ldots\}.$$

Along the rest of this paper, for a δ-sequence Δ of any type (from A to E), S_Δ will denote the semigroup spanned by Δ. *During a while, δ-sequence will mean δ-sequence of some of the above types.* Afterwards, we will restrict this concept to δ-sequences of types from C to E.

By using the formulae after (3.2) and from the finite sequence of positive integers satisfying (I), (II) and (III) attached to a curve χ as in Theorem 3.7 by Abhyankar and Moh, one can recover the proximity relation, dual graph and structure of the HNE attached to the minimal embedded resolution of the singularity at infinity of χ. Indeed, to do it, one essentially needs to consider the continued fractions of quotients of the type m_l/e_l, m_l and e_l being the values defined below (3.2) (see [**21**]).

The concept of δ-sequence in Definition 4.8 is defined in such a way that the mentioned equalities happen for any type of valuation, although we need, for that purpose, to use an extended version of the Euclidian Algorithm that can also involve values either in $\mathbb{Z}^2$ or in $\mathbb{R}$ [**23**]. Next example, and for the δ-sequences given in Example 4.9, shows the attached pairs, (m_l, e_l), and the corresponding elements in the extended Euclidian algorithm. They provide the dual and proximity graphs (and the structure of the HNE) of the attached valuation at infinity. This valuation

has the property that its semigroup at infinity is spanned by the mentioned δ-sequence.

EXAMPLE 4.10. Consider the examples given in Example 4.9. All of them satisfy $\delta_0 - \delta_1$ divides δ_0. So, we have to use the sequent formulae:

$$d_i = \gcd(\delta_0, \ldots, \delta_{i-1}) \quad n_i = d_i/d_{i+1}$$
$$e_0 = \delta_0 - \delta_1, \quad e_i = d_{i+2}$$
$$m_0 = \delta_0 + n_1\delta_1 - \delta_2, \quad m_i = n_{i+1}\delta_{i+1} - \delta_{i+2}.$$

The type A δ-sequence is $\{18, 12, 33, 4, -5\}$ and we get the pairs

$$(m_l, e_l) : (21, 6), (62, 3), (2, 1)$$

with continued fractions: $\langle 3; 2\rangle$, $\langle 20; 1, 2\rangle$ and $\langle 2\rangle$. The equality $n_g\delta_g - \delta_{g+1} = 17$ indicates that the last 17 points of $\mathcal{C}_\nu$ are free.

Now consider the type B δ-sequence, then (m_l, e_l): $((0, 21), (0, 6)), ((0, 63), (0, 3))$ and $((1, 0), (0, 1))$ with continued fractions: $\langle 3; 2\rangle$, $\langle 20; 1, 2\rangle$ and $\langle\infty\rangle$; this last one corresponds to blowing-up at infinitely many free points.

With respect to the type C δ-sequence, $\{(6, 6), (4, 4), (11, 11), (1, 2)\}$, it holds (m_l, e_l): $((7, 7), (2, 2))$ and $((21, 20), (1, 1))$. The continued fractions are $\langle 3; 2\rangle$ and $\langle 20; 1, \infty\rangle$ and the generalized Euclidian Algorithm provides $(21, 20) = \mathbf{20}(1, 1) + (1, 0)$; $(1, 1) = \mathbf{1}(1, 0) + (0, 1)$ and $(1, 0) = \infty(0, 1)$.

$\{3/2, 1, 33/12, 4/12, (75 + 32\sqrt{2})/12(7 + 3\sqrt{2})\}$ is our δ-sequence of type D and the pairs (m_l, e_l) are $(21/12, 1/2)$, $(62/12, 3/12)$ and $((9+4\sqrt{2})/12(7+3\sqrt{2}), 1/12)$, being the continued fractions $\langle 3; 2\rangle$, $\langle 20; 1, 2\rangle$ and $\langle 1; 3, 2, \sqrt{2}\rangle$.

Finally, we consider the Type E δ-sequence and then the pairs (m_l, e_l) reproduce the behavior of the one of type A.

Valuations at infinity satisfy an Abhyankar-Moh type theorem as one can see in [**23**]. However, the interesting result for us is the converse of that theorem which also happens and it will be essential for our purposes:

THEOREM 4.11. (See [**21**, Theorem 4.9] for type C, D and E valuations and [**23**, Remark 4.4] for the remaining ones). *Let Δ be a δ-sequence and set $\mathbb{F}[x, y]$ the polynomial ring in two indeterminates over an arbitrary perfect field $\mathbb{F}$. Then, there exists a plane valuation at infinity ν over the field $\mathbb{F}(x, y)$ such that the semigroup at infinity $S_{\nu,\infty}$ is spanned by Δ.*

5. Codes given by plane valuations at infinity

We devote this section to study a large family of evaluation codes associated with certain weights functions given by either only one or finitely many plane valuations at infinity.

5.1. Codes given by one valuation.

We have explained that the weight functions are suitable objects to get (primal and dual) evaluation codes that can be decoded up to half of their designed distances. From this point of view, the semigroup of values is the most important element of the weight functions. Notwithstanding, and although one can provide some weight functions, there is no method to define large families of them and no classification is available. Valuations are very close objects to weight functions and, in the plane case, they have been classified [**46, 19**]. The following result, proved in [**20**, Proposition 2.2], shows how to obtain weight functions from valuations.

PROPOSITION 5.1. *Let $\mathfrak{K}$ be the quotient field of a regular local domain $\mathfrak{R}$ with maximal $\mathfrak{m}$. Let $\nu : \mathfrak{K}^* \to \mathfrak{G}$ be a valuation of $\mathfrak{K}$ which is centered at $\mathfrak{R}$. Assume that the canonical embedding of the field $\mathfrak{k} := \mathfrak{R}/\mathfrak{m}$ into the field $\mathfrak{R}_\nu/\mathfrak{m}_\nu$ is an isomorphism.*

Set $w : \mathfrak{K}^* \to \mathfrak{G}$ the mapping given by $w(f) = -\nu(f)$, $f \in \mathfrak{K}^*$. If $\mathfrak{A} \subseteq \mathfrak{K}^*$ is a $\mathfrak{k}$-algebra such that $w(\mathfrak{A})$ is a cancellative, commutative, free of torsion, well-ordered semigroup with zero, Γ, where the associated ordering is admissible, then $w : \mathfrak{A} \longrightarrow w(\mathfrak{A}) \cup \{-\infty\}$, $w(0) = -\infty$, is a weight function.

We are interested in the case $\dim R = 2$ because, as we have said, here we know a classification of valuations in five types. $R/m \cong R_\nu/m_\nu$ happens for any plane valuation except for those of type A. Thus type A valuations are not interesting for coding purposes. However they are very useful since the remaining types of valuations can be regarded as limits of type A valuations. We are neither interested in type B valuations, the reason comes from the fact that the semigroups provided by their attached weight type functions are not well-ordered. We have included its study by completion reasons. From now on, unless otherwise stated, *δ-sequence will mean δ-sequence of type C, D or E.*

The following two results which can be found in [**21**] show how to get weight functions over the polynomial ring $\mathbb{F}_q[x, y]$ only with a δ-sequence and the scope of the result because these functions satisfy a Matsumoto type result.

THEOREM 5.2. *Let $\Delta = \{\delta_0, \ldots, \delta_r\}, r \leq \infty$, be a δ-sequence. Set $\mathbb{F}_q[x, y]$ the polynomial ring in two indeterminates over an arbitrary finite field $\mathbb{F}_q$. Then:*

a)There exists a weight function $w_\Delta : \mathbb{F}_q[x, y] \longrightarrow S_\Delta \cup \{\infty\}$.

b) The map $-w_\Delta : \mathbb{F}_q(x, y) \to G(S_\Delta)$, $G(S_\Delta)$ being the group generated by S_Δ, is a plane valuation at infinity.

c) Let $\{q_i\}_{i=0}^r$ be a family of approximates for the valuation $-w_\Delta$. Then, for any $\alpha \in S_\Delta$, the vector spaces

$$O_\alpha := \{p \in \mathbb{F}_q[x, y] \mid w_\Delta(p) \leq \alpha\}$$

are spanned by the set of polynomials $\prod_{i=0}^m q_i^{\gamma_i}$ such that $\sum_{i=0}^m \gamma_i \delta_i := \beta$ runs over the unique expression of the values $\beta \in S_\Delta$ satisfying $\beta \leq \alpha$, $\gamma_0 \geq 0$, $\gamma_r \geq 0$ if it exists and $0 \leq \gamma_i < n_i$, whenever $1 \leq i < m$.

Recall that n_i is easily computed from Δ.

We also recall that Matsumoto in [**38**] proved that order domains given by weight functions on $\mathbb{Z}$ are affine coordinate rings of algebraic curves with exactly one branch at infinity. Now, we state a close result, proved in [**21**], involving our weight functions.

PROPOSITION 5.3. *Let $w : \mathbb{F}_q[x, y] \to S$ be a weight function on a semigroup S such that $S = S_\Delta$ for some δ-sequence Δ. Then, there exists a plane valuation at infinity $\nu : \mathbb{F}_q(x, y) \to G$ such that $-\nu$ and w coincide on the ring $\mathbb{F}_q[x, y]$.*

Next, we summarize the procedure to get (and some properties from) evaluation codes given by plane valuations. Firstly, one has to construct a δ-sequence of type C, D or E. Notice that those of type E have infinitely many elements but, for a concrete family of codes, we only need finitely many of them. For that construction, one needs a large enough δ-sequence in $\mathbb{N}_{>0}$. Notice that from a δ-sequence in $\mathbb{N}_{>0}$ $\mathcal{D} = \{\delta_0, \ldots, \delta_g\}$, there exists an easy-to-apply algorithm that provides another δ-sequences in $\mathbb{N}_{>0}$, $\mathcal{D}' = \{\delta'_0, \delta'_1, \ldots, \delta'_{g+1}\}$, such that $\delta_i/\delta'_i = \delta_0/\delta'_0$ for all $i =$

$1, 2, \ldots, g$. This means that the dual graph associated to $\mathcal{D}'$ is an enlargement of the one of $\mathcal{D}$. Once one gets such a δ-sequence in $\mathbb{N}_{>0}$, $\mathcal{D}$, with $g+1$ elements, there exist also easy-to-apply algorithms to obtain either δ-sequences of type C with $g+1$ elements or of type D with $g+2$ elements or pieces of one of type E. Recall that, depending on the type of valuation, the corresponding semigroup will be in $\mathbb{Z}^2$, $\mathbb{R}$ or $\mathbb{Q}$. Details can be found in [**21**].

With a δ-sequence Δ as above, following Theorem 5.2, one gets approximates $q_0 := x$, $q_1 := y$, $q_{i+1} := q_i^{n_i} - \prod_{j=0}^{i-1} q_j^{a_{ij}}$ and a weight function $w_\Delta : \mathbb{F}_q[x, y] \to S_\Delta$ such that generators for the vector spaces O_α are easy to compute from those approximates. In fact, they are monomials on the q_i's of suitable weights. Now, pick an epimorphism of $\mathbb{F}_q$-algebras $ev : \mathbb{F}_q[x, y] \to \mathbb{F}_q^n$ (usually, we get it by evaluating n points p_i, $1 \leq i \leq n$, in $\mathbb{F}_q^2$). Then, the *family of evaluation or primal codes* given by Δ will be $\{E_\alpha := ev(O_\alpha)\}_{\alpha \in S_\Delta}$ and the family of dual codes $\{C_\alpha\}_{\alpha \in S_\Delta}$ will be named *family of dual evaluation or dual codes* given by Δ. Notice that depending on n, there is a positive integer Ω_n such that the vector spaces C_α vanish whenever $\alpha \geq \Omega_n$.

As in the case of classical order functions, for $\beta \in S_\Delta$ set

$$\omega_\beta := \text{card}\{(\beta_1, \beta_2) \in S_\Delta^2 \ \mid \ \beta_1 + \beta_2 = \beta\}.$$

This allows us to define the *Feng-Rao (designed minimum) distances* of C_α

$$d(\alpha) := \min\{\omega_\beta | \alpha \leq \beta \in S_\Delta\}$$

and

$$d_{ev}(\alpha) := \min\{\omega_\beta | \alpha < \beta \in S_\Delta \text{ and } C_\beta \neq C_{\beta^+} \},$$

where $\beta^+ := \min\{\gamma \in S_\Delta | \gamma > \beta\}$.

Then, it happens

THEOREM 5.4. *With the above notations and if we denote $d(C_\alpha)$ the minimum distance of the dual code C_α, the following inequalities hold*

$$d(C_\alpha) \geq d_{ev}(\alpha) \geq d(\alpha).$$

It is worthwhile to add that Reed-Solomon codes are a particular case of codes of the type just described. This can be done by considering δ-sequences of type C with two elements [**21**, Proposition 5.6] and suitable evaluation maps. We conclude this section with some examples showing some of the parameters of the attached codes.

EXAMPLE 5.5. In this example, we give codes over the field $\mathbb{F}_7$ of length n=12. From the δ-sequence in $\mathbb{N}_{>0}$, $\Delta = \{11, 9\}$ we construct $\Delta_1 = \{(5, 1), (4, 1)\}$ which is of type C. $\Delta_2 = \{11/9, 1, (19 - \frac{2\sqrt{3}+1}{3\sqrt{3}+1})/9\}$ of type D and $\Delta_3 = \{11/9, 1, 3/2, 9/4, \ldots\}$ of type E. Our map ev is given by evaluating at the following set of points:

$$\{(1, 1), (2, 2), \ldots, (6, 6), (1, 2), (1, 3), \ldots, (1, 6), (2, 1)\}.$$

Note that $q_0 = x, q_1 = y$ are approximates for Δ_1 and q_0, q_1 and $q_2 = y^{11} - x^9$ for Δ_2. Table 1 shows the parameters of the corresponding codes and the parameters in the first 3 rows of the case given by Δ_1 cannot be improved. Symbols α, α' and α" correspond with suitable elements in the semigroups of the corresponding weight functions.

TABLE 1. Parameters for Example 5.5

k	$d_{\Delta_1}(C_\alpha)$	$d_{ev,\Delta_1}(\alpha)$	k	$d_{\Delta_2}(C_{\alpha'})$	$d_{ev,\Delta_2}(\alpha')$	k	$d_{\Delta_3}(C_{\alpha"})$	$d_{ev,\Delta_3}(\alpha")$
10	2	2	10	2	2	10	2	2
9	3	3	9	3	2	9	3	2
8	4	3	8	4	2	8	4	2
7	4	3	7	4	3	7	4	2
6	4	4	6	4	3	6	4	2
5	5	5	5	4	4	5	4	4
4	5	5	4	6	4	4	5	4
3	6	6	3	6	4	3	5	5
2	6	6	2	6	4	2	7	4
1	10	10	1	6	5	1	6	7

EXAMPLE 5.6. Our next families of codes are defined over the field $\mathbb{F}_{2^5}$ and their length is $n = 31$. Set ξ a primitive element of the field and consider the following δ-sequences of type C: $\Delta_1 = \{(21,0),(15,0),(35,0),(39,-1)\}$, $\Delta_2 = \{(2,1),(1,1)\}$ and $\Delta_3 = \{(5,5),(2,2),(7,8)\}$. For simplicity, we only give approximates for Δ_1, which are $q_0 = x, q_1 = y, q_2 = y^7 + x^5$ and $q_3 = x^{15} + x^{10}y^7 + x^{15}y^{14} + x^5 + y^{21}$. Finally, the mapping ev is given by evaluating at the points:

$$\{(\xi,\xi),(\xi,\xi^2),\ldots,(\xi,\xi^{14}),$$
$$(\xi^2,\xi),(\xi^2,\xi^2),\ldots,(\xi^2,\xi^{14}),(\xi^3,\xi^3),(\xi^4,\xi^4),(\xi^5,\xi^5)\}.$$

Table 2 shows some parameters for the attached codes:

TABLE 2. Parameters for Example 5.6

α	exp	k	$d_{\Delta_1}(C_\alpha)$	$d_{ev,\Delta_1}(\alpha)$	$d_{\Delta_2}(C_{\alpha'})$	$d_{ev,\Delta_2}(\alpha')$	$d_{\Delta_3}(C_{\alpha"})$	$d_{ev,\Delta_3}(\alpha")$
(15,0)	0100	29	2	2	2	2	2	2
(21,0)	1000	28	3	2	3	3	2	2
(30,0)	0200	27	3	2	3	3	3	2
(35,0)	0010	26	4	2	3	3	3	2
(36,0)	1100	25	4	2	4	4	3	2
(39,-1)	0001	24	4	3	5	5	5	3
(42,0)	2000	23	4	3	5	5	6	3
(45,0)	0300	22	5	3	5	5	6	3
(50,0)	0110	21	5	3	6	6	7	3

The columns α and exp correspond to the codes given by Δ_1 and show the elements in the semigroup S_{Δ_1} and the exponents of the approximates that give the new generator we must add the previous ones for obtaining a basis of the vector space O_α.

EXAMPLE 5.7. We finish with another example of a larger code. The field is the same as in Example 5.6, the length is $n = 34$ and it is given by the δ-sequence type C, $\Delta = \{\delta_{1,1} = (2,1), \delta_{2,1} = (1,1)\}$. The corresponding map $ev : \mathbb{F}_{2^5}[X_1, X_2] \to \mathbb{F}_{2^5}^{34}$ is defined by evaluating at the points $\{(\xi^i,\xi^i) \mid 1 \le 1 \le 30\} \cup \{(0,0),(1,\xi),(1,\xi^2),(1,\xi^3)\}$. A partial table of parameters is given in Table 3.

5.2. Codes given by finitely many valuations at infinity.

In the previous section we introduced a huge family of easy to construct and decode codes. We developed a method for obtaining that family from the so-called plane valuations at infinity. Examples within the mentioned family without theoretic development were previously given in [**48**]. With this procedure and working with a finite field $\mathbb{F}_q$ we can get codes of length at most q^2 by evaluating at points in the plane affine $\mathbb{F}_q^2$. We devote this section to explain how using several plane valuations as above one can get larger codes. In fact, we can obtain families

TABLE 3. Parameters for Example 5.7

k	d	d_{ev}
33	2	2
32	2	2
31	3	3
30	4	4
29	4	4
28	5	5
27	5	5
26	6	6
25	7	7

of codes of length q^m, $m \geq 2$, by considering $m-1$ δ-sequences (and therefore $m-1$ plane valuations at infinity). Our families of codes are determined by weight functions, so they are suitable for being decoded with the aid of the Berlekamp-Massey-Sakata algorithm and admit Feng-Rao type bounds. Complete details can be found in [**22**].

We start by introducing the concept of well-suited family of elements in a totally ordered commutative group $(G, \leq)$. Consider families $\Gamma = \{\gamma_{i,j}\}_{(i,j)\in\mathbb{I}}$ of elements in G which can be written of the form

$$\begin{array}{cccc} \gamma_{1,r_1} & & & \\ \gamma_{2,1}, & \gamma_{2,2}, & \ldots, & \gamma_{2,r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_{m,1}, & \gamma_{m,2}, & \ldots, & \gamma_{m,r_m}, \end{array} \tag{5.1}$$

where $r_1 := 1$ and $r_i \leq \infty$, for $2 \leq i \leq m$, such that Γ generates a cancellative well-ordered commutative with zero and with admissible ordering $\leq$ semigroup S_Γ, and $\gamma_{i,j}$ is not in the semigroup spanned by $\{\gamma_{l,s}\}_{(l,s)\in\mathbb{L}(i,j)}$, where $\mathbb{L}(i,j) := \{(l,s) \in \mathbb{I} | (l,s) <_{\mathcal{L}} (i,j)\}$, $<_{\mathcal{L}}$ being the lexicographical ordering in $\mathbb{Z}^2$, defined as $(i_1, j_1) <_{\mathcal{L}} (i_2, j_2)$ if either $i_1 < i_2$ or $i_1 = i_2$ and $j_1 < j_2$.

Then we can state our definition:

DEFINITION 5.8. A *well-suited* family of elements in G is a family Γ as above such that, for each $(i,j) \in \mathbb{I}$, $j \neq r_i$, there exists $n_{i,j} \in \mathbb{N}$, $n_{i,j} > 1$, satisfying the following properties:

(1) $n_{i,j}\gamma_{i,j} > \gamma_{i,j+1}$.
(2)
$$n_{i,j}\ \gamma_{i,j} \ = \sum_{(l,s)\in\mathbb{J}(i,j)} m_{l,s}\gamma_{l,s},$$
for some finite subset of indices, $\mathbb{J}(i,j)$, of $\mathbb{L}(i,j)$, where the coefficients $m_{l,s}$ are positive and $m_{l,s} < n_{l,s}$ whenever $s \neq r_l$.
(3) Any element $\gamma \in S_\Gamma$ can be expressed in a unique way in the form
$$\gamma = \sum_{(i,j)\in\mathfrak{I}} \mathfrak{m}_{i,j}\gamma_{i,j},$$
where $\mathfrak{I}$ is a finite subset of $\mathbb{I}$ and $0 < \mathfrak{m}_{i,j} < n_{i,j}$ when $j \neq r_i$.

Bearing in mind the behavior of the families of approximates for valuations at infinity, we note that well-suited sequences give rise to families of polynomials which will be useful to provide weight functions. Next we define such polynomials.

DEFINITION 5.9. Let $\Gamma = \{\gamma_{i,j}\}_{(i,j)\in\mathbb{I}}$ be a well-suited family of elements in a totally ordered commutative group G and consider the polynomial ring in m indeterminates over the finite field of q elements expressed, for convenience, $\mathbb{F}_q[X,m] := \mathbb{F}_q[X_1, X_2, \ldots, X_m]$. Fix a set $\Lambda = \{\lambda_{i,j}\}_{(i,j)\in\mathbb{I}}$ of nonzero elements in $\mathbb{F}_q$. We define the *family of approximated polynomials* attached to Γ and Λ as the family of polynomials in $\mathbb{F}_q[X,m]$, $\mathbb{P}_{\Gamma,\Lambda} := \{q_{i,j}\}_{(i,j)\in\mathbb{I}}$, given by $q_{i,1} := X_i$ and, for $j \neq 1$,

$$q_{i,j} := q_{i,j-1}^{n_{i,j-1}} - \lambda_{i,j-1} \prod q_{l,s}^{m_{l,s}}, \tag{5.2}$$

where the values $n_{i,j-1}$ and $m_{l,s}$, $(l,s) \in \mathbb{J}(i,j-1)$ correspond to the expression of $n_{i,j-1}\gamma_{i,j-1}$ given in item (2) of Definition 5.8.

Let us see an example to clarify our definitions.

EXAMPLE 5.10. The following set

$$\begin{array}{l} \{\gamma_{1,1} = (120,0,0), \\ \quad \gamma_{2,1} = (48,0,0), \qquad \gamma_{2,2} = (132,0,0), \qquad \gamma_{2,3} = (156,-12,0), \\ \gamma_{3,1} = (26,-2,0), \quad \gamma_{3,2} = (26,-2,-1)\}. \end{array}$$

is a well-suited family of elements in the additive group $\mathbb{Z}^3$ lexicographically ordered.

Next result (see [**22**, Theorem 2.1] for a proof) shows why having a well-suited family of elements is useful for our purposes.

THEOREM 5.11. *Let $\Gamma = \{\gamma_{ij}\}_{(i,j)\in\mathbb{I}}$ be a well-suited family of elements of a totally ordered commutative group G, expressed as in (5.1), and let $\mathbb{P}_{\Gamma,\Lambda} := \{q_{i,j}\}_{(i,j)\in\mathbb{I}}$ be the family of approximated polynomials attached to Γ and a set $\Lambda = \{\lambda_{i,j}\}_{(i,j)\in\mathbb{I}}$ of nonzero elements in $\mathbb{F}_q$. Then, there exists a weight function $w : \mathbb{F}_q[X,m] \to S_\Gamma \cup \{-\infty\}$ such that $w(q_{i,j}) = \gamma_{i,j}$.*

This is not a theoretical result because the weight of a polynomial $f \in \mathbb{F}_q[X,m]$ can be obtained by means of an algorithm, given in [**22**], that expresses f as a finite sum of terms of the type $\alpha \prod_{(i,j)\in\mathbb{I}} q_{i,j}^{k_{i,j}}$, where $\alpha \in \mathbb{F}_q$, $0 \leq k_{i,j} < n_{i,j}$ whenever $(i,j) \in \mathbb{I}$ and $j \neq r_i$, and $k_{i,j} = 0$ except for finitely many indices. Then $w(f)$ will be the maximum of the weights of those terms (which are easily obtained from the elements in Γ). We have given all the ingredients we need for stating our main result in this section [**22**, Theorem 2.2].

THEOREM 5.12. *Let $\Gamma = \{\gamma_{i,j}\}_{(i,j)\in\mathbb{I}}$ be a well-suited family and $ev : \mathbb{F}_q[X,m] \to \mathbb{F}_q^n$ an epimorphism of $\mathbb{F}_q$-algebras. Consider $\mathbb{P}_{\Gamma,\Lambda} := \{q_{i,j}\}_{(i,j)\in\mathbb{I}}$ a family of approximated polynomials attached to Γ. Then*

(1) *For each $\gamma \in S_\Gamma$, the vector space $L_\gamma := \{f \in \mathbb{F}_q[X,m] | w(f) \leq \gamma\}$ is generated by the set of polynomials $\prod_{(i,j)\in\mathfrak{I}} q_{i,j}^{\mathfrak{m}_{i,j}}$ such that $\mathfrak{I}$ and $\mathfrak{m}_{i,j}$ run over the indices and coefficients set corresponding to the unique expression (item (3) of Definition 5.8) of the values $\eta \in S_\Gamma$ such that $\eta \leq \gamma$.*

(2) *Let $d(C_\gamma)$, with $\gamma \in S_\Gamma$, denote the minimum distance of the dual code $C_\gamma := (ev(L_\gamma))^\perp$ and consider the same definitions given before Theorem 5.4 for the family of codes and its attached semigroups. Then $d(C_\gamma) \geq d_{ev}(\gamma) \geq d(\gamma)$.*

(3) *It happens that* $d(\gamma) \leq \min\left[\prod_{(i,j)\in\mathfrak{I}}(\mathfrak{m}_{i,j}+1)\right] \leq d_{ev}(\gamma)$*, where* $\mathfrak{I}$ *and* $\mathfrak{m}_{i,j}$ *run over the indices and coefficients set of the above mentioned unique expression of the values* $\eta \in S_\Gamma$ *such that* $\gamma \leq \eta < \Omega_n$*.*

We conclude this section and the whole paper by giving a procedure to get well-suited families. We will obtain them from suitable families of δ-sequences. As we have explained, one can compute from a δ-sequence a set of pairs that by means of an Euclidean type algorithm provide the dual graph of the corresponding plane valuation at infinity. Our procedure is supported on an extension of that algorithm for values in the additive semigroup, $\mathbb{R}^n_+$, of nonnegative elements in $\mathbb{R}^n$, $n \geq 1$, under the lexicographical ordering. n-tuples $(u_1, u_2, \ldots, u_n)$ in $\mathbb{R}^n_+$ will be usually expressed as $\underline{u}$ and the following version of the Euclidean division holds.

PROPOSITION 5.13. *Let* $\underline{u} \geq \underline{v} \in \mathbb{R}^n_+$ *be such that there exists an index* s $(1 \leq s \leq n)$ *satisfying* $u_j = v_j = 0$ *for* $j < s$ *and* $v_s > 0$*, then there exists a unique positive integer* a *such that* $\underline{u} = a\underline{v} + \underline{w}$ *and* $(0, 0, \ldots, 0) =: \underline{0} \leq \underline{w} < \underline{v}$*.*

Thus, if $\underline{u}_0 \geq \underline{u}_1$ are two elements in $\mathbb{R}^n_+$, one can perform successively Euclidian divisions:

$$\begin{array}{ccccc} \underline{u}_0 & = & a_0\underline{u}_1 + \underline{u}_2; & & \underline{0} < \underline{u}_2 < \underline{u}_1 \\ \underline{u}_1 & = & a_1\underline{u}_2 + \underline{u}_3; & & \underline{u}_1 < \underline{u}_3 < \underline{u}_2 \\ \vdots & \vdots & \vdots & & \vdots \\ \underline{u}_{l-1} & = & a_{l-1}\underline{u}_l + \underline{u}_{l+1}; & & \underline{u}_{l-1} < \underline{u}_{l+1} < \underline{u}_l \\ \vdots & \vdots & \vdots & & \vdots\ . \end{array} \tag{5.3}$$

Then, the following possibilities for the algorithm can happen:

(1) It stops and for some index k, one gets $\underline{u}_k = a_k\underline{u}_{k+1} + \underline{0}$.
(2) It never stops and we obtain an infinite sequence of natural numbers $a_l, l \geq 0$.
(3) It stops and, for some index k, one gets that there exists another index s, $1 \leq s \leq n$, such that the first s components $u_{k+1,j}$, $1 \leq j \leq s$, of $\underline{u}_{k+1}$ vanish, but $u_{k,s} \neq 0$, being $u_{k,1} = \cdots = u_{k,s-1} = 0$, that is, $a_k = \infty$.

When the first item (1) happens, we say that $\underline{u}_{k+1}$ is the greatest common divisor of $\underline{u}_0$ and $\underline{u}_1$. Moreover, for $\underline{u}, \underline{v} \in \mathbb{R}^n_+$ we shall write $a := \underline{u}/\underline{v}$ whenever there exists $a \in \mathbb{N}_{>0}$ such that $\underline{u} = a\underline{v}$, where we have considered the scalar multiplication. The above procedure establishes an equivalence relation on the subset $\mathcal{A}$ of pairs $(\underline{u}, \underline{v})$ of $\mathbb{R}^n_+ \times \mathbb{R}^n_+$ such that $\underline{u} \geq \underline{v}$ which produces large equivalence classes.

DEFINITION 5.14. Two pairs $(\underline{u}_0,\ \underline{u}_1)$ *and* $(\underline{v}_0,\ \underline{v}_1)$ *in the above set* $\mathcal{A}$ are *said to be* equivalent *(or related by the "Euclidean" relation* $\mathcal{R}_E$*) if the Euclidean algorithm (5.3) applied to both of them provides the same case and the same values* $\langle a_0; a_1, \ldots, a_l, \ldots\rangle$*.*

EXAMPLE 5.15. Consider the set $\mathcal{A}$ in $\mathbb{R}^2_+$. Then, the pairs $[(14, 9), (6, 4)]$ and $[(7, 9), (3, 6)]$ are in the same class represented by $\langle 2; 3, \infty\rangle$. The pairs $[(14, 7), (6, 3)]$, $[(14, 0), (6, 0)]$, $[(0, 7), (0, 3)]$ are in the same class $\langle 2; 3\rangle$. And, $[(\pi, 0), (e, 0)]$ and $[(\pi, 1), (e, 3)]$ are in the class $\langle 1; 6, 2, 2, 1, 2\ldots\rangle$.

The mentioned equivalence relation allows us to provide the concept of δ-sequence in $\mathbb{R}^n_+$. First, we introduce the so-called canonical δ-sequences. Set

$\Delta = \{\delta_i\}_{i=0}^r$, $r \leq \infty$, a δ-sequence and for all i write $\underline{\delta}_i := (\delta_i, 0, \ldots, 0) \in \mathbb{R}_+^n$, where we add $n-1$ zeroes except when the δ-sequence is of type C, in which case we add only $n-2$ zeroes. Obviously, $n \geq 2$ for δ-sequences of type C. Then, the set $\underline{\Delta} = \{\underline{\delta}_i\}_{i=0}^r$ is called the *canonical* δ-sequence in $\mathbb{R}_+^n$ corresponding to Δ.

DEFINITION 5.16. A sequence $\underline{\Delta} = \{\underline{\delta}_i\}_{i=0}^r$ of finitely or infinitely many elements in $\mathbb{R}_+^n$ is called to be a *δ-sequence in $\mathbb{R}_+^n$* if, for $1 \leq i \leq r-1$, the value $\underline{d}_i := \gcd(\underline{\delta}_0, \underline{\delta}_1, \ldots, \underline{\delta}_{i-1})$ is defined and each pair of the sequence $\{(\underline{m}_i, \underline{e}_i)\}$, defined as we did after (3.2), where $n_i := \underline{d}_i/\underline{d}_{i+1}$, $1 \leq i \leq r-1$, belongs to the same class with respect to the relation $\mathcal{R}_E$ that the pairs attached to some canonical δ-sequence in $\mathbb{R}_+^n$.

This means that the set of δ-sequences in $\mathbb{R}_+^n$ can be partitioned into equivalence classes containing what we call *equivalent δ-sequences represented by a canonical δ-sequence*.

Let us show a clearing example.

EXAMPLE 5.17. Let $\Delta = \{\delta_0 = (5,5), \delta_1 = (2,2), \delta_2 = (7,8)\}$ be a δ-sequence of type C. The attached canonical δ-sequence in $\mathbb{R}_+^4$ will be

$$\underline{\Delta} = \{\underline{\delta}_0 = (5,5,0,0), \underline{\delta}_1 = (2,2,0,0), \underline{\delta}_2 = (7,8,0,0)\}.$$

The sequence $\{(\underline{m}_i, \underline{e}_i)\}_{i=0,1}$ is given by $\underline{e}_0 = (3,3,0,0)$, $\underline{m}_0 = (5,5,0,0)$, $\underline{e}_1 = (1,1,0,0)$ because $(5,5,0,0) = 2(2,2,0,0) + (1,1,0,0)$ and $(2,2,0,0) = 2(1,1,0,0)$, $n_1 = 5$ and $\underline{m}_1 = 5(2,2,0,0) - (7,8,0,0) = (3,2,0,0)$. The pairs $[(5,5,0,0),(3,3,0,0)]$ and $[(3,2,0,0),(1,1,0,0)]$ determine the classes given by $\langle 1; 1, 3\rangle$ and $\langle 2; 1, \infty\rangle$.

An equivalent δ-sequence in $\mathbb{R}_+^4$ will be

$$\underline{\Delta}' = \{\underline{\delta}'_0 = (35,15,35,15), \underline{\delta}'_1 = (14,6,14,6), \underline{\delta}'_2 = (49,22,55,19)\}.$$

Indeed, $\underline{e}'_0 = (21,9,21,9)$, $\underline{m}'_0 = (35,15,35,15)$ and the pair $(\underline{m}'_0, \underline{e}'_0)$ is in the class $\langle 1; 1, 3\rangle$. Moreover, $\underline{d}'_2 = (7,3,7,3)$ because $(35,15,35,15) = 2(14,6,14,6) + (7,3,7,3)$ and $(14,6,14,6) = 2(7,3,7,3)$, therefore $n_1 = 5$ and so $\underline{e}'_1 = (7,3,7,3)$ and $\underline{m}'_1 = (21,8,15,11)$. Finally, we complete our explanation after checking that $(\underline{m}'_1, \underline{e}'_1)$ is in the class represented by $\langle 2; 1, \infty\rangle$.

It is important to notice that the semigroups spanned by equivalent δ-sequences in $\mathbb{R}_+^n$, lexicographically ordered, are isomorphic ordered semigroups [**22**].

As we have said, our aim is to obtain codes from well-suited families. Next, we define sum of δ-sequences and state a result which proves that they are families of the desired type.

DEFINITION 5.18. Let $(\Delta_i)_{i=2}^m$ be an ordered set of δ-sequences, all of them either of type C or D except the last one, Δ_m, which is also allowed to be of type E. A *sum* of these δ-sequences, $\sum_{i=2}^m \Delta_i$, is a family of elements in $\mathbb{R}_+^n$ (for some positive integer n) of the form

$$\begin{array}{cccc} \underline{\delta}_{1,r_1} & & & \\ \underline{\delta}_{2,1}, & \underline{\delta}_{2,2}, & \ldots, & \underline{\delta}_{2,r_2} \\ \vdots & \vdots & \vdots & \vdots \\ \underline{\delta}_{m,1}, & \underline{\delta}_{m,2}, & \ldots, & \underline{\delta}_{m,r_m}, \end{array} \tag{5.4}$$

$r_1 := 1$, $r_j < \infty$, $2 \leq j < m$ and $r_m \leq \infty$, such that $\{\underline{\delta}_{i-1,r_{i-1}}, \underline{\delta}_{i,1}, \ldots, \underline{\delta}_{i,r_i}\}$ is a δ-sequence in $\mathbb{R}_+^n$ in the same class as the canonical δ-sequence in $\mathbb{R}_+^n$ corresponding to

Δ_i, for $2 \leq i \leq m$. We also require that, for each i, the intersection of the subgroups spanned by $\{\underline{\delta}_{l,s} \mid (l,s) \in \mathbb{L}(i,r_i)\backslash\mathbb{L}(i-1,r_{i-1})\}$ and by $\{\underline{\delta}_{l,s} \mid (l,s) \in \mathbb{L}(i-1,r_{i-1})\}$ be trivial.

THEOREM 5.19. (See [**22**, Theorem 3.4]). *Let $\{\nu_i\}_{2\leq i\leq m}$ be a family of $m-1$ plane valuations at infinity as above whose semigroups at infinity are generated by their corresponding δ-sequences, $\{\Delta_i\}_{2\leq i\leq m}$, which define weight functions denoted by $\{w_{\Delta_i}\}_{2\leq i\leq m}$. Then any sum of δ-sequences $\Sigma := \sum_{i=2}^{m} \Delta_i$ is a well-suited family of elements in the additive group $\mathbb{R}^n$ such that the values in Equality (2) of Definition 5.8 depend only on one weight function w_{Δ_i}. Therefore, a sum Σ defines a weight function w_Σ with values in the semigroup generated by Σ defined on the polynomial ring in m indeterminates $\mathbb{F}_q[X,m]$.*

It is convenient to add that to perform a sum of δ-sequences can be done by an algorithmic procedure (see Section 3.4 of [**22**]).

We finish this paper with an example that shows how a family of codes defined over the field $\mathbb{F}_3$ can be constructed with a sum of two δ-sequences. Consider $\Delta := \{\frac{20}{8}, 1, \frac{15}{8}, \vartheta := \frac{1}{8}(60 - \frac{3+2\sqrt{2}}{2+\sqrt{2}})\}$, which is a δ-sequence of type D and the δ-sequence of type C $\Delta' := \{(4,0),(1,0),(1,-1)\}$. Δ comes from the δ-sequence in $\mathbb{N}_{>0}$, $\{20,8,15\}$, after using the procedure given in [**21**, Section 4.3.3] and taking the value

$$a = 1 + \frac{1}{1 + \frac{1}{1+\sqrt{2}}}.$$

Δ' is constructed from the δ-sequence in $\mathbb{N}_{>0}$, $\{8,2,1\}$. A sum, $\Delta + \Delta'$, is

$$\begin{array}{ccc} & (20,0) & \\ (8,0), & (15,0), & (8\vartheta,0) \\ (2\vartheta,0), & (2\vartheta,-1). & \end{array} \tag{5.5}$$

Here, $m-1=2$. The canonical δ-sequence relative to Δ is

$$\underline{\Delta} = \{(20/8,0),(1,0),(15/8,0),(\vartheta,0)\}$$

and Δ' coincides with its associated canonical δ-sequence. The pairs (m_0,e_0) and (m_1,e_1) corresponding to Δ' are $((4,0),(3,0))$ and $((3,1),(1,0))$, and they define the classes with respect to the relation $\mathcal{R}_E$ given by $\langle 1;3\rangle$ and $\langle 3;\infty\rangle$. This is also true in the sum as one can check.

The family of approximated polynomials has six polynomials in the indeterminates X_1, X_2, X_3, being $q_{1,1} = X_1$, $q_{2,1} = X_2$ and $q_{3,1} = X_3$. Moreover $q_{2,2} = -X_1^2 + X_2^5$, $q_{2,3} = X_1^8 - X_1^6X_2^5 - X_1^3 - X_1^2X_2^{15} + X_2^{20}$ and $q_{3,2} = -X_1^8 + X_1^6X_2^5 + X_1^3 + X_1^2X_2^{15} - X_2^{20} + X_3^4$. Indeed, $n_{2,1} = 5$, $n_{2,2} = 4$ and $n_{3,1} = 4$; $q_{2,2}$ comes from the fact that $5(8,0) = 2(20,0)$, $q_{2,3}$ from the equality $4(15,0) = 3(20,0)$ and finally $q_{3,1}$ is deduced from the fact that $4(2\vartheta,0) = 8(\vartheta,0)$. The weight function $w_{\Delta+\Delta'}$ satisfies $w_{\Delta+\Delta'}(q_{i,j}) = \delta_{i,j}$, where the values $\delta_{i,j}$ are those given in (5.5) ordered as in (5.4) and, for instance, to compute $w_{\Delta+\Delta'}(-X_1^2X_3 + X_2^5X_3)$ one must take into account that $X_1 = q_{1,1}, X_3 = q_{3,1}$ and $X_2^5 = q_{2,2} + q_{1,1}^2$, and then $w_{\Delta+\Delta'}(-X_1^2X_3 + X_2^5X_3) = w_{\Delta+\Delta'}(-q_{1,1}^2q_{3,1} + (q_{2,2}+q_{1,1}^2)q_{3,1}) = w_{\Delta+\Delta'}(q_{2,2}q_{3,1}) = (8+2\vartheta,0)$.

Consider the map ev given by evaluating the $\mathbb{F}_3$-algebra $\mathbb{F}_3[X_1,X_2,X_3]$ at the following set of points in $\mathbb{F}_3^3$:

$$\{(0,0,0),(0,1,0),(0,2,0),(1,0,0),(1,1,0),(1,2,0),(2,1,0),(2,1,1),$$

$$(2,1,2),(2,0,1),(2,0,0),(2,0,2)\}.$$

Then, we get a family of codes of length 12 whose parameters are shown in Table 4. As in Table 2, we also display the coefficients in the generating set $\Delta+\Delta'$, expressed as in (5.4), of the elements in the semigroup defining the code; these elements are lexicographically ordered. That is, the coefficients 000000, 010000, 000001, ... correspond to the elements in the semigroup $S_{\Delta+\Delta'}$: $(0,0)$, $(8,0)$, $(2\vartheta,-1)$, ..., which appear in an increasing way according to the lexicographical ordering and determine the polynomials $1, q_{1,1}, q_{3,2}, \ldots$. These monomials span the vector space to be evaluated for obtaining the desired family of codes. We note that

TABLE 4. Parameters for the family given by $\Delta+\Delta'$

coef.		k	d	d_{ev}
000000		11	2	2
010000		10	2	2
000001		9	2	2
000010		8	2	2
001000		7	3	2
020000		6	4	2
100000		5	4	4
010001		4	4	4
010010		3	6	4
011000	*	2	7	4
110000		1	12	4

the code given in * is the same as that given by the coefficients 030000, that is $C_{(23,0)} = C_{(24,0)}$.

References

[1] S.S. Abhyankar and T.T. Moh, *Newton Puiseux expansion and generalized Tschirnhausen transformation*, J. Reine Angew. Math. **260** and **261** (1973) 47–83 and 29–54.

[2] H.E. Andersen and O. Geil, *Evaluation codes from order domain theory*, Finite Fields Appl. **14** (2008) 92–123.

[3] A. Barvinok, *Integer points in polyhedra*, Zurich Lect. Advanced Math., EMS, 2008.

[4] P. Beelen and D. Ruano, *The order bound for toric codes*, in *AAECC 2009*, LNCS 5527, 1-10, Springer, 2009.

[5] E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

[6] A. Campillo, *Algebroid curves in positive characteristic*, Lect. Notes Math. 613, Springer-Verlag, 1980.

[7] A. Campillo and J. Castellanos, *Curve singularities*, Actualités Mathématiques, Hermann, 2005.

[8] A. Campillo and J.I. Farrán, *Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models*, Finite Fields Appl. **6** (2000) 71–92.

[9] A. Campillo and J.I. Farrán, *Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes*, Math. Comp. **71** (2001) 1759–1780.

[10] A. Campillo, J.I. Farrán and M. J. Pisabarro, *Evaluation codes at singular points of differential equations*, Appl. Algebra Engrg. Comm. Comput. **18** (2007) 191–203.

[11] A. Campillo and J. Olivares, *Polarity with respect to a foliation and Cayley-Bacharach theorems*, J. Reine Angew. Math. **534** (2001) 95–118.

[12] J.A. De Loera, *The many aspects of counting lattice points in polytopes*, Math. Semesterber. **52** (2005) 175–195.

[13] W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 3-1-5 — A computer algebra system for polynomial computations, TU Kaiserslautern, 2012. Available via `http://www.singular.uni-kl.de`.
[14] F. Delgado, C. Galindo and A. Nuñez, *Saturation for valuations on two-dimensional regular local rings*, Math. Z. **234** (2000) 519–550.
[15] J.I. Farrán and C. Lossen, `brnoeth.lib`, *A* SINGULAR *library for the Brill-Noether algorithm, Weierstrass semigroups and AG codes, 2001.* Available via `http://www.singular.uni-kl.de`.
[16] G.L. Feng and T.R.N. Rao, *Decoding of algebraic geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39** (1993) 37–45.
[17] M. Fujimoto and M. Suzuki, *Construction of affine plane curves with one place at infinity*, Osaka J. Math. **39** (2002) 1005–1027.
[18] W. Fulton, *Algebraic curves*, W.A. Benjamin, Inc. (1969).
[19] C. Galindo, *Plane valuations and their completions*, Comm. Algebra **23** (1995) 2107–2123.
[20] C. Galindo and M. Sanchis, *Evaluation codes and plane valuations*, Des. Codes Crypt. **41** (2006) 199–219.
[21] C. Galindo and F. Monserrat, *δ-sequences and evaluation codes defined by plane valuations at infinity*, Proc. Lond. Math. Soc. **98** (2009) 714–740.
[22] C. Galindo and F. Monserrat, *Evaluation codes defined by finite families of plane valuations at infinity*, Des. Codes Cryptogr. (2012). D.O.I. 10.1007/s10623-012-9738-7.
[23] C. Galindo and F. Monserrat, *The Abhyankar-Moh theorem for plane valuations at infinity*, J. Algebra **374** (2013) 181–194.
[24] O. Geil, *Evaluation codes from an affine variety code perspective*, in Advances in Algebraic Geometry Codes, E. Martínez-Moro, C. Munuera, D. Ruano (Eds.) 153–180, World Scientific, 2008.
[25] O. Geil and R. Pellikaan, *On the structure of order domains*, Finite Fields Appl. **8** (2002), 369–396.
[26] O. Geil, R. Matsumoto and D. Ruano, *Feng-Rao decoding of primary codes*, Finite Fields Appl. **23** (2013) 35–52.
[27] L. Gold, J. Little and H. Schenk, *Cayley-Bacharach and evaluation codes on complete intersections*, J. Pure Appl. Algebra **196** (2005) 91–99.
[28] J.P. Hansen, *Toric varieties, Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002) 289–300.
[29] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic Geometry codes*, in Handbook of Coding Theory, V. Pless, W.C. Huffman and R.A. Brualdi, 871–961 (vol. 1), Elsevier, Amsterdam, 1998.
[30] C.D Jensen, *Fast decoding of codes from algebraic geometry*, IEEE Trans. Inform. Theory **40** (1994) 223–230.
[31] D. Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004) 63–79.
[32] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose and T. Høholdt, *Construction and decoding of a class of algebraic geometric codes*, IEEE Trans. Inform. Theory **35** (1989) 811–821.
[33] J. Justesen, K.J. Larsen, H.E. Jensen and T. Høholdt, *Fast decoding of codes from algebraic plane curves*, IEEE Trans. Inform. Theory **38** (1992) 111–119.
[34] J.B. Little, *Algebraic Geometry codes from higher dimensional varieties*, in Advances in Algebraic Geometry Codes, E. Martínez-Moro, C. Munuera, D. Ruano (Eds.) 257–293, World Scientific, 2008.
[35] J. Little and H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006) 999–1014.
[36] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, vol. 16, Amsterdam, 1977.
[37] J.L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inform. Theory **15** (1969) 122–127.
[38] R. Matsumoto, *Miura's generalization of one point AG codes is equivalent to Høholdt, van Lint and Pellikaan's generalization*, IEICE Trans. Fundam. **E82-A (10)** (1999) 2007–2010.
[39] E. Martínez-Moro and D. Ruano, *Toric codes*, in Advances in Algebraic Geometry Codes, E. Martínez-Moro, C. Munuera, D. Ruano (Eds.) 295–322, World Scientific, 2008.

[40] A.J. Reguera, *Semigroups and clusters at infinity*, in Algebraic Geometry and Singularities, La Rábida, 1991, Progr. Math. **134** (1996) 339–374.
[41] D. Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields Appl. **13** (2007) 962–976.
[42] S. Sakata, *Extension of the Berlekamp-Massey algorithm to N dimensions*, Inform. and Comput. **84** (1990) 207–239.
[43] S. Sakata, J. Jensen and T. Høholdt, *Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-Rao bound*, IEEE Trans. Inform. Theory **41** (1995) 1762–1768.
[44] S. Sakata, J. Justesen, Y. Madelung, H.E. Jensen and T. Høholdt, *Fast decoding of algebraic geometric codes up to designed minimun distance*, IEEE Trans. Inform. Theory **41** (1995) 1672–1677.
[45] A.N. Skorobogatov and S.G. Vlădut, *On the decoding of algebraic geometric codes*, IEEE Trans. Inform. Theory **36** (1990) 1051-1060.
[46] M. Spivakovsky, *Valuations in function fields of surfaces*, Amer. J. Math. **112** (1990) 107–156.
[47] M.E. O'Sullivan, *Decoding of codes defined by a single point on a curve*, IEEE Trans. Inform. Theory **41** (1995) 1709–1719.
[48] M.E. O'Sullivan, *New codes for the Belekamp-Massey-Sakata algorithm*, Finite Fields Appl. **13** (2001) 293–317.
[49] I. Soprunov and J. Soprunova, *Toric codes and Minkowski length of polytopes*, SIAM J. Discrete Math. **23** (2009) 384–400.
[50] H. Stichtenoth, *Algebraic Function Fields and Codes*, Graduate Texts Math. vol. 254, Springer, 2008.
[51] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982) 21–28.
[52] O. Zariski and P. Samuel, *Commutative Algebra, vol. II*, Springer-Verlag, 1960.

J. I. Farrán, Departamento de Matemática Aplicada, Univ. de Valladolid, Spain
E-mail address: jifarran@eii.uva.es

C. Galindo, Departamento de Matemáticas and IMAC, Univ. Jaume I, Spain
E-mail address: galindo@uji.es