ON THE EVALUATION CODES GIVEN BY SIMPLE δ-SEQUENCES

C. GALINDO AND R. PÉREZ-CASALES

Abstract. Plane valuations at infinity are classified in five types. Valuations in one of them determine weight functions which take values on semigroups of $\mathbb{Z}^2$. These semigroups are generated by δ-sequences in $\mathbb{Z}^2$. We introduce simple δ-sequences in $\mathbb{Z}^2$ and study the evaluation codes of maximal length that they define. These codes are geometric and come from order domains. We give a bound on their minimum distance which improves the Andersen-Geil one. We also give coset bounds for the involved codes.

1. Introduction

Error-correcting codes defined with tools of Algebraic Geometry were introduced by Goppa [28, 29]. Among their virtues are that they include very useful codes as Reed-Solomon and Reed-Muller ones and some of them attain the Varshamov-Gilbert bound [58]. In addition, some deep results of Algebraic Geometry such as the Riemann-Roch Theorem allow us to get good estimations for their parameters.

The concepts of order and weight function were introduced in [31] with the aim of avoiding technicalities in the treatment of some codes defined with Algebraic Geometry. Such functions, w, are defined over a $\mathbb{F}_q$-algebra, $\mathbb{F}_q$ being the finite field of q elements where the codes are supported. In this approach, w takes values onto a sub-semigroup S of the semigroup of nonnegative integers $\mathbb{N}_0$. One-point AG codes can be regarded as codes of this type given by certain weight functions and their associated order domains are affine coordinate rings of algebraic curves with exactly one place at infinity [43].

There is no need of considering S as a sub-semigroup of $\mathbb{N}_0$. In fact, one can consider more general semigroups [24] and this procedure gives rise to a huge family of codes which has not been much studied. An order function defines a filtration of vector spaces contained in its corresponding order domain and, together with an evaluation map, determine two families of error-correcting codes, usually named evaluation and dual families of codes. Lately, these families have been called primary and dual families of (evaluation) codes defined by the pair order function and evaluation map [27].

Dual families have been considered the most interesting ones. This fact is due to the knowledge, on the one hand, of the so-called order bounds on the minimum distance of these codes and, on the other hand, of successful decoding algorithms. The mentioned bounds were stated by Feng and Rao in the context of codes on affine varieties [11, 12, 13] and, afterwards, they have been translated to the order domains case [31]. With respect to the decoding algorithms, which have been mostly described in the context of AG codes, the so-called Berlekamp-Massey-Sakata algorithm [4, 41, 49, 50, 51] was used to get fast

Supported by Spain Ministry of Economy MTM2012-36917-C03-03 and by Universitat Jaume I P1-1B2012-04.

implementations of the modified algorithm of [33, 55] (see [34, 32]) and of the majority voting scheme for unknown syndromes of Feng and Rao [11], [57] (see also [52, 53]). This last procedure is capable of correcting errors up to half of the order bound.

The above mentioned primary family of codes has been studied in a recent paper [3]. There were also introduced the improved primary codes and an order-type bound for primary codes. In the recent literature, this bound has been named the Andersen-Geil bound. On the other hand, in [30] has been proved that AG codes can be decoded beyond the capacity of the algorithms previously mentioned. With a mix of this interpolation based list decoding and the syndrome decoding with majority voting scheme, it is shown in [37, 38] how to decode certain family of one-point AG codes up to half of the Andersen-Geil bound (see also [25, 26, 39]). These papers increase the interest on primary codes. Furthermore, a connection between the Feng-Rao and Andersen-Geil bounds is described in [27], which allows us to decode primary codes and suggests the authors to rename Andersen-Geil bound as Feng-Rao (or order) bound for primary codes. In the sequel, we will use this terminology. The above procedures do not guarantee decoding up to the actual distance, this can be carried out by using the affine variety code point of view [14, 40]. Notice that this point of view is also useful to construct quantum codes [15, 16, 17].

A lot of weight functions can be defined when we have no restriction on the semigroup S. We know little about these functions, however this is not the case of a close object: valuations. They have been studied because of their relation with Singularity Theory in Algebraic Geometry and plane valuations are completely classified [56] (see also [59]). As a consequence, valuations seem to be one of the best sources for obtaining weight functions. In [21, Proposition 2.2], one can see how to get weight functions from valuations and, in [18], a class of plane valuations which fits to these purposes, plane valuations at infinity, is introduced. Semigroups of weight functions defined by them are well-known because they are generated by the so-called δ-sequences. These valuations are related to curves with only one place at infinity, which have useful properties for coding theory as one can see in the paper [7]. To construct the above mentioned weight functions, one only needs a δ-sequence. Order bounds for the codes of the corresponding dual families and some well-behaved examples can be seen in [18]. To compute the minimum distance for primary families seems to be a difficult problem since there exist different types of δ-sequences (in $\mathbb{Z}^2$, $\mathbb{Q}$ and $\mathbb{R}$) providing different weight functions that must be combined with evaluation maps. Notice that these codes have length at most q^2, but this length can be increased as much as one desires by considering several valuations [19].

In this paper, we introduce what we call simple δ-sequences in $\mathbb{Z}^2$ and study the families of codes over $\mathbb{F}_q$ of maximal length given by them as a part of a general study of evaluation codes given by δ-sequences we are carrying through. The supporting order domain of codes given by δ-sequences is the polynomial ring in two indeterminates. These codes are obtained by evaluating polynomials at points in $\mathbb{F}_q^2$. Unlike the codes defined by algebraic curves, we do not need to worry about looking for rational points. Our codes can also be defined by considering weight functions over quotients of $\mathbb{F}_q$-algebras (see Section 3.1) and when one uses simple δ-sequences, the corresponding Δ-set has a plain structure. Recall that the Δ-set is the set of elements in the semigroup of the weight function giving different codes. We describe it for simple δ-sequences of two elements in Section 3.1 and,

otherwise, in Proposition 3.4. We complete this last result with an algorithm, Algorithm 1, that computes the mentioned Δ-set.

Reed-Muller codes $\mathrm{RM}_q(r,2)$ are included in (and improved by) families of codes given by δ-sequences with two elements. For codes in these families and with the help of our knowledge of their Δ-sets, in Proposition 3.3, we prove that their minimum distances behave as in the dual case and reach the primary Feng-Rao bound.

Our main results (Theorems 3.9 and 3.10) deal with bounding the minimum distance of codes given by simple δ-sequences with more than two elements. Theorem 3.9 provides a bound under suitable conditions of the ground field and Theorem 3.10 proves that the mentioned bound is at least as good as the primary Feng-Rao one. Notice that, in some cases, this last bound is significantly improved by ours, as one can see in Example 3.12 and in Figure 2.

In Section 4, we prove that, among the δ-sequences with two elements, $\{(1,0),(1,-1)\}$ gives the best family of primary codes. Moreover, the simple δ-sequences that enlarge the previous one are candidates for improving the mentioned family. Some good codes over different fields obtained with our procedure can be found in Table 1. These codes have the dual advantage that they have the best known parameters and can be decoded up to the distance bound in an efficient way. With respect to so-called improved primary codes, we show that the δ-sequences with two elements give the best ones and that the family of obtained codes coincides with the so-called hyperbolic one in two variables. For δ-sequences with more than two elements, we introduce the δ-improved codes which, in our examples, are at least as good as the hyperbolic ones.

In our final section, the ideas previously developed in the paper are applied to obtain coset bounds for the codimension one pairs of the family of codes given by simple δ-sequences. These bounds are useful to study thresholds for qualified and unqualified sets for secret sharing schemes based on linear codes. A brief description of secret sharing schemes is given in this section and we refer to [10, 36] and references therein for more details. Our bounds are presented in Theorem 5.2. We also give an example of two codes of codimension one with larger coset bound than that of the example given in [10, Example 5.4].

We organize this paper as follows. Section 2 describes the main notions and results related with the construction of the evaluation codes defined by δ-sequences. We give the notion of δ-sequence and some properties of the attached semigroups. Furthermore, we show how to construct weight functions from δ-sequences and, also, some results we will use in the paper concerning their associated evaluation codes. In Section 3 we state the main results of this paper. There, we describe the algebraic structure of the evaluation codes of maximal length given by δ-sequences. We also study the evaluation codes defined by simple δ-sequences and we give the mentioned bound on the minimum distance of these codes. Section 4 studies the parameters and performances of the primary codes defined by simple δ-sequences and their associated improved codes, and Section 5 contains the mentioned results about coset bounds.

2. Preliminaries

In this section we introduce the main notions and results related with the construction of evaluation codes defined by δ-sequences.

2.1. **δ-sequences.** Denote by $\mathbb{N}$ the set positive integers, the so-called δ-sequences in $\mathbb{N}$ were introduced by Abhyankar and Moh to study semigroups at infinity of projective plane curves with only one branch at infinity [1, 2]. In [18] this notion is extended by introducing the concepts of δ-sequence in $\mathbb{Z}^2$, $\mathbb{R}$ and $\mathbb{Q}$. These sequences span semigroups at infinity of plane valuations at infinity and, as a consequence, allow us to define weight functions and attached families of evaluation codes.

Definition 2.1. A *δ-sequence in* $\mathbb{N}$ is a finite sequence $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\}$ of positive integers, with $g \geq 1$, which satisfies the following conditions:

1) If $d_i = \gcd(\gamma_0, \gamma_1, \ldots, \gamma_{i-1})$ for $1 \leq i \leq g+1$ and $n_i = d_i/d_{i+1}$ for $1 \leq i \leq g$, then $d_{g+1} = 1$ and $n_i > 1$ for $1 \leq i \leq g$.
2) $n_i\gamma_i$ belongs to the semigroup generated in $\mathbb{N}_0$ by $\gamma_0, \gamma_1, \ldots, \gamma_{i-1}$ for $1 \leq i \leq g$.
3) $\gamma_0 > \gamma_1$ and $n_i\gamma_i > \gamma_{i+1}$ for $1 \leq i \leq g-1$.

S_Γ will denote the additive semigroup generated by Γ and when $g \geq 2$, the vector $\underline{n} := (n_1, n_2, \ldots, n_{g-1})$ will be called the ν-vector of Γ. Clearly, $\gamma_0 = \prod_{i=1}^{g} n_i$ and S_Γ is a telescopic semigroup [31, Section 5.4]. As a consequence, when $g \geq 2$, the product $n_i\gamma_i$, $1 \leq i \leq g$, can be expressed in a *unique form* as:

$$n_i\gamma_i = a_{i0}\gamma_0 + a_{i1}\gamma_1 + \cdots + a_{i,i-1}\gamma_{i-1}, \tag{1}$$

$a_{ij}, 0 \leq j \leq i-1$, being integers such that $a_{i0} \geq 0$, $\gcd(n_i, a_{i0}, \ldots, a_{i,i-1}) = 1$ and $0 \leq a_{ij} < n_j$ for $1 \leq j \leq i-1$. So, every $\gamma \in S_\Gamma$ can be represented in an unique form as:

$$\gamma = b_0\gamma_0 + b_1\gamma_1 + \cdots + b_g\gamma_g, \tag{2}$$

where the b_i's are nonnegative integers such that $0 \leq b_i < n_i$ for $1 \leq i \leq g$. To obtain (2), it suffices to consider an expression $\gamma = \sum_{i=0}^{g} c_i\gamma_i$ and use (1) when $c_i \geq n_i$, $i > 0$.

A *family of approximate polynomials* (or simply, approximates) for Γ is any sequence $Q_0, Q_1, \ldots, Q_g$ of polynomials in the polynomial ring in two indeterminates, $\mathbb{F}_q[X, Y]$, obtained as follows: $Q_0 := X$, $Q_1 := Y$ and

$$Q_{i+1} := Q_i^{n_i} - \lambda_i \prod_{j=0}^{i-1} Q_j^{a_{ij}}, \tag{3}$$

where the values λ_i, $1 \leq i \leq g-1$, are nonzero elements in $\mathbb{F}_q$ and the exponents a_{ij} are the coefficients described in (1).

Every δ-sequence Γ in $\mathbb{N}$ attached with a singular curve with only one place at infinity determines a sequence of pairs, (e_i, m_i), which characterize the topology of the corresponding curve [6, 18]. This sequence is defined as follows: if $\gamma_0 - \gamma_1$ does not divide γ_0, then

$$e_0 := \gamma_0 - \gamma_1, \quad m_0 := \gamma_0,$$
$$e_i := d_{i+1}, \quad m_i := n_i\gamma_i - \gamma_{i+1} \text{ for } 1 \leq i \leq g-1;$$

and otherwise

$$e_0 := \gamma_0 - \gamma_1, \quad m_0 := \gamma_0 + n_1\gamma_1 - \gamma_2$$

$$e_i := d_{i+2}, \quad m_i := n_{i+1}\gamma_{i+1} - \gamma_{i+2} \text{ for } 1 \leq i \leq g-2.$$

Let $\Gamma^* = \{\gamma_0^*, \gamma_1^*, \ldots, \gamma_g^*\}$ be a δ-sequence in $\mathbb{N}$. For our purposes, we only need to consider the following two cases.

Case i): $\gamma_0^* - \gamma_1^*$ does not divide γ_0^* and $g \geq 1$ and *case ii):* $\gamma_0^* - \gamma_1^*$ divides γ_0^* and $g \geq 2$. We write $h = g-1$ in case i) and otherwise h will be $g-2$. In both cases, set $\langle a_1; a_2, \ldots, a_t\rangle$, $a_t \geq 2$, the continued fraction expansion of the quotient m_h/e_h given by the last existing pair (e_i, m_i) attached with Γ^* and defined as in the above paragraph. To finish, we define the finite recurrence relation

$$\mathbf{y}_i = a_{t-i}\mathbf{y}_{i-1} + \mathbf{y}_{i-2} \quad 1 \leq i \leq t-1 \quad \text{with} \quad \mathbf{y}_{-1} = (0,1) \text{ and } \mathbf{y}_0 = (1,0)\,. \tag{4}$$

The following concept, introduced in [18], will be essential for our purposes.

Definition 2.2. With the above notations, a *δ-sequence in $\mathbb{Z}^2$* is a finite sequence $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\} \subset \mathbb{Z}^2$, given by a δ-sequence in $\mathbb{N}$ as in the above paragraph, $\Gamma^* = \{\gamma_0^*, \gamma_1^*, \ldots, \gamma_g^*\}$, and defined as follows.

- If Γ^* belongs either to the case i) with $g \geq 2$ or to the case ii) with $g \geq 3$, then
$$\gamma_i = \frac{\gamma_i^*}{A\,a_t + B}\,(A,B) \text{ for } 0 \leq i \leq g-1, \text{ and}$$
$$\gamma_g = \frac{\gamma_g^* + A'\,a_t + B'}{A\,a_t + B}\,(A,B) - \left(A', B'\right),$$
where $(A,B) = \mathbf{y}_{t-2}$ and $(A',B') = \mathbf{y}_{t-3}$.
- If Γ^* belongs to the case i) with $g = 1$, then $\gamma_0 = \mathbf{y}_{t-1}$ and $\gamma_1 = \gamma_0 - \mathbf{y}_{t-2}$.
- Finally, if Γ^* belongs to the case ii) with $g = 2$, then $\gamma_0 = j\,\mathbf{y}_{t-2}$, $\gamma_1 = \gamma_0 - \mathbf{y}_{t-2}$ and $\gamma_2 = \gamma_0 + n_1\gamma_1 - \mathbf{y}_{t-1}$, where $j = \gamma_0^*/\left(\gamma_0^* - \gamma_1^*\right) \in \mathbb{N}$ and $n_1 = \gamma_0^*/\gcd\left(\gamma_0^*, \gamma_1^*\right)$.

Codes in this paper will be defined from functions $w : A \to S \cup \{\infty\}$, where A is a domain and S certain type of semigroup, called weight functions (see Definition 2.6). A weight function w defines a valuation $\nu := -w$ of the quotient field of A. A δ-sequence in $\mathbb{Z}^2$ could be defined as the minimal generating set of the semigroup $-\nu(R)$ provided by the affine domain corresponding with a plane valuation at infinity ν of type C (see [18, 19] for details). However this definition is not constructive. Plane valuations are classified in five types according to the structure of their dual graphs. This structure determines the topology encoded by the valuation [56]. Plane valuations at infinity cover a large class of plane valuations and are the most natural for coding purposes. In this case, generators of the semigroup $-\nu(R)$ allow us to get the dual graph of ν (which is infinite) by using continued fractions and recurrence relations. This is the reason behind the previous definition. To run over all possibilities, one must distinguish between the cases where $\gamma_0^* - \gamma_1^*$ does not divide γ_0^* and those where the opposite happens. This was observed in [1, 2] for the close family of curves with only one place at infinity. Notice that the valuations here involved are related with singularities and the quotient $\gamma_0^*/(\gamma_0^* - \gamma_1^*)$ does not reflect a singularity whenever $\gamma_0^* - \gamma_1^*$ divides γ_0^*, so the corresponding values e_0 and m_0 must be defined in a different way as the formulae before Definition 2.2 show.

According to the above definition, we will say that Γ is the δ-sequence in $\mathbb{Z}^2$ determined by the δ-sequence in $\mathbb{N}$, Γ^*. Γ generates an additive well-ordered semigroup (with respect to the lexicographic order $<$ in $\mathbb{Z}^2$ with $(0,1) < (1,0)$), which will be denoted as S_Γ. As

an example, we can say that $\Gamma = \{(18,9),(6,3),(4,2),(1,1)\}$ is a δ-sequence determined by $\Gamma^* = \{45,15,10,3\}$. Indeed, the pair (m_2, e_2) for Γ^* is $(3 \cdot 10 - 3, 5) = (27,5)$ and $\langle a_1; a_2, a_3\rangle = \langle 5; 2, 2\rangle$, so $t = 3$, $\mathbf{y}_{-1} = (0,1)$, $\mathbf{y}_0 = (1,0) = \mathbf{y}_{t-3} = (A', B')$ and $(A, B) = 2(1,0) + (0,1) = (2,1)$.

Two δ-sequences in $\mathbb{N}$ that determine the same δ-sequence in $\mathbb{Z}^2$ share the same ν-vector. Indeed, one can define values $d_i = \gcd(\gamma_0, \gamma_1, \dots \gamma_{i-1}) \in \mathbb{Z}^2$, $1 \leq i \leq g$, by using an extended version of the Euclidean algorithm [19, Proposition 3.2], and therefore quotients $n_i = d_i/d_{i+1}$, $1 \leq i \leq g-1$, in the sense that $d_i = n_i d_{i+1}$. For instance, in the above example, $\gcd((18,9),(6,3)) = (6,3)$ because by the extended Euclidean algorithm $(18,9) = 3(6,3) + (0,0)$, $\gcd((18,9),(6,3),(4,2)) = (2,1)$ and $3 = (6,3)/(2,1)$. The construction of Γ proves that these values n_i coincide with those n_i^* for Γ^* since each γ_i, $0 \leq i \leq g-1$, is a multiple (by a pair) of γ_i^*. Note also that $d_i = \frac{d_i^*}{d_g^*}(A, B)$, $1 \leq i \leq g$, and, as we have said, $n_i = d_i/d_{i+1} = d_i^*/d_{i+1}^* = n_i^*$, $1 \leq i \leq g-1$. The above fact allows us to extend the notion of approximate polynomial to δ-sequences in $\mathbb{Z}^2$.

Definition 2.3. A family of *approximate polynomials* for a δ-sequence in $\mathbb{Z}^2$, Γ, is a sequence of approximate polynomials for any δ-sequence in $\mathbb{N}$, Γ^*, that determines Γ. Moreover, when $g \geq 2$, the *ν-vector* of Γ is defined as the ν-vector of Γ^*.

The semigroup S_Γ of a δ-sequence in $\mathbb{Z}^2$, Γ, is telescopic in sense of that it is cancellative, well-ordered and generated by a finite set $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ lexicographically ordered, where the points $\{\alpha_i\}_{i=1}^{r-1}$ belong to the same line L which passes through $(0,0)$, $\alpha_r \notin L$ and there exists a telescopic sequence $\{\beta_i\}_{i=1}^{r-1}$ such that the morphism of ordered semigroups $\rho : \langle \alpha_1, \alpha_2, \dots, \alpha_{r-1}\rangle \to \langle \beta_1, \beta_2, \dots, \beta_{r-1}\rangle$, $\rho(\alpha_i) = \beta_i$, is an isomorphism (see Definition 5.1 and the remark before Section 5.2 in [18]). Then, the following result holds.

Proposition 2.4. [18, Proposition 5.2] *Let $\Gamma = \{\gamma_0, \gamma_1, \dots, \gamma_g\}$ be a δ-sequence in $\mathbb{Z}^2$ and, when $g \geq 2$, $\underline{n} := (n_1, n_2, \dots, n_{g-1})$ its ν-vector. Then, any element $\gamma \in S_\Gamma$ can be expressed in a unique form as*

$$\gamma = b_0\gamma_0 + b_1\gamma_1 + \cdots + b_g\gamma_g,$$

where $0 \leq b_0, b_g$ and, when $g \geq 2$, $0 \leq b_i < n_i$ for $1 \leq i \leq g-1$.

Finally, we state an straightforward property of the δ-sequences, which will be used to deduce the main result of this paper.

Lemma 2.5. *Let $\Gamma = \{\gamma_0, \gamma_1, \dots, \gamma_g\}$ be a δ-sequence in $\mathbb{N}$ (respectively, in $\mathbb{Z}^2$) with $g \geq 2$. Let $(n_1, n_2, \dots, n_{g-1})$ be the ν-vector of Γ. Suppose that $\gamma_0 = n_1\gamma_1$, then $\Gamma' = \{\gamma_1, \gamma_2, \dots, \gamma_g\}$ is a δ-sequence in $\mathbb{N}$ (respectively, in $\mathbb{Z}^2$) with ν-vector $(n_2, n_3, \dots, n_{g-1})$.*

2.2. **Weight functions determined by δ-sequences.** δ-sequences Γ in $\mathbb{Z}^2$ provide weight functions $\omega_\Gamma : \mathbb{F}_q[X,Y] \to S_\Gamma \cup \{-\infty\}$ as it was shown in [18, Theorem 4.9]. Next, we show how ω_Γ works. In the rest of this paper, δ-sequence will mean δ-sequence in $\mathbb{Z}^2$. Let us recall the definition of weight function.

Definition 2.6. Let A be an algebra over $\mathbb{F}_q$ and set S an additive, commutative and well-ordered semigroup. We also denote by $<$ the ordering in S. Extend S to the semigroup $S_{-\infty} = S \cup \{-\infty\}$ by considering that $-\infty < s$ whenever $S \ni s \neq -\infty$ and $-\infty + s = -\infty$

for all $s \in S_{-\infty}$. A *weight function* is a surjective map $w : A \to S_{-\infty}$ which satisfies the following conditions for all $a, b \in A$:

1) $w(a) = -\infty$ if and only if $a = 0$,
2) $w(\lambda\, a) = w(a)$ for all $\lambda \in \mathbb{F}_q - \{0\}$,
3) $w(a+b) \leq \max\{w(a), w(b)\}$,
4) if $w(a) = w(b)$, $a \neq 0$, then there exist $\lambda \in \mathbb{F}_q - \{0\}$ such that $w(a - \lambda\, b) < w(b)$,
5) $w(ab) = w(a) + w(b)$.

In this paper, an algebra which has a weight function as above is called an *order domain* over $\mathbb{F}_q$.

In order to define a weight function associated to the δ-sequence $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\}$, we first consider a family of approximates, $Q_0, Q_1, \ldots, Q_g$, and we take into account that the following set is a basis of $\mathbb{F}_q[X, Y]$ as a vector space over $\mathbb{F}_q$:

$$\left\{ Q^\beta := \prod_{i=0}^{g} Q_i^{b_i} \;\mid\; \beta = \sum_{i=0}^{g} b_i \gamma_i \in S_\Gamma \text{ and } \mathbf{b} := (b_0, b_1, \ldots, b_g) \in \Omega_{\underline{n}} \right\},$$

where $\Omega_{\underline{n}} := \left\{ \mathbf{b} \in \mathbb{Z}^{g+1} \mid 0 \leq b_0, b_g \text{ and } 0 \leq b_i < n_i \text{ for } 1 \leq i \leq g-1 \text{ if } g \geq 2 \right\}$. The reader can see a proof of this fact in [18, Theorem 4.9] and a shorter and simpler one in [46].

This basis is well-behaving, which means that for $\alpha, \beta, \gamma \in S_\Gamma$, $l(\alpha, \gamma) < l(\beta, \gamma)$ whenever $\alpha < \beta$, where $l(\alpha, \beta) = \min\{\gamma \in \Gamma \mid Q^\alpha Q^\beta \in R_\gamma\}$ and R_γ is the subspace generated by $\{Q^\beta \mid \beta \leq \gamma\}$ (see [24, Definition 3.1]). Then, as a consequence of [24, Proposition 3.3] and [22, Proposition I.3.18], it happens that the mapping $\omega_\Gamma : \mathbb{F}_q[X, Y] \to S_\Gamma \cup \{-\infty\}$ given by $\omega_\Gamma(0) := -\infty$ and

$$\omega_\Gamma(F) := \max\left\{ \beta \in S_\Gamma \mid Q^\beta \text{ belongs to the support of } F \right\}$$

is a weight function. Moreover, ω_Γ is the unique weight function such that $\omega_\Gamma(Q_i) = \gamma_i$ for $0 \leq i \leq g$. From now on, ω_Γ (ω if no confusion arises) will be called the *weight function determined by* Γ.

2.3. **Evaluation codes defined by weight functions.** In this section, we are going to describe primary and dual families of evaluation codes given by weight functions and some of their properties. Our main references are [31, 22, 3].

Let A be an order domain with attached weight function $w : A \to S_{-\infty}$. Let $\mathcal{B} := \{f_s \mid s \in S\}$ be a well-behaving basis of A such that $w(f_t) < w(f_s)$ whenever $t < s$. Consider a surjective $\mathbb{F}_q$-algebra morphism $\varphi : A \to \mathbb{F}_q^n$, with $n \in \mathbb{N}$, that is, a linear mapping over $\mathbb{F}_q$ such that $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in A$, where $*$ represents the component-wise product. Then, the *primary (or evaluation) code determined by* an element $s \in S$ is defined as the vector subspace $E(s)$ of $\mathbb{F}_q^n$ given by

$$E(s) := \operatorname{span}_{\mathbb{F}_q}\{\varphi(f_t) \mid t \leq s\},$$

and the *dual code determined by* s is the vector subspace $C(s)$ of $\mathbb{F}_q^n$ given by

$$C(s) := E(s)^\perp = \{\mathbf{c} \mid \mathbf{c} \cdot \varphi(f_t) = 0 \text{ for } t \leq s\},$$

where $\cdot$ denotes the inner product on $\mathbb{F}_q^n$. The map φ is surjective, so there exists $\xi \in S$ such that $E(\xi) = \mathbb{F}_q^n$ and, therefore, $C(\xi) = \{\mathbf{0}\}$.

Now, set $s_1 := 0$ and for $2 \leq i \leq n$, let s_i be the smallest element in S such that it is greater than $s_1, s_2, \ldots, s_{i-1}$ and $E(t) \neq E(s_i)$ for all $t < s_i$. Then, we write $\Delta(A, w, \varphi)$ the set $\{s_1, s_2, \ldots, s_n\}$. It is clear that $\{\varphi(f_{s_i}) \mid 1 \leq i \leq n\}$ is a basis of $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. For $s \in \Delta(A, w, \varphi)$, set

$$M(s) := \left\{t \in \Delta(A, w, \varphi) \mid t = s + s' \text{ for some } s' \in \Delta(A, w, \varphi)\right\}$$

and for $s \in S$,

$$N(s) := \left\{t \in S \mid t + s' = s \text{ for some } s' \in S\right\}.$$

Also, write $\sigma(s) := \#M(s)$ and $\mu(s) := \#N(s)$. Then, one can define the *improved primary l-code*, $0 < l \leq n$, as

$$\tilde{E}(l) := \operatorname{span}_{\mathbb{F}_q}\{\varphi(f_{s_i}) \mid s_i \in \Delta(A, w, \varphi) \text{ and } \sigma(s_i) \geq l\}.$$

And, dually,

$$\tilde{C}(l) := \left\{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \varphi(f_{s_i}) = 0 \text{ where } s_i \in \Delta(A, w, \varphi) \text{ and } \mu(s_i) < l\right\}.$$

The following result summarizes the known bounds for the minimum distances, d, of the primary and dual codes defined by w and φ (see [12, 13, 31, 22, 3]).

Theorem 2.7. *Let $s \in S$ and $0 < l \leq n$. For primary codes, the following bounds (named, in case 1), either Andersen-Geil or primary Feng-Rao or primary order bounds) hold.*

1) $d(E(s)) \geq \min\{\sigma(t) \mid t \in \Delta(A, w, \varphi) \text{ with } t \leq s\}$,
2) $d\left(\tilde{E}(l)\right) \geq l$.

And, for dual ones, one gets the bounds (called, in case 1), either Feng-Rao or dual Feng-Rao or order ones).

1) $d(C(s)) \geq d_\varphi(s) \geq d(s)$, *where*

$$d_\varphi(s) := \min\{\mu(t) \mid t \in \Delta(A, w, \varphi) \text{ such that } t > s\}$$

and $d(s) := \min\{\mu(t) \mid t > s\}$,
2) $d\left(\tilde{C}(l)\right) \geq l$.

Generally speaking, it is a hard task to compute $\Delta(A, w, \varphi)$. However, under some restrictions and when A is an affine algebra, in [3] it is described a way to do it. We will use this way to give a bound on the minimum distance of the primary codes given by simple δ-sequences. First, let us explain some known facts.

Set $\mathbf{A} = \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ the polynomial ring in m indeterminates. Suppose that weights $p(X_1)$, $p(X_2)$, $\ldots$, $p(X_m) \in \mathbb{N}_0^r \setminus \{\mathbf{0}\}$ and a monomial ordering $<$ in $\mathbb{N}_0^r$ are known. A monomial $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m}$, where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{N}_0^m$, has weight $p(X^\alpha) := \sum_{i=1}^m \alpha_i p(X_i)$ and, for $F \in \mathbf{A}$, the *weight of* F is defined as

$$p(F) := \max\{p(X^\alpha) \mid X^\alpha \text{ belongs to the support of } F\}.$$

Let $\mathcal{M}$ be the set of monomials in $\mathbf{A}$, then p induces a *weighted degree ordering* on $\mathcal{M}$ defined as $M_1 <_p M_2$ if $p(M_1) < p(M_2)$ or $p(M_1) = p(M_2)$ and $M_1 \prec M_2$, where $\prec$ is some fixed monomial ordering in $\mathcal{M}$.

Recall that the footprint (or Hilbert staircase) of an ideal of the ring $\mathbf{A}$, endowed with a monomial ordering, are those monomials which are not leading ones of any polynomial

in the ideal. Assume that I is an ideal of $\mathbf{A}$ and $\mathcal{G}$ a Gröbner basis of I with respect to the weighted degree ordering $<_p$ such that the monomials in the footprint $\Delta_{<_p}(I)$ have mutually distinct weights and all the polynomials in $\mathcal{G}$ have exactly two monomials with highest weight in their support. Then, it holds:

Theorem 2.8. [3] *With the above conditions, $R := \mathbf{A}/I$ is an order domain with weight function ρ given by $\rho(0) = -\infty$ and $\rho(F+I) = p(F)$, for $F \neq 0$.*

Furthermore, if $\varphi : R \to \mathbb{F}_q^n$ is the $\mathbb{F}_q$-algebra morphism given by

$$\varphi(F+I) = (F(P_1), F(P_2), \ldots, F(P_n)),$$

where $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, P_2, \ldots, P_n\}$ is the variety of I over $\mathbb{F}_q$ and

$$I_q = I + \langle X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m \rangle,$$

then, $\Delta(R, \rho, \varphi) = p\left(\Delta_{<_p}(I_q)\right)$.

Improved dual codes and their weaker relatives (defined without considering the map φ) can also be introduced as follows. Fix a positive integer l and define $R(l) := \{s \in S \mid \mu(s) < l\}$ and $r(l) = \#\, R(l)$. Also consider the set $R_\varphi(l) := \{s \in S \mid \mu(s) < l \text{ and } C(s) \neq C(s^-)\}$, where $s^- := \max\{t \in S \mid t < s\}$ and set $r_\varphi(l) = \#\, R_\varphi(l)$.

Then, define the codes

$$\mathfrak{E}(l) := \operatorname{span}_{\mathbb{F}_q}\{\varphi(f_t) \mid t \in R(l)\},$$

and $\mathfrak{E}_\varphi(l)$ which is defined analogously but replacing $R(l)$ with $R_\varphi(l)$. We are interested in the dual codes $\mathfrak{C}(l) := (\mathfrak{E}(l))^\perp$ and $\mathfrak{C}_\varphi(l) := (\mathfrak{E}_\varphi(l))^\perp$. Clearly, $\tilde{C}(l) = \mathfrak{C}_\varphi(l)$.

It can be shown that $\mathfrak{C}(l)$ and $\mathfrak{C}_\varphi(l)$ have minimum distance at least l. A proof can be derived following that given in [31, Proposition 4.23] for semigroups included in $\mathbb{N}_0$. In addition, the dimension of $\mathfrak{C}(l)$ is at least $n - r(l)$ and that of $\mathfrak{C}_\varphi(l)$ equals $n - r_\varphi(l)$.

3. Evaluation codes defined by simple δ-sequences

δ-sequences (in $\mathbb{Z}^2$, $\mathbb{R}$ or $\mathbb{Q}$) were introduced in [18] as generating sets of semigroups of weight functions defined by plane valuations at infinity. Order bounds for dual evaluation codes were also given. Using several weight functions of this type, larger codes also given by weight functions can be constructed [19].

In the first part of this section, we show how to translate the study of evaluation codes given by δ-sequences (in $\mathbb{Z}^2$) to the context we have just explained in order to apply Theorem 2.8.

The notion of simple δ-sequence is introduced in the second part of this section, where its corresponding primary codes of maximal length are studied. There, we will show that simple δ-sequences Γ are the only ones yielding, under certain conditions, a footprint with only one monomial block (see (5) for the definition). Furthermore, we will use that fact to compute in some cases and estimate, in the other ones, the minimum distances of these codes. In fact, for certain values of q, we will give a bound on their minimum distances which improves the primary Feng-Rao one.

3.1. **Evaluation codes defined by δ-sequences.** As an initial example, we mention that the Reed-Muller code $\mathrm{RM}_q(r,2)$ belongs to the family of evaluation codes given by the δ-sequence $\{(1,0),(1,-1)\}$. In particular, $E((r,0)) = \mathrm{RM}_q(r,2)$. Weighted Reed-Muller codes in two variables are included in the set of codes given by δ-sequences with two elements. Indeed, if we consider weights $0 < b < a \in \mathbb{N}$, then there exists a δ-sequence of the type $\{(a,a'),(b,b')\}$ whose attached family of codes contains the weighted Reed-Muller codes with weights a and b. For instance for $a = 5$ and $b = 3$, one can use the δ-sequence $\{12,7\}$ in $\mathbb{N}$ which gives rise to the δ-sequence $\{(5,2),(3,1)\}$ in $\mathbb{Z}^2$.

Throughout this section we will consider a δ-sequence $\Gamma = \{\gamma_0,\gamma_1,\ldots,\gamma_g\}$ whose ν-vector, when $g \geq 2$, is $\underline{n} = (n_1,n_2,\ldots,n_{g-1})$. ω_Γ will denote the weight function determined by Γ and $Q_0,Q_1,\ldots,Q_g$ a sequence of approximates for Γ where, for the sake of simplicity, $\lambda_i = 1$ in the expression (3). In addition, $\varphi : \mathbb{F}_q[X,Y] \to \mathbb{F}_q^{q^2}$ will be the $\mathbb{F}_q$-algebra morphism given by $\varphi(F) = \left(F(P_1),F(P_2),\ldots,F\left(P_{q^2}\right)\right)$, where the P_i's are the points in $\mathbb{F}_q^2$ in some order.

Set $\mathbf{A} := \mathbb{F}_q[Z_0,Z_1,\ldots,Z_g]$ and, when $g \geq 2$, consider the set defined by the equalities in (1):

$$\mathcal{Z}_\Gamma := \left\{ Z_1^{n_1} - Z_0^{a_{10}} - Z_2, Z_2^{n_2} - Z_0^{a_{20}} Z_1^{a_{21}} - Z_3, \ldots, Z_{g-1}^{n_{g-1}} - \prod_{i=0}^{g-2} Z_i^{a_{g-1,i}} - Z_g \right\}.$$

Let I_Γ be the following ideal of the ring $\mathbf{A}$:

$$I_\Gamma = \begin{cases} \{0\} & \text{if } g = 1 \\ \langle \mathcal{Z}_\Gamma \rangle & \text{if } g \geq 2 \end{cases}.$$

Denote $\mathbf{b} = (b_0,b_1,\ldots,b_g) \in \mathbb{N}_0^{g+1}$, write $Z^{\mathbf{b}} := Z_0^{b_0} Z_1^{b_1} \cdots Z_g^{b_g}$, and define $w\left(Z^{\mathbf{b}}\right) = \sum_{i=0}^g b_i\gamma_i$ and the weight of a polynomial $H \in \mathbf{A}$, $w(H)$, as the highest weight (with respect to lexicographic ordering in $\mathbb{Z}^2$ with $(0,1) < (1,0)$) of a monomial in the support of H. Now, if $\mathcal{M}$ denotes the set of monomials in $\mathbf{A}$, one can consider on $\mathcal{M}$ the weighted degree ordering $<_{wl}$ defined as $M_1 <_{wl} M_2$ if $w(M_1) < w(M_2)$ or $w(M_1) = w(M_2)$ and $M_1 <_l M_2$, where $<_l$ is the lexicographic ordering in $\mathcal{M}$ with $Z_0 <_l Z_1 <_l \cdots <_l Z_g$.

With respect to the ordering $<_{wl}$, $\mathcal{Z}_\Gamma$ is the reduced Gröbner basis of I_Γ and the footprint of I_Γ is $\Delta_{<_{wl}}(I_\Gamma) := \left\{Z^{\mathbf{b}} \mid \mathbf{b} \in \Omega_{\underline{n}}\right\}$. So, it is straightforward to check that $\mathbf{A}$ and I_Γ satisfy the conditions in Theorem 2.8. Thus, $R := \mathbf{A}/I_\Gamma$ has a weight function $\rho : R \to S_\Gamma \cup \{-\infty\}$ given by $\rho(0) = -\infty$ and $\rho(h) = w(H)$, where $h = H + I_\Gamma$ is the equivalence class of the polynomial H modulo I_Γ. Therefore, the set $\mathcal{B} := \left\{z^{\mathbf{b}} \mid Z^{\mathbf{b}} \in \Delta_{<_{wl}}(I_\Gamma)\right\}$, where $z^{\mathbf{b}} := z_0^{b_0} z_1^{b_1} \cdots z_g^{b_g}$ and $z_i = Z_i + I$ for $0 \leq i \leq g$, is a basis of R as an $\mathbb{F}_q$-vector space. Moreover, $\mathcal{B}$ is a well-behaving basis of R determined by ρ. Hence, we have that $R = \mathrm{span}_{\mathbb{F}_q}\left\{z^{\mathbf{b}} \mid \mathbf{b} \in \Omega_{\underline{n}}\right\}$. Furthermore, the mapping $\psi : R \to \mathbb{F}_q[X,Y]$ induced by $\psi(z_i) = Q_i$, $0 \leq i \leq g$, is an isomorphism of $\mathbb{F}_q$-vector spaces.

$\mathbb{F}_q^2$ is the variety $\mathbb{V}_{\mathbb{F}_q}(I_\Gamma)$ when $g = 1$ and, otherwise, it is the set

$$\{(s,t,Q_2(s,t),\ldots,Q_g(s,t)) \mid s,t \in \mathbb{F}_q\},$$

where $Q_2(s,t) = t^{n_1} - s^{a_{10}}$ and, for $2 \leq i \leq g-1$,

$$Q_{i+1}(s,t) = (Q_i(s,t))^{n_i} - s^{a_{i0}} t^{a_{i1}} (Q_2(s,t))^{a_{i2}} \cdots (Q_{i-1}(s,t))^{a_{i,i-1}}.$$

This allows us to set $\mathbb{V}_{\mathbb{F}_q}(I_\Gamma) = \left\{V_1, V_2, \ldots, V_{q^2}\right\}$ and consider the evaluation morphism $\bar{\varphi} : R \to \mathbb{F}_q^{q^2}$ given by

$$\bar{\varphi}\left(f = F + I\right) = \left(F\left(V_1\right), F\left(V_2\right), \ldots, F\left(V_{q^2}\right)\right).$$

Now, let $\beta = \sum_{i=0}^{g} b_i\gamma_i$ be the unique expression of some fixed element $\beta \in S_\Gamma$, where $\mathbf{b} \in \Omega_{\underline{n}}$. Denote by z^β the product $z^{\mathbf{b}}$ and, using a similar notation for other elements $\eta \in S_\Gamma$, define $\bar{E}\left(\beta\right) := \operatorname{span}_{\mathbb{F}_q}\left\{\bar{\varphi}\left(z^\eta\right) \mid S_\Gamma \ni \eta \leq \beta\right\}$, and $\bar{C}\left(\beta\right) := \bar{E}\left(\beta\right)^\perp$. Then, it is clear that $\bar{E}\left(\beta\right) = E\left(\beta\right)$, where $E\left(\beta\right)$ is the *primary code of maximal length defined by* Γ. That is, the code attached to β and given by the weight function ω_Γ determined by Γ and the former morphism φ. Similarly, $\bar{C}\left(\beta\right) = C\left(\beta\right)$. Thus, if we define the ideal $I_{\Gamma,q} := I_\Gamma + \langle Z_i^q - Z_i \mid 0 \leq i \leq g\rangle$, it happens that $\Delta\left(\mathbb{F}_q\left[X, Y\right], \omega_\Gamma, \varphi\right) = w\left(\Delta_{<_{wl}}\left(I_{\Gamma,q}\right)\right)$, where $\Delta_{<_{wl}}\left(I_{\Gamma,q}\right)$ is the footprint of $I_{\Gamma,q}$ with respect to the ordering $<_{wl}$.

Along this paper, this last set

$$\Delta_{\Gamma,q} := \Delta\left(\mathbb{F}_q\left[X, Y\right], \omega_\Gamma, \varphi\right)$$

will be called the Δ-*set* of Γ for q. And now, the problem of computing it is reduced to obtain the reduced Gröbner basis of $I_{\Gamma,q}$ with respect to $<_{wl}$ and, from it, to get the weights of the elements in the footprint of $I_{\Gamma,q}$. When $g = 1$, the footprint of $I_{\Gamma,q} = \langle Z_0^q - Z_0, Z_1^q - Z_1\rangle$ is the set

$$\Delta_{<_{wl}}\left(I_{\Gamma,q}\right) = \left\{Z_0^{b_0} Z_1^{b_1} \mid 0 \leq b_0, b_1 < q\right\}.$$

Hence, the Δ-set of Γ for q is $\Delta_{\Gamma,q} = \{b_0\gamma_0 + b_1\gamma_1 \mid 0 \leq b_0, b_1 < q\}$. We conclude this section with an example which reflects where the obstruction for the case $g > 1$ can appear.

Example 3.1. Let $\Gamma = \{\gamma_0, \gamma_1, \gamma_2\}$ be a δ-sequence with ν-vector (n_1), where we have set $a_{10} = a$, i.e. $n_1\gamma_1 = a\gamma_0$, and $n_1 = q = ma + r$ with $m > 0$ and $0 \leq r < a$. Suppose $\gamma_1 > \gamma_2$ and $m\gamma_1 \geq \left(a - r + 1\right)\gamma_0$. Then, with the above notations, the reduced Gröbner basis of $I_{\Gamma,q}$ with respect to the ordering $<_{wl}$ is

$$\mathcal{G} = \left\{\left(Z_1 - Z_2\right)^{m+1} - Z_0^{a-r+1}, Z_0^r\left(Z_1 - Z_2\right)^m - Z_0, Z_0^a - Z_1 + Z_2, Z_2^q - Z_2\right\}.$$

So, $\Delta_{<_{wl}}\left(I_{\Gamma,q}\right) = \left\{Z_0^t Z_1^u Z_2^v \mid t < a, u < m, v < q\right\} \cup \left\{Z_0^t Z_1^m Z_2^v \mid t < r, v < q\right\}$ and

$$\Delta_{\Gamma,q} = \left\{t\gamma_0 + u\gamma_1 + v\gamma_2 \mid t < a,\ u < m,\ v < q\right\} \cup \left\{t\gamma_0 + m\gamma_1 + v\gamma_2 \mid t < r,\ v < q\right\}.$$

For any δ-sequence Γ, the footprint of $I_{\Gamma,q}$ is a union of disjoint monomial blocks, that is, sets of the form

$$\mathbb{B}_{\mathbf{s}}^{\mathbf{t}} := \left\{Z^{\mathbf{b}} \ \mid\ s_i \leq b_i < t_i, 0 \leq i \leq g\right\}, \tag{5}$$

where $\mathbf{s} := (s_0, s_1, \ldots, s_g)$ and $\mathbf{t} := (t_0, t_1, \ldots, t_g)$ are fixed vectors in $\mathbb{N}^{g+1}$. When the footprint only contains a monomial block, good estimations of the parameters of the corresponding evaluation codes can be given. Next, we are going to introduce a class of δ-sequences satisfying this property.

3.2. **Evaluation codes defined by simple δ-sequences.** In this paragraph we keep the above notations.

Definition 3.2. A δ-sequence Γ is said to be *simple* if either $g = 1$ or otherwise $\gamma_i = n_{i+1}\gamma_{i+1}$ for $0 \leq i \leq g-2$ and $\gamma_{g-1} > \gamma_g$.

Two direct consequences of Definition 3.2 are:

1) $\gamma_i = \prod_{j=i+1}^{g-1} n_j \gamma_{g-1}$ for $0 \leq i \leq g-2$.

2) $I_\Gamma = \left\langle Z_1^{n_1} - Z_0 - Z_2, Z_2^{n_2} - Z_1 - Z_3, \ldots, Z_{g-1}^{n_{g-1}} - Z_{g-2} - Z_g \right\rangle$.

Examples of simple δ-sequences are those of the form

$$\Gamma = \{(n_1 n_2 \cdots n_{g-1}, n_1 n_2 \cdots n_{g-1}), (n_2 n_3 \cdots n_{g-1}, n_2 n_3 \cdots n_{g-1}), \ldots$$

$$\ldots, (n_{g-1}, n_{g-1}), (1,1), (1,0)\},$$

where the set $\{n_i\}_{i=1}^g$ contains positive integers $n_i \geq 2$ but $n_g > 2$. Notice that Γ can be defined from the δ-sequence in $\mathbb{N}$

$$\Gamma^* = \{n_1 n_2 \cdots n_g, n_2 n_3 \cdots n_g, \ldots, n_g, 1\}.$$

These sets span the semigroups at infinity of the so-called Abhyankar-Moh-Suzuki curves.

For a start, we study primary codes of maximal length defined by δ-sequences of two elements. This is the simplest case whose Δ-set has only one monomial block. Consider $\beta = b_0\gamma_0 + b_1\gamma_1 \in \Delta_{\Gamma,q}$, clearly $\sigma(\beta) = (q-b_0)(q-b_1)$. Write

$$\bar{H}_\beta = \left\{(u,v) \in \mathbb{N}_0^2 \mid u, v < q \text{ and } u\gamma_0 + v\gamma_1 \leq \beta\right\},$$

and *let $<_R$ be the lexicographical ordering on $\mathbb{N}_0^2$ with $(1,0) <_R (0,1)$*. Then the least value of the product $(q-u)(q-v)$ where (u,v) runs over $\bar{H}_\beta$ is reached for $(U,V) = \max_{<_R} \bar{H}_\beta$. Therefore, by Theorem 2.7, $d(E(\beta)) \geq (q-U)(q-V)$.

On the other hand, write $\mathbb{F}_q = \{l_0, l_1, \ldots, l_{q-1}\}$ and consider the polynomial $G = \prod_{i=0}^{U-1}(X - l_i)\prod_{i=0}^{V-1}(Y - l_i)$. Clearly $\varphi(G) \in E(\beta)$ and G has exactly $q^2 - (q-U)(q-V)$ zeros in $\mathbb{F}_q^2$. Hence, the weight of the codeword $\varphi(G)$ is $(q-U)(q-V)$, which proves

$$d(E(\beta)) = (q-U)(q-V).$$

The equality $\mu(\beta) = (b_0+1)(b_1+1)$ allows us to determine the minimum distance in the dual case:

$$d(C(\beta)) = (U+1)(V+1),$$

where $(U,V) = \min_{<_R} \hat{H}_\beta (:= \left\{(u,v) \in \mathbb{N}_0^2 \mid u, v < q \text{ and } u\gamma_0 + v\gamma_1 > \beta\right\})$.

Thus, we have proved the following result.

Proposition 3.3. *Let $\Gamma = \{\gamma_0, \gamma_1\}$ be a δ-sequence and keep the above notations. For any $\beta = b_0\gamma_0 + b_1\gamma_1 \in \Delta_{\Gamma,q}$, it holds that the minimum distances of the associated maximal length evaluation codes $E(\beta)$ and $C(\beta)$ satisfy:*

1) $d(E(\beta)) = (q-U)(q-V)$ *where* $(U,V) = \max_{<_R} \bar{H}_\beta$.
2) $d(C(\beta)) = (U+1)(V+1)$ *where* $(U,V) = \min_{<_R} \hat{H}_\beta$.

As a consequence, the evaluation codes of maximal length given by δ-sequences of two elements reach the Feng-Rao bounds in both primary and dual cases. Moreover, every dual code is a primary one associated with the same δ-sequence. In fact, set $\Delta_{\Gamma,q} = \left\{s_1 < s_2 < \cdots < s_{q^2}\right\}$, where $<$ denotes the ordering on S_Γ, and $s_i = b_{i0}\gamma_0 + b_{i1}\gamma_1$, then $C(s_k) = E\left(s_{q^2-k}\right)$.

Next, we will show how to adapt the former ideas to codes of maximal length defined by arbitrary simple δ-sequences. Below, we state that, under certain conditions, simple δ-sequences are the only ones whose footprint has only one monomial block. In the following, we will assume that $g \geq 2$ and we will stand $\mathbf{0}$ for the zero-vector and $\mathbf{B} := (B_0, B_1, \ldots, B_g)$ for another different vector, both in $\mathbb{N}_0^{g+1}$.

Proposition 3.4. *Let $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\}$ be a δ-sequence with ν-vector $\underline{n}$ and such that $\gamma_0 > \gamma_1 > \cdots > \gamma_g$. Suppose that $q \geq \max\{n_i \mid 1 \leq i \leq g-1\}$. Then, the footprint of the ideal $I_{\Gamma,q}$, with respect to the ordering $<_{wl}$, has only one monomial block of the form $\mathbb{B}_{\mathbf{0}}^{\mathbf{B}}$ if, and only if, Γ is simple and q a multiple of n_i for $1 \leq i \leq g-1$.*

Proof. Suppose that q is a power of a prime number p and $\Delta_{<_{wl}}(I_{\Gamma,q}) = \mathbb{B}_{\mathbf{0}}^{\mathbf{B}}$. Then, by [8, 9] $\#\Delta_{<_{wl}}(I_{\Gamma,q}) = \prod_{i=0}^{g} B_i = q^2$ because $I_{\Gamma,q}$ is a radical ideal. So B_i is a power of p for all index i. The set of leading monomials of the elements in the reduced Gröbner basis, $\mathcal{G}$, of $I_{\Gamma,q}$ with respect to $<_{wl}$ is $\left\{Z_0^{B_0}, Z_1^{B_1}, \ldots, Z_g^{B_g}\right\}$. Set $SP(F,G)$ the S-polynomial of two polynomials F and G and, for $1 \leq i \leq g-1$, define

$$S_i := SP\left(Z_i^{n_i} - \prod_{j=0}^{i-1} Z_j^{a_{ij}} - Z_{i+1}, Z_i^q - Z_i\right) = Z_i^{q-n_i}\left(\prod_{j=0}^{i-1} Z_j^{a_{ij}} + Z_{i+1}\right) - Z_i,$$

where the a_{ij}'s are those coefficients appearing in the equality (1). Write $q = k_i n_i + r_i$ $(0 \leq r_i < n_i)$ and $\to$ the relation of reduction modulo $I_{\Gamma,q}$, then

$$S_i \to Z_i^{r_i}\left(\prod_{j=0}^{i-1} Z_j^{a_{ij}} + Z_{i+1}\right)^{k_i} - Z_i.$$

Let us see that $r_i = 0$ for all i. By contradiction, if we assume $r_i > 0$ then, the leading monomial of the remainder of S_i modulo $I_{\Gamma,q}$ will yield, via Buchberger's algorithm, a polynomial in $\mathcal{G}$ whose leading monomial is a product of more than one power $Z_j^{b_j}$ because not all values a_{ij} equal zero. Therefore this leading monomial is different from $Z_j^{B_j}$, which gives the desired contradiction. So $r_i = 0$, which implies that, for $1 \leq i \leq g-1$, q is multiple of n_i and n_i and k_i are powers of p.

Now, $S_1 \to (Z_0^{a_{10}} + Z_2)^{k_1} - Z_1 = Z_0^{k_1 a_{10}} - Z_1 + Z_2^{k_1}$ and

$$SP\left(Z_0^{k_1 a_{10}} - Z_1 + Z_2^{k_1}, Z_0^q - Z_0\right) \to Z_0^{s_1}\left(Z_1 - Z_2^{k_1}\right)^{m_1} - Z_0,$$

where we have set $q = k_1 a_{10} m_1 + s_1$ and $0 \leq s_1 < k_1 a_{10}$. Reasoning as in the above paragraph, $s_1 = 0$ and so $a_{10} m_1 = n_1$. Hence a_{10} is a power of p and, as it is co-prime with n_1 (see (1), again), we have that $a_{10} = 1$ and $m_1 = n_1$. Then $\gamma_0 = n_1\gamma_1$.

Let us prove that $\gamma_1 = n_2\gamma_2$. Assume $a_{20} > 0$. If $a_{21} = 0$, then considering a δ-sequence in $\mathbb{N}$, $\Gamma^* = \{\gamma_i^*\}_{i=0}^g$, that determines Γ and its attached values $\{n_i\}_{i=0}^g$, it happens, on the one hand, that $d_3 = n_3n_4\cdots n_g$ holds. On the other hand $n_2\gamma_2^* = a_{20}\gamma_0^*$ implies $d_3 = z\ n_3n_4\cdots n_g$, where $z = \gcd(n_1n_2, n_2, a_{20}n_1)$, which is a contradiction because the values n_i are powers of p. Then $a_{20} > 0$ implies $a_{21} > 0$ which cannot happen by the monomial structure of $\Delta_{<_{wl}}(I_{\Gamma,q})$. So $a_{20} = 0$ and a similar argument to the previous one, with S_2 instead of S_1, proves $a_{21} = 1$ and thus $\gamma_1 = n_2\gamma_2$. Finally, by extending inductively this reasoning for $2 \leq i \leq g-1$, we get

$$a_{i0} = a_{i1} = \cdots = a_{i,i-2} = 0 \text{ and } a_{i,i-1} = 1,$$

and this proves $\gamma_i = n_{i+1}\gamma_{i+1}$ for $0 \leq i \leq g-2$.

We have just shown an implication. For the converse, we will apply induction on g. For $g = 2$, with the above notation and taking into account that

$$SP\left(Z_1^{n_1} - Z_0 - Z_2, Z_1^q - Z_1\right) \to Z_0^{k_1} - Z_1 + Z_2^{k_1}$$

and

$$SP\left(Z_0^{k_1} - Z_1 + Z_2^{k_1}, Z_0^q - Z_0\right) \to Z_1^{n_1} - Z_2^q - Z_0 =$$

$$= (Z_1^{n_1} - Z_0 - Z_2) - (Z_2^q - Z_2) \to 0,$$

it happens that the reduced Gröbner basis of $I_{\Gamma,q}$ with respect to $<_{wl}$ is

$$\mathcal{G} = \left\{Z_0^{k_1} - Z_1 + Z_2^{k_1}, Z_1^{n_1} - Z_0 - Z_2, Z_2^q - Z_2\right\},$$

hence $\Delta_{<_{wl}}(I_{\Gamma,q})$ has only one monomial block with $B_0 = k_1$, $B_1 = n_1$ and $B_2 = q$.

Now, let $\Gamma = \{\gamma_0, \ldots, \gamma_g\}$ be a simple δ-sequence as in the statement and consider the δ-sequence $\Gamma' = \{\gamma_1, \gamma_2, \ldots, \gamma_g\}$ (see Lemma 2.5). By induction hypothesis, $\Delta_{<_{wl}}\left(I_{\Gamma',q}\right)$ contains only one monomial block. Let $\mathcal{G}'$ be the reduced Gröbner basis of $I_{\Gamma',q}$ with respect to the corresponding ordering and suppose that the set of leading monomials of $\mathcal{G}'$ is $\left\{Z_1^{B_1}, Z_2^{B_2}, \ldots, Z_g^{B_g}\right\}$, with $B_1B_2\cdots B_g = q^2$. It is clear that

$$I_{\Gamma,q} = \left\langle \mathcal{G}' \cup \{Z_1^{n_1} - Z_0 - Z_2, Z_0^q - Z_0\}\right\rangle.$$

Let $T = Z_1^{B_1} + H$ be the polynomial of $\mathcal{G}'$ with leading monomial $Z_1^{B_1}$ and consider the S-polynomial $S := SP\left(Z_1^{n_1} - Z_0 - Z_2, T\right)$.

Suppose that $n_1 \leq B_1$ and write $B_1 = k\ n_1$, where k is a power of p. Then $S \to Z_0^k + Z_2^k + H$. Moreover,

$$SP\left(Z_0^k + Z_2^k + H, Z_0^q - Z_0\right) \to Z_2^q + H^m + Z_0 \to \left(Z_0^k + Z_2^k + H\right)^m - (Z_0^q - Z_0) \to 0,$$

where $q = k\ m$. Hence, $\mathcal{G} = \left\{Z_0^k + Z_2^k + H, Z_1^{n_1} - Z_0 - Z_2\right\} \cup (\mathcal{G}' - \{T\})$ and, thus, the set of leading monomials of $\mathcal{G}$ is $\left\{Z_0^k, Z_1^{n_1}, Z_2^{B_2}, \ldots, Z_g^{B_g}\right\}$.

Otherwise, $n_1 > B_1$, and so $S \to Z_0 + Z_2 + H^l$, where $n_1 = l\ B_1$. The leading monomial of the polynomial $Z_0 + Z_2 + H^l$ is Z_0 because

$$w(Z_0) = \gamma_0 = l\ B_1\gamma_1 > l\ w(H) = w\left(H^l\right).$$

Moreover,

$$SP\left(Z_0+Z_2+H^l, Z_0^q-Z_0\right)\to Z_2^q+H^{ql}+Z_0\to (Z_2^q-Z_2)+\left(Z_0+Z_2+H^l\right)\to 0.$$

Therefore, $\mathcal{G}=\left\{Z_0+Z_2+H^l\right\}\cup\mathcal{G}'$ and the set of leading monomials of $\mathcal{G}$ is

$$\left\{Z_0, Z_1^{B_1}, Z_2^{B_2}, \ldots, Z_g^{B_g}\right\},$$

which concludes the proof. □

As a consequence of the above proof, we state the following algorithm. It computes the vector $\mathbf{B}$ that determines the footprint $\Delta_{<_{wl}}(I_{\Gamma,q})$ of the ideal $I_{\Gamma,q}$ given by a simple δ-sequence Γ. Γ must satisfy that any coordinate n_i of its ν-vector divides q.

Algorithm 1.
Input: q, g, $n_1,\ldots,n_{g-1}$.

$B_g=q$,
$B_{g-1}=n_{g-1}$,
$i=g-2$,
While $i\geq 1$ **do**:
  If $n_iB_{i+1}\cdots B_{g-1}\leq q$ **then** $B_i=n_i$
  else $B_i=q/\left(B_{i+1}\cdots B_{g-1}\right)$,
  $i=i-1$,
$B_0=q/\left(B_1\cdots B_{g-1}\right)$.

Output: $B_0, B_1, \ldots, B_g$.

The following result will be useful further on.

Lemma 3.5. *Let $\Gamma=\{\gamma_0,\gamma_1,\ldots,\gamma_g\}$ be a simple δ-sequence whose ν-vector is $\underline{n}$. Suppose that $q=\prod_{i=0}^{g-1}n_i$ with $n_0\geq 1$. Then:*

(1) *The reduced Gröbner basis of the ideal $I_{\Gamma,q}$ with respect to the ordering $<_{wl}$ is*

$$\mathcal{G}=\left\{Z_0^{n_0}-Z_{g-1}+Z_2^{n_0}+Z_3^{n_0n_1}+\cdots+Z_g^{n_0n_1\cdots n_{g-2}}, Z_1^{n_1}-Z_0-Z_2,\right.$$
$$\left.Z_2^{n_2}-Z_1-Z_3,\ldots,Z_{g-1}^{n_{g-1}}-Z_{g-2}-Z_g, Z_g^q-Z_g\right\}.$$

(2) *The reduced Gröbner basis, with respect to $<_{wl}$, of the ideal of the ring of polynomials $\mathbb{F}_q[Z_0,Z_1,\ldots,Z_g]$:*

$$J:=\left\langle Z_1^{n_1}-Z_0, Z_2^{n_2}-Z_1,\ldots,Z_{g-1}^{n_{g-1}}-Z_{g-2}, Z_0^q-Z_0,\ldots,Z_g^q-Z_g\right\rangle$$

is

$$\left\{Z_0^{n_0}-Z_{g-1}, Z_1^{n_1}-Z_0, Z_2^{n_2}-Z_1,\ldots,Z_{g-1}^{n_{g-1}}-Z_{g-2}, Z_g^q-Z_g\right\}.$$

Proof. We reason by induction on g to prove Item (1). The case $g=1$ is obvious and the case $g=2$ was demonstrated in the proof of Proposition 3.4. So, suppose that Item (1) holds for $g=k-1\geq 2$. Set

$$I_{\Gamma,q}=\left\langle Z_1^{n_1}-Z_0-Z_2,\ldots,Z_{k-1}^{n_{k-1}}-Z_{k-2}-Z_k, Z_0^q-Z_0,\ldots,Z_k^q-Z_k\right\rangle$$

the ideal given by the simple δ-sequence $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_k\}$. Then, by Lemma 2.5,

$$J_{\Gamma',q} = \left\langle Z_2^{n_2} - Z_1 - Z_3, \ldots, Z_{k-1}^{n_{k-1}} - Z_{k-2} - Z_k, Z_1^q - Z_1, \ldots, Z_k^q - Z_k \right\rangle$$

is the ideal determined by the simple δ-sequence $\Gamma' = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}$. By induction hypothesis, the reduced Gröbner basis of $J_{\Gamma',q}$, with respect to the ordering $<_{wl}$, is

$$\mathcal{B} = \left\{ Z_1^{n_0 n_1} - Z_{k-1} + Z_3^{n_0 n_1} + \cdots + Z_k^{n_0 n_1 \cdots n_{k-2}}, Z_2^{n_2} - Z_1 - Z_3, \ldots \right.$$

$$\left. Z_{k-1}^{n_{k-1}} - Z_{k-2} - Z_k, Z_k^q - Z_k \right\},$$

hence, $I_{\Gamma,q} = \langle \{Z_1^{n_1} - Z_0 - Z_2, Z_0^q - Z_0\} \cup \mathcal{B} \rangle$. Now, consider the following S-polynomials and reduction modulo $I_{\Gamma,q}$:

$$SP\left(Z_1^{n_1} - Z_0 - Z_2, Z_1^{n_0 n_1} - Z_{k-1} + Z_3^{n_0 n_1} + \cdots + Z_k^{n_0 n_1 \cdots n_{k-2}}\right) =$$

$$Z_0^{n_0} - Z_{k-1} + Z_2^{n_0} + Z_3^{n_0 n_1} + \cdots + Z_k^{n_0 n_1 \cdots n_{k-2}},$$

$$SP\left(Z_0^{n_0} - Z_{k-1} + Z_2^{n_0} + Z_3^{n_0 n_1} + \cdots + Z_k^{n_0 n_1 \cdots n_{k-2}}, Z_0^q - Z_0\right) =$$

$$\left(Z_2^{n_0} + Z_3^{n_0 n_1} + \cdots + Z_k^{n_0 n_1 \cdots n_{k-2}} - Z_{k-1}\right)^{n_0 n_1 \cdots n_{k-1}} + Z_0 \to$$

$$\left(Z_2^{n_0 n_{k-1}} + Z_3^{n_0 n_1 n_{k-1}} + \cdots + Z_{k-1}^{n_0 n_1 \cdots n_{k-3} n_{k-1}} - Z_{k-2}\right)^{n_0 n_1 \cdots n_{k-2}} + Z_0.$$

Iterating the procedure, we get the S-polynomial and the reduction

$$\left(Z_2^{n_0 n_2 \cdots n_{k-1}} - Z_1\right)^{n_1} + Z_0 = Z_2^q - Z_1^{n_1} + Z_0 \to 0,$$

which proves Item (1) by applying Buchberger's algorithm.

Now we prove Item (2). We also reason by induction on g. The case $g = 1$ is also clear. So, we assume that it holds for $g = k - 1 \geq 1$. By induction hypothesis, the reduced Gröbner basis of the ideal

$$\langle Z_1^{n_1} - Z_0, Z_2^{n_2} - Z_1, \ldots, Z_{k-1}^{n_{k-1}} - Z_{k-2}, Z_0^q - Z_0, \ldots, Z_k^q - Z_k \rangle$$

is the reduced Gröbner basis of

$$\langle Z_1^{n_1} - Z_0, Z_0^q - Z_0, Z_1^{n_0 n_1} - Z_{k-1}, Z_2^{n_2} - Z_1, \ldots, Z_{k-1}^{n_{k-1}} - Z_{k-2}, Z_k^q - Z_k \rangle.$$

Then, consider the following S-polynomials and reductions:

$$SP(Z_1^{n_1} - Z_0, Z_1^{n_0 n_1} - Z_{k-1}) = Z_0 Z_1^{n_0 n_1 - n_1} - Z_{k-1} \to Z_0^{n_0} - Z_{k-1},$$

where we have divided repeatedly by $Z_1^{n_1} - Z_0$,

$$SP(Z_0^{n_0} - Z_{k-1}, Z_0^q - Z_0) = Z_0^{q-n_0} Z_{k-1} - Z_0 \to Z_{k-1}^{n_1 n_2 \cdots n_{k-1}} - Z_0,$$

after dividing repeatedly by $Z_0^{n_0} - Z_{k-1}$. Then, from the above right hand side, we obtain the reduction $\to Z_{k-2}^{n_1 n_2 \cdots n_{k-2}} - Z_0$ (dividing by $Z_{k-1}^{n_{k-1}} - Z_{k-2}$) and, after several steps, a similar iterative procedure gives $\to Z_1^{n_1} - Z_0 \to 0$, which concludes the proof. □

Proposition 3.4 and Algorithm 1 allow us to get Feng-Rao bounds for evaluation codes defined by simple δ-sequences. Let us see it.

Proposition 3.6. *Let $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\}$ be a simple δ-sequence whose ν-vector is $\underline{n}$. Suppose that the prime power q is a multiple of n_i for $1 \leq i \leq g-1$. Then, the Δ-set $\Delta_{\Gamma,q}$ equals $\{\sum_{i=0}^{g} b_i\gamma_i \mid 0 \leq b_i < B_i \text{ for } 0 \leq i \leq g\}$, where the values B_i, $0 \leq i \leq g$, are the exponents computed by Algorithm 1. Moreover, let $\beta \in \Delta_{\Gamma,q}$, then the minimum distances of the associated maximal length evaluation codes $E(\beta)$ and $C(\beta)$ satisfy:*

$$d\left(E\left(\beta\right)\right) \geq \min\left\{\prod_{i=0}^{g}\left(B_i - b_i\right) \mid \eta = \sum_{i=0}^{g} b_i\gamma_i \in \Delta\left(\mathbb{F}_q\left[X,Y\right],\omega,\varphi\right) \text{ and } \eta \leq \beta\right\}$$

and

$$d\left(C\left(\beta\right)\right) \geq \min\left\{\prod_{i=0}^{g}\left(b_i + 1\right) \mid \eta = \sum_{i=0}^{g} b_i\gamma_i \in \Delta\left(\mathbb{F}_q\left[X,Y\right],\omega,\varphi\right) \text{ and } \eta > \beta\right\}.$$

We have seen that these bounds are reached when $g = 1$, however, in the general case, it is not true. The main goal in this section is to see that, for large enough values of q, the primary Feng-Rao (or Andersen-Geil) bound of the primary codes defined by simple δ-sequences can be improved. Before to state it, we need some consequences of the notion of simple δ-sequence and, to show them, we will use the following result.

Lemma 3.7. *Consider $N_1, N_2, \ldots, N_{t-1} \in \mathbb{N}$ and $r \in \mathbb{N}_0$. Then, r can be expressed in a unique way as*

$$r = r_1 + r_2N_1 + r_3N_1N_2 + \cdots + r_{t-1}N_1N_2\cdots N_{t-2} + r_tN_1N_2\cdots N_{t-1},$$

where $0 \leq r_i < N_i$ for $1 \leq i \leq t-1$.

Proof. The proof follows after dividing (Euclidean division) r by N_1 and the successively obtained quotients by the corresponding N_i, $2 \leq i \leq t-1$. □

In the sequel, the previous stated equality will be expressed as $\psi_{(N_1,N_2,\ldots,N_{t-1})}(r) = (r_1, r_2, \ldots, r_t)$ and $r_i = \psi^i_{(N_1,N_2,\ldots,N_{t-1})}(r)$, $1 \leq i \leq t$.

Proposition 3.8. *Let Γ be as in Proposition 3.6. Then $\Lambda = \{\gamma_{g-1}, \gamma_g\}$ is a δ-sequence, and $\Delta_{\Gamma,q} = \Delta_{\Lambda,q}$ whenever $q \geq \prod_{i=1}^{g-1} n_i$.*

Proof. By Lemma 2.5, it is clear that Λ is a δ-sequence. Thus, it suffices to see that $\Delta_{\Lambda,q} \subseteq \Delta_{\Gamma,q}$ because both sets have the same cardinality. Indeed, let $\beta = b\gamma_{g-1} + e\gamma_g \in \Delta_{\Lambda,q}$ and consider the unique vector $\psi_{(n_{g-1},\ldots,n_2,n_1)}(b) = (b_{g-1}, \ldots, b_1, b_0)$ attached to b by Lemma 3.7. Here, $b_i < n_i$ for $1 \leq i \leq g-1$ and $b_0 < n_0$ holds as a consequence of the facts $b < q$ and $\prod_{i=0}^{g-1} n_i = q$. By using item 1) given below Definition 3.2, it happens that $\beta = \sum_{i=0}^{g} b_i\gamma_i \in \Delta_{\Gamma,q}$, where $b_g = e$, which finishes the proof. □

Again, let $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_g\}$ be a simple δ-sequence with ν vector $\underline{n}$. Recall Lemma 3.7 and for $u \in \mathbb{N}_0$, set $u_i := \psi^{g-i}_{(n_{g-1},\ldots,n_2,n_1)}(u)$, $0 \leq i \leq g-1$. Then, $u = u_0\prod_{i=1}^{g-1} n_i + u_1\prod_{i=2}^{g-1} n_i + \cdots + u_{g-2}n_{g-1} + u_{g-1}$, with $u_i < n_i$ for $1 \leq i \leq g-1$. Now, we are ready to state and prove our main results.

Theorem 3.9. *Let Γ, $\underline{n}$ and u be as above. Suppose that q is a multiple of n_i for $1 \leq i \leq g-1$ and $q \geq \prod_{i=1}^{g-1} n_i$. Let $\beta \in \Delta_{\Gamma,q}$. Then, the minimum distance of the associated maximal length primary code $E(\beta)$ satisfies:*

$$d\left(E\left(\beta\right)\right) \geq \left(q-U\right)\left(q-V\right),$$

where $(U,V) = \max_{<_R} \bar{H}_\beta$ and

$$\bar{H}_\beta := \left\{ (u,v) \mid \eta = \left(\sum_{i=0}^{g-1} u_i \gamma_i \right) + v\gamma_g \in \Delta_{\Gamma,q},\ \eta \leq \beta \right\}.$$

Proof. Proposition 3.8 and its proof show that $\Lambda = \{\gamma_{g-1}, \gamma_g\}$ is a δ-sequence such that $\Delta_{\Lambda,q} = \Delta_{\Gamma,q}$ and, moreover,

$$\bar{H}_\beta = \left\{ (u,v) \mid \eta = u\gamma_{g-1} + v\gamma_g \in \Delta_{\Lambda,q},\ \eta \leq \beta \right\}.$$

Denote by $\varphi_\Gamma : \mathbb{F}_q[X,Y] \to \mathbb{F}_q^{q^2}$ the map giving the family of codes $E(\beta)$ and set $\{Q_i\}_{i=0}^g$ the approximates defined by Γ. Pick a nonzero word $\mathbf{c} = \varphi_\Gamma(F)$, $F = F(X,Y) \in \mathbb{F}_q[X,Y]$ and regard F as a polynomial in $\mathbb{F}_q\left[Q_0, Q_1, \ldots, Q_g\right]$, that is,

$$F\left(X,Y\right) = F\left(Q_0, Q_1, \ldots, Q_g\right) = \sum_{\eta = \sum_{i=0}^g s_i\gamma_i \in \Delta_{\Gamma,q},\ \eta \leq \beta} \lambda_\eta Q_0^{s_0} Q_1^{s_1} \cdots Q_g^{s_g}.$$

Consider the polynomial

$$G\left(X,Y\right) = F\left(X^{\prod_{i=1}^{g-1} n_i}, X^{\prod_{i=2}^{g-1} n_i}, \ldots, X^{n_{g-2}n_{g-1}}, X^{n_{g-1}}, X, Y\right).$$

If we denote $\{E_\Lambda(\beta)\}$ the family of codes of maximal length given by the δ-sequence Λ with corresponding weight function ω_Λ, then it holds

$$\omega_\Lambda\left(G\right) \leq \left(b_0 \prod_{i=1}^{g-1} n_i + b_1 \prod_{i=2}^{g-1} n_i + \cdots + b_{g-1} \right) \gamma_{g-1} + b_g\gamma_g = \beta.$$

So, $\mathbf{e} = \varphi_\Gamma(G) \in E_\Lambda(\beta)$.

Let Z_F (respectively, Z_G) be the set of zeros of the polynomial F (respectively, G) in $\mathbb{F}_q^2$. Consider the ideals of the ring $\mathbb{F}_q\left[Q_0, Q_1, \ldots, Q_g\right]$:

$$I = \left\langle F\left(Q_0, Q_1, \ldots, Q_g\right), Q_1^{n_1} - Q_0 - Q_2, Q_2^{n_2} - Q_1 - Q_3, \ldots, Q_{g-1}^{n_{g-1}} - Q_{g-2} - Q_g \right\rangle$$

and

$$J = \left\langle F\left(Q_0, Q_1, \ldots, Q_g\right), Q_1^{n_1} - Q_0, Q_2^{n_2} - Q_1, \ldots, Q_{g-1}^{n_{g-1}} - Q_{g-2} \right\rangle.$$

Then, $Z_F = \left\{ (u_0, u_1) \mid (u_0, u_1, \ldots, u_g) \in \mathbb{V}_{\mathbb{F}_q}\left(I\right) \right\}$ and

$$Z_G = \left\{ (u_{g-1}, u_g) \mid (u_0, u_1, \ldots, u_g) \in \mathbb{V}_{\mathbb{F}_q}\left(J\right) \right\}.$$

Hence, $\#Z_F = \#\mathbb{V}_{\mathbb{F}_q}\left(I\right)$ and $\#Z_G = \#\mathbb{V}_{\mathbb{F}_q}\left(J\right)$.

Now, set $I_q = I + R_q$ and $J_q = J + R_q$, where $R_q := \langle Q_0^q - Q_0, Q_1^q - Q_1, \ldots, Q_g^q - Q_g \rangle$. Thus $\#Z_F = \#\mathbb{V}_{\mathbb{F}_q}\left(I\right) = \#\mathbb{V}_{\mathbb{F}_q}\left(I_q\right) = \#\Delta_<\left(I_q\right)$ and an analogous equality happens for J and J_q, $<$ being any monomial ordering in $\mathbb{F}_q\left[Q_0, Q_1, \ldots, Q_g\right]$.

Consider the reduced Gröbner bases of I_q and J_q with respect to the weighted degree lexicographic ordering $<=<_{wl}$ with $w(Q_i)=\gamma_i$, for $0\leq i\leq g$. Write $q=\prod_{i=0}^{g-1}n_i$, where $n_0\geq 1$. By Lemma 3.5, we have that

$$I_q=\langle F(Q_0,Q_1,\ldots,Q_g),Q_0^{n_0}-Q_{g-1}+Q_2^{n_0}+Q_3^{n_0n_1}+\cdots+Q_g^{n_0n_1\cdots n_{g-2}},$$

$$Q_1^{n_1}-Q_0-Q_2,\ldots,Q_{g-1}^{n_{g-1}}-Q_{g-2}-Q_g,Q_g^q-Q_g\rangle,$$

and

$$J_q=\left\langle F(Q_0,Q_1,\ldots,Q_g),Q_0^{n_0}-Q_{g-1},Q_1^{n_1}-Q_0,\ldots,Q_{g-1}^{n_{g-1}}-Q_{g-2},Q_g^q-Q_g\right\rangle.$$

Notice that for every generator above showed S of the ideal I_q (respectively, J_q) there exists a unique generator T of J_q (respectively, I_q) such that $S=T+H$, where $w(S)=w(T)>w(H)$. When applying the Buchberger's algorithm in order to compute the reduced Gröbner bases of I_q and J_q with respect to $<_{wl}$, we will only need to consider the S-polynomials derived from F. By the above arguments, every S-polynomial of generators of I_q (respectively, J_q) contains, as a summand, the S-polynomial of the corresponding generators of J_q (respectively, I_q). Inductively we get that if S_1 and S_2 are elements from the set obtained in the kth iteration of the Buchberger's algorithm for I_q, then there exist elements T_1 and T_2 taken from the set obtained in the kth iteration of the Buchberger's algorithm for J_q such that $S_1=T_1+H_1$ and $S_2=T_2+H_2$, where $w(S_i)=w(T_i)>w(H_i)$ for $i=1,2$. Thus, $SP(S_1,S_2)=SP(T_1,T_2)+H$, where H depends on H_1 and H_2. Moreover, $SP(S_1,S_2)\to 0$ in the kth iteration of the Buchberger's algorithm for I_q if, and only if, $SP(T_1,T_2)\to 0$ in this iteration of the Buchberger's algorithm for J_q. So, the reduced Gröbner bases of I_q and J_q with respect to $<_{wl}$, have the same size and their sets of leading monomials are equal. Therefore, $\Delta_{<_{wl}}(I_q)=\Delta_{<_{wl}}(J_q)$ and $\#Z_F=\#Z_G$. Hence, we have that

$$\mathrm{wt}(\mathbf{c})=q^2-\#Z_F=q^2-\#Z_G=\mathrm{wt}(\mathbf{e})\geq(q-U)(q-V),$$

where the inequality holds by Proposition 3.3 and then, $d(E(\beta))\geq(q-U)(q-V)$. □

Theorem 3.10. *The bound on the minimum distance of the primary codes given in Theorem 3.9 is at least as good as the primary Feng-Rao one.*

Proof. The case when $g=1$ is clear because, by Proposition 3.3, both bounds are equal and they are reached.

Assume $g\geq 2$ and let $\beta\in\Delta_{\Gamma,q}$ and $(U,V)=\max_{<_R}\bar{H}_\beta$ be. Without loss of generality, we can suppose $q=\prod_{i=0}^{g-1}n_i$, where $n_0\geq 1$. Recall that q is a prime power and this is an important fact (see the proof of Proposition 3.4). By Theorem 3.9, $d(E(\beta))\geq(q-U)(q-V)$. Write $\psi_{(n_{g-1},\ldots,n_2,n_1)}(U)=(u_{g-1},\ldots,u_1,u_0)$ by Lemma 3.7. Then $\sum_{i=0}^{g}u_i\gamma_i\leq\beta$, where $u_g=V$. To prove the result, it suffices to see that $q-U\geq\prod_{i=0}^{g-1}(n_i-u_i)$, because then

$$(q-U)(q-V)\geq\prod_{i=0}^{g}(n_i-u_i)\geq$$

$$\geq \min\left\{\prod_{i=0}^{g}(n_i - s_i) \mid \eta = \sum_{i=0}^{g} s_i\gamma_i \in \Delta_{\Gamma,q} \text{ and } \eta \leq \beta\right\},$$

which concludes the proof.

Let us show, by induction, the mentioned inequality. For a start, when $g = 2$ one gets

$$(n_0 - u_0)(n_1 - u_1) = n_0n_1 - u_0n_1 - (n_0 - u_0)u_1 \leq n_0n_1 - u_0n_1 - u_1 = q - U.$$

Now, consider an index $2 \leq k < g - 1$ and set

$$W_k = \prod_{i=0}^{k} n_i - u_0\prod_{i=1}^{k} n_i - \cdots - u_{k-1}n_k - u_k.$$

By induction hypothesis, suppose that $\prod_{i=0}^{k}(n_i - u_i) \leq q - U = W_k$ holds, then

$$\prod_{i=0}^{k+1}(n_i - u_i) \leq \prod_{i=0}^{k+1} n_i - u_0\prod_{i=1}^{k+1} n_i - \cdots - u_kn_{k+1} - W_ku_{k+1} \leq$$

$$\leq \prod_{i=0}^{k+1} n_i - u_0\prod_{i=1}^{k+1} n_i - u_1\prod_{i=2}^{k+1} n_i \cdots - u_kn_{k+1} - u_{k+1},$$

which concludes the proof. □

Remark 3.11. In this remark we show that our bound is reached when $g = 2$. Keep the above notations and consider a simple δ-sequence $\Gamma = \{\gamma_0, \gamma_1, \gamma_2\}$ with $\gamma_0 = n_1\gamma_1$ and $q = n_0n_1$, $n_0 \geq 1$. Let $\beta = b_0\gamma_0 + b_1\gamma_1 + b_2\gamma_2$, with $b_i < n_i$ for $0 \leq i \leq 2$ and $n_2 = q$. Write $\mathbb{F}_q = \{l_0, l_1, \ldots, l_{q-1}\}$ and consider the polynomial

$$F = \prod_{i=0}^{U-1}(Y - l_i) \cdot \prod_{i=0}^{V-1}(Y^{n_1} - X - l_i).$$

Then, our assertion is proved because $\varphi_\Gamma(F) \in E(\beta)$ and the set of zeros of F in $\mathbb{F}_q^2$ is

$$\{(l_i, l_j) \mid 0 \leq i \leq q-1,\ 0 \leq j \leq U-1\} \cup \left\{\left(l_i + l_j^{n_1}, l_j\right) \mid 0 \leq i \leq V-1,\ U \leq j \leq q-1\right\},$$

whose cardinality is $qU + qV - UV$.

We end this section with an example which shows that our bound improves the primary Feng-Rao one in some cases.

Example 3.12. Consider the δ-sequence $\Gamma = \{(64, 0), (8, 0), (1, 0), (1, -1)\}$. According to our notation set $\Lambda = \{(1, 0), (1, -1)\}$. The ν-vector of Γ is $(8, 8)$. Write $q = 256$ and pick $\beta = (140, -128) \in \Delta_{\Gamma,q}$. Since

$$\beta = 0 \cdot (64, 0) + 1 \cdot (8, 0) + 4 \cdot (1, 0) + 128 \cdot (1, -1),$$

the primary Feng-Rao bound of the code $E(\beta)$ is less than or equal to

$$(4 - 0)(8 - 1)(8 - 4)(256 - 128) = 14336.$$

Finally, the fact that β can be expressed as $\beta = 12 \cdot (1, 0) + 128 \cdot (1, -1)$ and the equality $(0, 140) = \max_{<_R} \bar{H}_\beta$ show that the bound on the minimum distance of $E(\beta)$ in Theorem 3.9 is $(256 - 0)(256 - 140) = 29696$.

4. Parameters

We devote this section to the study of the performance of families of primary codes of maximal length defined by simple δ-sequences.

Firstly, we are going to compare the behavior of those families defined by δ-sequences of two elements. We will see that $\mathfrak{G} = \{(1,0),(1,-1)\}$ provides the best one. Fix a field $\mathbb{F}_q$ and consider a δ-sequence $\Gamma = \{\gamma_0 = (s_0, s_1), \gamma_1 = (t_0, t_1)\}$. Write $\Delta_{\Gamma,q} = \left\{\alpha_1, \alpha_2, \ldots, \alpha_{q^2}\right\}$ with $\alpha_i < \alpha_{i+1}$ for $1 \leq i \leq q^2 - 1$ and set $\mathcal{E}_\Gamma = \left\{E(\alpha_i) \mid 1 \leq i \leq q^2\right\}$ the family of primary codes (of maximal length) determined by Γ. Clearly, the sequence $\{d(E(\alpha_i))\}_{i=1}^{q^2}$ is decreasing and, as a consequence of Proposition 3.3, the jumps in this sequence occur for elements of the form $U\gamma_0 + V\gamma_1 \in \Delta_{\Gamma,q}$, where $(U,V) = \max_{<_R} \bar{H}_\alpha$, for some $\alpha \in \Delta_{\Gamma,q}$. Thus, the mentioned jumping set is

$$\Lambda_{\Gamma,q} = \{\beta_{b+c+1} = b\gamma_0 + c\gamma_1 \mid (b,c) \in L\},$$

where $L = \{(0,i) \mid 0 \leq i \leq q-1\} \cup \{(i,q-1) \mid 1 \leq i \leq q-1\}$. Let $\mathcal{E}_{\Gamma_1}, \mathcal{E}_{\Gamma_2}$ be two families of primary codes corresponding to the δ-sequences $\Gamma_1 = \{\gamma_{10}, \gamma_{11}\}$ and $\Gamma_2 = \{\gamma_{20}, \gamma_{21}\}$, then the minimum distance of the codes $E(b\gamma_{10} + c\gamma_{11}) \in \mathcal{E}_{\Gamma_1}$ and $E(b\gamma_{20} + c\gamma_{21}) \in \mathcal{E}_{\Gamma_2}$, $(b,c) \in L$, is equal to $(q-b)(q-c)$. So, to compare these families, we say that $\mathcal{E}_{\Gamma_1}$ is better than or equal to $\mathcal{E}_{\Gamma_2}$ if $\dim E(b\gamma_{10} + c\gamma_{11}) \geq \dim E(b\gamma_{20} + c\gamma_{21})$ for all $(b,c) \in L$.

Let us see what happens with these dimensions. On the one hand, suppose that $\beta = \beta_{k+1} = k\gamma_1$. The dimension of $E(\beta)$ is the number of pairs $(x,y) \in \mathbb{N}_0^2$, with $0 \leq x, y < q$, such that $x\gamma_0 + y\gamma_1 \leq k\gamma_1$. This number coincides with the cardinality of the set

$$\{(x,y) \mid x < t_0(k-y)/s_0,\ y < k\} \cup \{(x,y) \mid x = t_0(k-y)/s_0,\ y < k\} \cup \{(0,k)\},$$

except when $t_0/s_0 > t_1/s_1$, in which case the above second set is empty. On the other hand, when $\beta = \beta_{k+q} = k\gamma_0 + (q-1)\gamma_1$, the dimension of $E(\beta)$ is equal to the cardinality of the set

$$\{(x,y) \mid x < k,\ y \leq q-1\} \cup \{(x,y) \mid x = k,\ y \leq q-1\} \cup$$
$$\cup \{(x,y) \mid x > k,\ y \leq q-1-s_0(x-k)/t_0\},$$

except when $t_0/s_0 > t_1/s_1$. In this last case, the last set must be defined by the inequality $y < q-1-s_0(x-k)/t_0$. This proves our assertion since the best family of codes happens with $t_0/s_0 = 1$ and $\mathfrak{G}$ is the unique δ-sequence with this ratio. To illustrate this fact, in Figure 1 we plot the performances of the relative parameters of the primary codes of maximal length defined by the δ-sequences $\Gamma_1 = \{(1,0),(1,-1)\}$, $\Gamma_2 = \{(11,4),(3,1)\}$ and $\Gamma_3 = \{(5,1),(1,0)\}$, for $q = 256$. As usual, $[n,k,d]$ stands for the parameters, length, dimension and distance of the codes.

We conclude this study of the case of δ-sequences with two elements by recalling that the Reed-Muller code $\mathrm{RM}_q(r,2)$ coincides with the evaluation code $E((r,0))$ defined by the δ-sequence $\mathfrak{G}$. In fact,

$$E((r,0)) = \mathrm{span}_{\mathbb{F}_q}\left\{\varphi\left(Q_0^{b_0}Q_1^{b_1}\right) \mid b_0(1,0) + b_1(1,-1) \leq (r,0)\right\},$$

where φ is the evaluation at all points in $\mathbb{F}_q^2$. Since $Q_0 = X$ and $Q_1 = Y$, we evaluate polynomials in X and Y of total degree less than or equal to r.

For sufficiently large values of q, the proof of Theorem 3.9 suggests that the families of primary codes of maximal length defined by δ-sequences of two elements can be improved

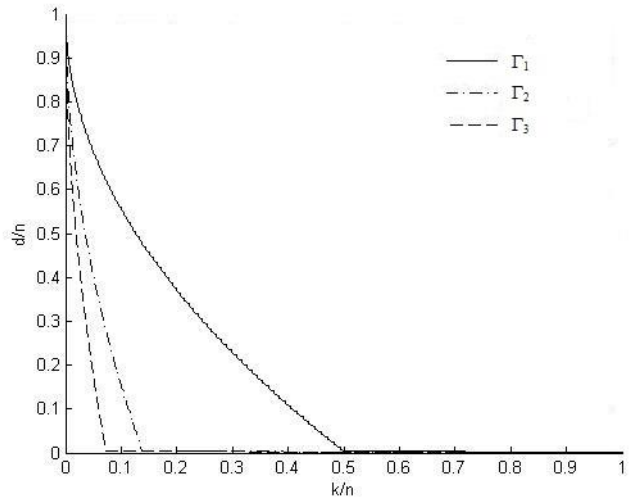

FIGURE 1. Relative parameters of the codes $E(\beta)$ over $\mathbb{F}_{256}$, defined in Section 3, and given by the δ-sequences Γ_1, Γ_2 and Γ_3

with families associated to larger simple δ-sequences. Since $\mathfrak{G} = \{(1,0),(1,-1)\}$ gives the best family, we conclude that to get better families of codes of maximal length, one should consider δ-sequences with the form

$$\Gamma = \{(a_0,0),(a_1,0),\ldots,(a_{g-2},0),(1,0),(1,-1)\},$$

where $a_j = \prod_{i=j+1}^{g-1} n_i$ and $n_i > 1$ for $1 \leq i \leq g-1$. Moreover, the primary Feng-Rao bound of some codes given by δ-sequences Γ as above is rather improved by the bound we gave in the previous section. As a complement of this information, we consider the family of evaluation codes of maximal length given by the simple δ-sequence in Example 3.12 for $q = 256$ and, in Figure 2, we plot the estimated relative parameters determined by Theorem 3.9 (continuous line) and those given by the primary Feng-Rao bound (discontinuous line).

To finish our study of primary codes, we give a table, Table 1, containing the parameters of some good codes given by δ-sequences. Theorem 3.9 shows that their distances are larger than or equal to 4. According to [45], all these codes have the best known parameters. Codes with Feng-Rao distance equal to 4 and the same remaining parameters can be obtained with the δ-sequence $\mathfrak{G}$ and they can be efficiently decoded by [27]. Therefore, we have described codes that constitute an improvement with respect to the previously known.

TABLE 1. Some good decodable codes

Field	δ-sequence	Primary Code	n	k	$d \geq$
$\mathbb{F}_9$	$\{(3,0),(1,0),(1,-1)\}$	$E((13,-5))$	81	75	4
$\mathbb{F}_{16}$	$\{(8,0),(2,0),(1,0),(1,-1)\}$	$E((27,-12))$	256	250	4
$\mathbb{F}_{25}$	$\{(5,0),(1,0),(1,-1)\}$	$E((45,-21))$	625	619	4
$\mathbb{F}_{32}$	$\{(16,0),(2,0),(1,0),(1,-1)\}$	$E((59,-28))$	1024	1018	4

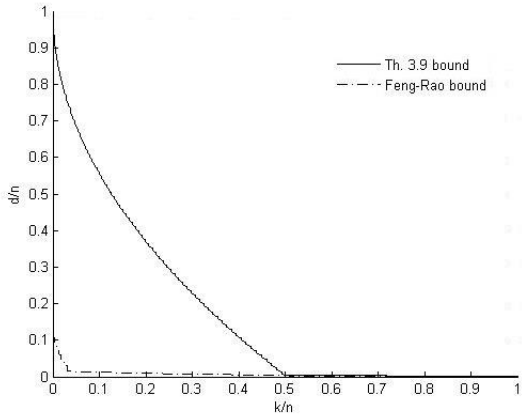

FIGURE 2. Relative parameters of the codes $E(\beta)$ over $\mathbb{F}_{256}$, defined by the δ sequence Γ given in Example 3.12, according to the bound in Theorem 3.9 and the Feng-Rao bound

Next, we study the case of improved codes.

Consider the polynomial ring $R = \mathbb{F}_q[X, Y]$ and its weight function defined by the graded lexicographical order on the monomials with $Y < X$. Then the families of codes $\{\mathfrak{C}(q^2 - l)\}_{l=0}^{q^2-1}$ and $\{\mathfrak{C}_\varphi(q^2-l)\}_{l=0}^{q^2-1}$ defined in Section 2.3 constitute the so-called hyperbolic codes in two variables. These codes (in finitely many variables) were introduced in [42] and also in [47] with the name of hyperbolic cascaded Reed-Solomon codes (see also [48]). From now on, we will use this name for the codes in the family $\{\mathfrak{C}_\varphi(q^2 - l)\}_{l=0}^{q^2-1}$. Notice that there is not an hyperbolic code for each possible dimension. It is not hard to show that the improved dual code $\tilde{C}(l)$, $0 < l \leq q^2$, for the δ-sequence $\mathfrak{G}$ coincides with $\mathfrak{C}_\varphi(l)$. In addition, reasoning as in [23], the equality of primary and dual improved evaluation codes given by $\mathfrak{G}$ can be proved (see also [5]) and also that l is the actual distance of $\tilde{E}(l)$.

The δ-sequences with two elements determine the same family of improved evaluation codes of maximal length $\tilde{E}\,(l)$ for $0 < l \leq q^2$. The dimension of the code $\tilde{E}\,(l)$ equals the number of solutions $(b, c) \in \mathbb{N}_0^2$ of the inequality $(q - b)\,(q - c) \geq l$, where $b, c < q$. And this number is equal to

$$k_l = \left(\sum_{b=0}^{\lfloor (q^2-l)/q \rfloor} \left\lfloor \frac{q^2 - bq - l}{q - b} \right\rfloor \right) + \left\lfloor \frac{q^2 - l}{q} \right\rfloor + 1. \tag{6}$$

In fact, the inequality $(q - b)\,(q - c) \geq l$ is equivalent to $c \leq (q^2 - bq - l)/(q - b)$ and, then, the first summand of the sum in (6) determines the number of solutions c, $1 \leq c < q$, of the previous inequality, where b runs over all possible values, $0 \leq b \leq q^2 - l/q$. The summand $\left\lfloor \frac{q^2-l}{q} \right\rfloor + 1$ corresponds to the number of solutions where $c = 0$. As a consequence,

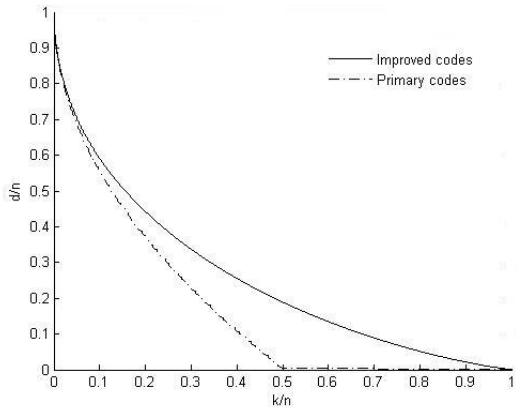

FIGURE 3. Relative parameters for improved codes $\tilde{E}(l)$ and primary codes $E(\beta)$ over $\mathbb{F}_{256}$ given by the δ-sequence $\mathfrak{G} = \{(1,0),(1,-1)\}$

$k_l \geq (q^2 - l + q) - lH_q$, where $H_q = \sum_{j=1}^{q} (1/j)$. Taking into account Theorem 2.7,

$$\frac{k_l}{q^2} + \frac{l}{q^2} H_q \geq 1 + \frac{q-l}{q^2},$$

where k_l/q^2 and l/q^2 are the relative parameters of the improved evaluation codes $\tilde{E}(l)$. In Figure 3, we contrast the performance of the family of improved primary codes (continuous line) and that of the family of primary codes defined by the δ-sequence $\{(1,0),(1,-1)\}$ (discontinuous line). In both cases, we are speaking of maximal length codes and our field is $\mathbb{F}_{256}$. Note that the family $\{\tilde{E}(l)\}_{l \leq q^2}$ behaves like that of hyperbolic codes.

Now consider a simple δ-sequence Γ with ν-vector $\underline{n}$ that satisfies the conditions in Theorem 3.9. Then, the family of improved codes of maximal length given by Γ is

$$\tilde{E}(l) = \text{span}_{\mathbb{F}_q} \left\{ \varphi\left(Q_0^{b_0} Q_1^{b_1} \cdots Q_g^{b_g}\right) \mid \prod_{i=0}^{g} (n_i - b_i) \geq l \text{ with } b_i < n_i \right\},$$

for $1 \leq l \leq q^2$, where $q = \prod_{i=0}^{g-1} n_i = n_g$ and $\{Q_i\}_{i=0}^{g}$ is the sequence of approximates for Γ. Therefore, the best performances happen for δ-sequences of two elements because the number of solutions of the inequality $\prod_{i=0}^{g} (n_i - b_i) \geq l$ decreases when g increases.

The bound in Theorem 3.9 suggests the following definition for what we call δ-improved codes.

Definition 4.1. Let $\Gamma = \{\gamma_i\}_{i=0}^{g}$ a simple δ-sequence whose ν-vector is $\underline{n} = (n_i)_{i=1}^{g-1}$. The *$\delta$-improved primary evaluation l-code*, $1 \leq l \leq q^2$, of maximal length is defined as

$$E^{\delta}(l) := \text{span}_{\mathbb{F}_q} \left\{ \varphi\left(\prod_{i=0}^{g} Q_i^{b_i}\right) \mid \tau\left(\sum_{i=0}^{g} b_i \gamma_i\right) \geq l \right\},$$

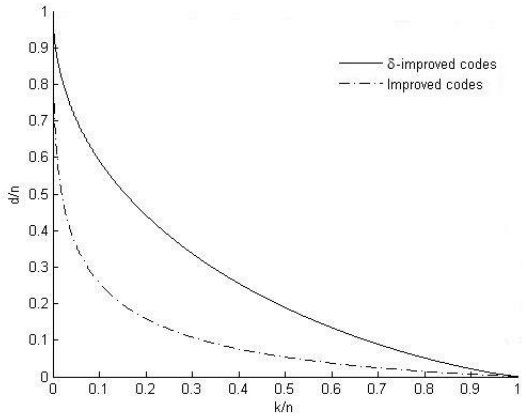

FIGURE 4. Relative parameters of δ-improved and improved codes over $\mathbb{F}_{256}$ given by the δ-sequence in Example 3.12

where $\{Q_i\}_{i=0}^{g}$ is a family of approximates and

$$\tau\left(\sum_{i=0}^{g} b_i\gamma_i\right) := \left(q - \sum_{i=0}^{g-2}(b_i \prod_{j=i+1}^{g-1} n_j) - b_{g-1}\right)(q - b_g)$$

is derived as the bound in Theorem 3.9.

Set $\beta = \sum_{i=0}^{g} b_i\gamma_i \in \Delta_{\Gamma,q}$ and such that $\sigma(\beta) = \prod_{i=0}^{g}(n_i - b_i) \geq l$. The inequality $\tau(\beta) \geq \sigma(\beta)$ holds by Theorem 3.10 and so $\tilde{E}(l) \subset E^{\delta}(l)$ for all index l. Therefore, $\dim \tilde{E}(l) \leq \dim E^{\delta}(l)$. Consider now a nonzero element $\mathbf{c}$ in $E^{\delta}(l)$, then $\mathbf{c} = \varphi(F)$ for some polynomial

$$F(X,Y) = \sum_{\eta=\sum_{i=0}^{g} s_i\gamma_i \in \Delta_{\Gamma,q},\ \tau(\eta)\geq l} \lambda_\eta Q_0^{s_0} Q_1^{s_1} \cdots Q_g^{s_g}.$$

Modifying F to get a polynomial $G(X,Y)$ as in the proof of Theorem 3.9, one obtains $\mathbf{0} \neq \mathbf{e} = \varphi(G) \in \tilde{E}(l)$ which proves the following sequence of inequalities $\mathrm{wt}(\mathbf{c}) \geq \mathrm{wt}(\mathbf{e}) \geq l$. As a consequence, we have proved the following result.

Proposition 4.2. *With the above notations and for any prescribed distance l ($1 \leq l \leq q^2$), the inclusion of codes $\tilde{E}(l) \subset E^{\delta}(l)$ holds and the minimum distance of the δ-improved codes satisfies $d\left(E^{\delta}(l)\right) \geq l$.*

The above result proves that the performance of the family of δ-improved primary codes is better than that of improved primary ones. Figure 4 shows the curves of (estimated) relative parameters for δ-improved codes (continuous line) and improved ones (discontinuous line) corresponding to the field $\mathbb{F}_{256}$ and the δ-sequence in Example 3.12.

5. Coset bounds

We conclude this paper with a short section devoted to give coset bounds for codes defined by simple δ-sequences. To do it, we will use some ideas of the proof of Theorem

3.9. One of the main motivations for studying coset bounds is their relation with secret sharing schemes (SSSs) [36]. With a SSS, one desires encode a *secret* into a family of information segments called *shares* but only certain subfamilies can determine the secret. These subfamilies are called the access structure of the SSS. Elements in the access structure are the so-called *qualified subsets*. Obviously, *unqualified subsets* are those which are not in the access structure. It seems that McEliece and Sarwate in [44] were the first who gave a relation between linear codes and SSSs by relating the scheme in [54] with Reed-Solomon codes. Recently, Duursma and Park [10] have given a construction of SSSs considering linear codes $E_1 \subset E$ of length n such that $\dim E/E_1 = 1$. The extension of codes $E_1 \subset E$ corresponds an extension of dual codes $(E^\perp :=)D \subset D_1(:= E_1^\perp)$ whose difference set provides the shares for the secret. This one is an element in the base field $\mathbb{F}_q$. The qualified and unqualified subsets of this SSS are said to be for D_1/D. The main result for our purposes is the following one. It can be found in [10, Corollary 1.7].

Proposition 5.1. *The smallest qualified subset for D_1/D is of size $d(E/E_1)$ and the largest unqualified subset for D_1/D is of size $n - d(D_1/D)$, where for a inclusion of codes $C' \subset C$ of codimension 1, $d(C/C')$ denotes its minimum distance which is equal to* $\min\{d(x,0) \mid x \in C, x \notin C'\}$.

Returning to codes defined by δ-sequences, consider one of them Γ with ν-vector $\underline{n}$ and set $\{E(\beta)\}_{\beta\in\Delta_{\Gamma,q}}$ the family of primary evaluation codes of maximal length that provides. Denote by σ the function defined in Section 2.3 and by τ that introduced in Definition 4.1.

Theorem 5.2. *With the above notations and for any element $\beta \in \Delta_{\Gamma,q}$, it holds that $d(E(\beta)/E(\beta^-)) \geq \tau(\beta)$, where $\beta^- =$* $\max\{\alpha \in \Delta_{\Gamma,q} \mid \alpha < \beta\}$.

Proof. Set $\Delta_{\Gamma,q} = \{\alpha_1 < \alpha_2 < \cdots < \alpha_{q^2}\}$, $\beta = \alpha_t$ and $\beta^- = \alpha_{t-1}$. Denote $\{F_{\alpha_j}\}_{j=1}^{q^2}$ the set of monomials in the elements $\{Q_i\}_{i=0}^{g}$ with weights α_j whose evaluation gives generating vectors for the codes. Pick a nonzero element $\mathbf{c} = \varphi(F)$ in $E(\alpha_t)$ which is not in $E(\alpha_{t-1})$. Write $M(\alpha_t) = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_{\sigma(\beta)}}\}$ the set defined in Section 2.3. It is clear that for each r, $1 \leq r \leq \sigma(\beta)$, there exists $\alpha_{k_r} \in \Delta_{\Gamma,q}$ satisfying $\alpha_{j_r} = \alpha_{k_r} + \alpha_t$ and therefore the vectors in the set $\{\varphi(F) * \varphi(F_{\alpha_{k_r}})\}$ are linearly independent (recall that $*$ means componentwise product). This proves the following inequality involving Hamming weights $\mathrm{wt}(\mathbf{c}) \geq \sigma(\beta)$ (see [3, Theorem 8]). Now, reasoning as in the proof of Theorem 3.9, consider the polynomial G introduced in that proof and derived from F. Then we get that $\mathrm{wt}(\mathbf{c}) = \mathrm{wt}(\mathbf{e}) \geq \tau(\beta)$, where $\mathbf{e} = \varphi(G)$ and the inequality holds because $\tau(\beta)$ is the value $\sigma_\Lambda(\beta)$, σ_Λ being the σ function for the δ-sequence Λ formed by the last two elements in Γ. □

To finish this section and this paper, we present an example of two codes $E_1 \subset E$ over the field $\mathbb{F}_{32}$ of length 1024 and such that $\dim E = 882$, $\dim E/E_1 = 1$ and $d(E/E_1) \geq 77$. Indeed, we use the code $E = E((46,-21))$ defined by the δ-sequence $\{(16,0),(4,0),(1,0),(1,-1)\}$. Here the ν-vector is $(4,4)$ and $\mathbf{B} = (2,4,4,32)$. Since $(46,-21) = 1(16,0) + 2(4,0) + 1(1,0) + 21(1,-1)$, we get $\tau((46,-21)) = 77$. The obtained bound coset in [10, Example 5.4] was 45 for an extension of two-point AG-codes $C_1 \subset C$ with C of the same dimension as E and length 1023.

6. Akcnowledgements

The authors would like to thank the reviewers for their valuable comments and effort to improve the manuscript.

References

[1] S.S. Abhyankar and T.T. Moh, Newton-Puiseux expansion and generalized Tschirnhausen transformation, *J. Reine Angew. Math.* **260** (1973) 47-83; *J. Reine Angew. Math.* **261** (1973) 29-54.
[2] S.S. Abhyankar, *Lectures on expansion techniques in Algebraic Geometry*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics **57** (Tata Institute of Fundamental Reserch, Bombay, 1977).
[3] H. Andersen and O. Geil, Evaluation codes from order domain theory, *Finite Fields Appl.* **14** (2008) 92-123.
[4] E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
[5] M. Bras-Amorós and M.E. O'Sullivan, Duality for some families of correction capability optimized evaluation codes, *Adv. Math. Commun.* **2** (2008) 15-33.
[6] A. Campillo, *Algebroid curves in positive characteristic*, Lect. Notes in Math. **613**, Springer, Berlin, 1980.
[7] 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.
[8] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Springer, 1998.
[9] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry*, 3rd edition, Springer, 2007.
[10] I.M. Duursma and S. Park, Coset bounds for algebraic geometric codes, *Finite Fields Appl.* **16** (2010) 36-55.
[11] 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.
[12] G.L. Feng and T.R.N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, *IEEE Trans. Inform. Theory* **40** (1994) 1003-1012.
[13] G.L. Feng and T.R.N Rao, Improved geometric Goppa codes, part I: Basic theory, *IEEE Trans. Inform. Theory* **41** (1995) 1678-1693.
[14] J. Fitzgerald and R.F. Lax, Decoding affine variety codes using Gröbner bases, *Des. Codes Cryptogr.* **13** (1998) 147-158.
[15] C. Galindo and F. Hernando, Quantum codes from affine variety codes and their subfield subcodes. *Des. Codes Crytogr.* **76** (2015) 89-100.
[16] C. Galindo, F. Hernando, D. Ruano, New quantum codes from evaluation and matrix-product codes. To appear in *Finite Fields Appl.* (2015).
[17] C. Galindo, F. Hernando and D. Ruano, Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.* (2015) DOI 10.1007/s11128-015-1057-2.
[18] C. Galindo and F. Monserrat, δ-sequences and evaluation codes defined by plane valuations at infinity, *Proc. London Math. Soc.* **98** (2009) 714-740.
[19] C. Galindo and F. Monserrat, Evaluation codes defined by finite families of plane valuations at infinity. *Des. Codes Crypt.* **70** (2014) 189-213.
[20] C. Galindo and F. Monserrat, The Abhyankar-Moh theorem for plane valuations at infinity, *J. Algebra* **374** (2013) 181-194.
[21] C. Galindo and M. Sanchis, Evaluation codes and plane valuations, *Des. Codes Crypt.* **41 (2)** (2006) 199-219.
[22] O. Geil, *Codes based on an $\mathbb{F}_q$-algebra*, Ph.D. thesis, Aalborg University, Denmark, 1999.
[23] O. Geil and T. Høholdt, On hyperbolic codes, Proceedings of AAECC-14, Lect. Notes Comp. Sc. **2227** (2001) 159-171.
[24] O. Geil and R. Pellikaan, On the structure of order domains, *Finite Fields Appl.* **8** (2002) 369-396.

[25] O. Geil, R. Matsumoto and D. Ruano, List decoding algorithms based on voting in Gröbner bases for general one-point AG codes. Information Theory Proceedings -ISIT- (2012) 86-90.
[26] O. Geil, R. Matsumoto and D. Ruano, List decoding algorithms based on Gröbner bases for general one-point AG codes, in Proc. 2012 IEEE International Symposium on Information theory, Cambridge, MA, USA (2012) 86-90.
[27] O. Geil, R. Matsumoto and D. Ruano, Feng-Rao decoding of primary codes, *Finite Fields Appl.* **23** (2013) 35-52.
[28] V.D. Goppa, "Geometry and codes", Mathematics and its applications **24**, Kluwer, Dordrecht (1991).
[29] V.D. Goppa, Codes associated with divisors, *Problems Inform. Transmission* **13** (1997) 22-26.
[30] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE Transf. Inform. Theory* **45** (1999) 1757-1767.
[31] T. Høholdt, J.H. van Lint and R. Pellikaan, Algebraic geometry codes, *Handbook of Coding Theory* **1** (1998) 871-961.
[32] C.D Jensen, Fast decoding of codes from algebraic geometry, *IEEE Trans. Inform. Theory* **40** (1994) 223-230.
[33] 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.
[34] 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.
[35] C. Kirfel and R. Pellikaan, The minimun distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inform. Theory* **41** (1995) 1720-1732.
[36] J. Kurihara, T. Uyematsu and R. Matsumoto, Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hammimg weight, *IEICE Trans. Fundam.* **E95-A (11)** (2012) 2067-2075.
[37] K. Lee, Unique decoding of plane AG codes revisited. *J. Appl. Math. Inf.* **32** (2014) 83-98.
[38] K. Lee, M. Bras-Amorós and M.E. O'Sullivan, Unique decoding of plane AG codes via interpolation, *IEEE Trans. Inform. Theory* **58** (2012) 3941-3950.
[39] K. Lee, M. Bras-Amorós and M.E. O'Sullivan, Unique decoding of general AG codes, *IEEE Trans. Inform. Theory* **60** (2014) 2038-2053.
[40] C. Marcolla, E. Orsini and M. Sala, Improved decoding of affine-variety codes, *J. Pure Appl. Algebra* **216** (2012) 147-158.
[41] J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Theory* **15** (1969) 122-127.
[42] J.L. Massey, D.J. Costello and J. Justensen, Polynomial weights and code constructions, *IEEE Trans. Inform. Theory* **19** (1973) 101-110.
[43] 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.
[44] R.J. McEliece and D.V. Sarwate, On sharing secrets and Reed-Solomon codes, *Commun. ACM* **24** (1981) 583-584.
[45] MinT, Online database for optimal parameters of (t, m, s)-nets, (t, s)-sequences, orthogonal arrays, linear codes and OOAs, available at http://mint.sbg.ac.at/.
[46] R. Pérez-Casales, Ph.D. thesis, in preparation.
[47] K. Saints and C. Heegard, *On hyperbolic cascaded Reed-Solomon codes* in Proc. AAECCC-10, Lect. Notes Comp. Sc. **673** (1993) 291-303.
[48] K. Saints and C. Heegard, Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases, *IEEE Trans. Inform. Theory* **41** (1995) 1733-1751.
[49] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, *Inform. and Comput.* **84** (1990) 207-239.
[50] S. Sakata. *The BMS algorithm*, Gröbner bases, coding and cryptography, 143-163. RISC Book Series (Springer, 2009).
[51] S. Sakata. *The BMS algorithm and decoding of AG codes*, Gröbner bases, coding and cryptography, 165-185. RISC Book Series (Springer, 2009).

[52] 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.
[53] 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.
[54] A. Shamir, How to share a secret, *Commun. ACM* **22** (1979) 612-613.
[55] A.N. Skorobogatov and S.G. Vlădut, On the decoding of algebraic geometric codes, *IEEE Trans. Inform. Theory* **36** (1990) 1051-1060.
[56] M. Spivakovsky, Valuations in function fields of surfaces, *Amer. J. Math.* **112** (1990) 107-156.
[57] M.E. O'Sullivan, Decoding of codes defined by a single point on a curve, *IEEE Trans. Inform. Theory* **41** (1995) 1709-1719.
[58] 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.
[59] O. Zariski and P. Samuel, *Commutative Algebra, vol. II* (Springer-Verlag, 1960).

Current address: **Carlos Galindo**: Departamento de Matemáticas & Instituto Universitario de Matemáticas y Aplicaciones de Castellón (IMAC), Universitat Jaume I. Campus de Riu Sec, 12071 Castellón, Spain.
Reynaldo Pérez-Casales: Departamento de Ciencia de la Computación, Facultad de Matemática y Computación, Universidad de Oriente, Santiago de Cuba, Cuba.
E-mail address: galindo@mat.uji.es rperez@csd.uo.edu.cu