View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Finite Fields and Their Applications 16 (2010) 265–276

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Improved evaluation codes defined by plane valuations

M. Borges-Quintana [a], M.A. Borges-Trenard [a], C. Galindo [b,*,1]

[a] *Departamento de Matemática, FcMC, Universidad de Oriente, Santiago de Cuba, Cuba*
[b] *Departamento de Matemáticas and Instituto Universitario de Matemáticas y Aplicaciones de Castellón (IMAC), Campus de Riu Sec s/n, Universitat Jaume I, 12071 Castellón, Spain*

ARTICLE INFO

Article history:
Received 4 August 2009
Revised 16 February 2010
Available online 9 April 2010
Communicated by Simeon Ball

MSC:
primary 94B27
secondary 14B05, 11T71

Keywords:
Evaluation codes
Valuations
Weight functions
Order structures

ABSTRACT

We study improved evaluation codes associated with finitely generated order structures given by plane valuations. We show minimal sets of generators of the semigroups of these structures and provide parameters for the corresponding improved evaluation codes.
© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Order structures (T, o, S) for coding purposes were introduced in [9]. To define them over a finite field of q elements $\mathbb{F}_q$, one needs a $\mathbb{F}_q$-algebra T and an order function $o : T \to S$ on a sub-semigroup S of the set of nonnegative integers. Order structures define a filtration of vector spaces contained in T, whose images, by an evaluation map ϕ, provide two families of error-correcting codes (evaluation codes and their dual codes). Well-known codes as the one-point geometric Goppa codes or weighted Reed–Muller codes can be regarded as codes given by order structures. The concept of order structure was introduced to simplify the treatment of some algebraic geometry codes related with algebraic curves. However, the extension given in [7] of that concept to more general semigroups S has facilitated the enlarging of the theory to codes on more general varieties [5,14,6].

* Corresponding author.
E-mail address: galindo@mat.uji.es (C. Galindo).
1 Supported by Spain Ministry of Education MTM2007-64704, JCyL VA025A07 and Bancaixa P1-1B2009-03.

1071-5797/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2010.03.002

The main advantages of using order structures in coding theory appear when one uses weight functions w instead of order functions o in the definition. A weight function ω is an order function which also satisfies $\omega(xy) = \omega(x) + \omega(y)$, $x, y \in T$. In this case, lower bounds for the minimum distance can be obtained of their associated dual codes, as Goppa distance and Feng–Rao distances (also called order bounds) and, furthermore, those codes can be decoded by using the so-called Berlekamp–Massey–Sakata algorithm, correcting a number of errors that depends on the above bounds [9,17]. Notice that the advantage of the mentioned algorithm is that it allows us to get fast implementations of the modified algorithm of [11,18] (see [12,10]) and of the majority voting scheme for unknown syndromes of Feng and Rao [4].

A concept very close to that of weight function is that of valuation. Valuations have a geometrical meaning and therefore they can be very useful to provide codes associated with algebraic varieties. Unfortunately, there is not available any general classification of valuations, but there is a classification of valuations of function fields of nonsingular surfaces (also called plane valuations) [19,16,8], that allows us to decide which of them are suitable for providing in an explicit manner order structures and evaluation codes. The first examples that use that classification were given in [17] and a more systematic development can be found in [5]. Furthermore, by considering certain class of plane valuations named at infinity, it is possible to get weight functions with finitely and infinitely generated semigroups in $\mathbb{N}^2$ or $\mathbb{R}$, whose attached domain is the polynomial ring in two indeterminates, that provide a large class of codes with good parameters [6]. The examples in [17] concerning plane valuations are particular cases of the theory developed in [6].

When a family of evaluation codes is constructed from a weight function, one must evaluate some elements f_i in R, $\phi(f_i)$, picked according the order considered in the semigroup S. The set of vectors obtained by evaluating the whole set of the above elements f_i generates the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$, n being the length of the code. However, to get a basis of $\mathbb{F}_q^n$, usually, we do not need some of those f_i, since some vectors $\phi(f_i)$ can be linearly dependent of the previous picked vectors $\phi(f_j)$. Andersen and Geil in [1] study evaluation codes taking into account the selection of convenient f_i for finitely generated order structures, especially for the case when as ϕ it is considered the natural evaluation map and we evaluate as much points as possible. The paper [5] provides order structures given by plane valuations centered at a two-dimensional local regular Noetherian domain where the semigroup of the order function is forced to be the same as the one of the corresponding valuation. The semigroup of these order structures can be, or not, finitely generated. In this paper, we study the finitely generated case particularizing to our situation the ideas given in [1]. Concretely, we shall describe the semigroups and the ideals defining our order structures, we shall compute the maximum length and the dimension of the corresponding codes where a lower bound for the minimum distance has been prefixed.

We can compute the parameters of our codes because we use as ϕ, the natural evaluation map, φ, that evaluates at all the points in the zero set of the ideal defining the corresponding $\mathbb{F}_q$-algebra T. To complete the paper, we add a comparing example where relative dimensions of one of our families of codes and of codes with similar relative minimum distance obtained without evaluating at all the zero set attached to T are showed.

Finally, we briefly summarize the contents of the paper. In Section 2, some generalities about plane valuations are exposed, recalling its classification; furthermore, we study in detail the order structures that the mentioned types of valuations define, whose semigroups associated will be described later on. Section 3 is the main one of the paper; it is devoted to study the improved evaluation codes introduced in [1] but particularized to the order structures given in Section 2. The parameters (length, dimension, and minimum distance) of the codes we study are discussed in Theorem 3.1, where the length is explicitly given and it is showed how to compute the distance, while Corollary 3.1 provides a direct formulae for computing that distance in the binary case. Section 4 develops the above mentioned comparing example and Section 5 is devoted to the description of the value semigroup of the types of valuations used in the paper, including a clearing example.

2. Order structures given by plane valuations

In this paper we shall use order structures given by plane valuations and, for this reason, in our first subsection, we recall some facts, concerning valuations, that will be useful.

2.1. Plane valuations

We start with the definition of valuation.

Definition 2.1. A *valuation* of a field K is a mapping

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

where G is a totally ordered commutative group, that satisfies

- $\nu(u+v) \geqslant \min\{\nu(u), \nu(v)\}$;
- $\nu(uv) = \nu(u) + \nu(v)$

for $u, v \in K^*$.

We shall only consider valuations ν of the quotient field K of a local regular Noetherian domain R. The sub-ring of K, $R_\nu := \{u \in K^* \mid \nu(u) \geqslant 0\} \cup \{0\}$, is called the *valuation ring of* ν. R_ν is a local ring whose maximal ideal is $m_\nu := \{u \in K^* \mid \nu(u) > 0\} \cup \{0\}$. The Krull dimension of the ring R_ν will be named the rank of the valuation ν ($\mathrm{rk}(\nu)$). Now, set m the maximal ideal of R, we say that ν is *centered at* R if $R \subseteq R_\nu$ and $R \cap m_\nu = m$. In this case, the ideals contraction to R of ideals in R_ν are called *valuation ideals* or ν*-ideals*. Finally, the subset of G, $\nu(R \setminus \{0\})$, is called the *semigroup* of the valuation ν (relative to R) and usually denoted by S. It is a commutative with zero semigroup of G.

In this paper, we are interested in codes given by order functions defined by valuations centered at domains R as above whose order semigroup coincides with the semigroup of the corresponding valuation.

There is no known classification of valuations as above in the general case, however there is a classification for the case when the dimension of the ring R is two. This is due to Spivakovsky [16], improves a previous one given by Zariski [19], and it is based in the one to one correspondence existing between the set of plane valuations and the set of simple sequences of quadratic transformations of the scheme Spec$R$. We shall use for our purposes this class of valuations. Above mentioned classification divides valuations in five types that we denote by A, B (with two subtypes), C, D and E. The rank of a valuation equals the number of nonzero isolated subgroups of its value group G. We recall that a subgroup H of an ordered group G is isolated if it is a segment with respect to the ordering, i.e. if $h \in H$, $g \in G$ and $-h \leqslant g \leqslant h$, then $g \in H$. The rank and other two parameters, the rational rank and the transcendence degree, have been used classically to describe (and classify in the two-dimensional case) valuations. For a valuation ν as above, the rational rank of ν (rat. $\mathrm{rk}(\nu)$) is the dimension of the $\mathbb{Q}$-vector space $G \otimes_{\mathbb{Z}} \mathbb{Q}$, where $\mathbb{Z}$ ($\mathbb{Q}$, respectively) is the set of integer (rational, respectively) numbers. The transcendence degree of ν (tr. $\deg(\nu)$) is the transcendence degree of the field $K_\nu := R_\nu/m_\nu$ over $k := R/m$. Two useful inequalities involving these parameters are $\mathrm{rk}(\nu) \leqslant$ rat. $\mathrm{rk}(\nu)$ and rat. $\mathrm{rk}(\nu) +$ tr. $\deg(\nu) \leqslant \dim R$. Table 1 relates the above parameters with the cited Spivakovsky's classification of valuations.

Valuations of type B-II can also be subdivided according that they admit or not generating sequences (see Definition 2.4 further on). In the affirmative case, we are talking about type B-II-a valuations. The reader can found a more complete development of the above ideas in [5].

There are some types of valuations to which our methods do not apply. Indeed, valuations of types A, B (except B-II-a) and E will not be used. The reason is that type A valuations do not provide order functions in the manner we shall describe, the obstruction being that the dimension of the k-vector spaces P_α/P_{α^+} of the graded algebra $\mathrm{gr}_\nu R$ defined in Section 2.3 needs not be 1. Valuations of type B, except type B-II-a, do not admit generating sequences and they cannot satisfy the

Table 1
Classification of plane valuations.

Type	Subtype	rk	rat. rk	tr. deg
A	–	1	1	1
B	I	2	2	0
	II	1	1	0
C	–	2	2	0
D	–	1	2	0
E	–	1	1	0

forthcoming Theorem 2.1. Finally, type E valuations do not give finitely ordered structures to which is devoted this paper.

The essential information about valuations we shall need is in their value semigroups. To simplify the reading of this paper, we have relegated to Section 5 the detailed description of the value semigroups of those valuations which we are interested in, while we state in our next proposition the ambient space where these semigroups are. First, recall that a numerical semigroup is a sub-semigroup Γ of the nonnegative integers $\mathbb{N}$ such that $\mathbb{N} \setminus \Gamma$ is finite. Any numerical semigroup admits a finite minimal generating set that we shall usually denote $\{\bar{\beta}_i^*\}_{i=0}^g$. This set satisfies $0 < \bar{\beta}_0^* < \bar{\beta}_1^* < \cdots < \bar{\beta}_g^*$, $\bar{\beta}_i^*$ does not belong to the semigroup spanned by $\bar{\beta}_0^*, \bar{\beta}_1^*, \ldots, \bar{\beta}_{i-1}^*$, $1 \leqslant i \leqslant g$, and $\gcd(\bar{\beta}_0^*, \bar{\beta}_1^*, \ldots, \bar{\beta}_{i-1}^*) \neq 1$ whenever $1 \leqslant i \leqslant g-1$, and $\gcd(\bar{\beta}_0^*, \bar{\beta}_1^*, \ldots, \bar{\beta}_g^*) = 1$. Notice that our notation for these generating sets respects the usual one for numerical semigroups within the context of plane curves [2].

Proposition 2.1. *(See [3].) Let ν be a type B-II-a (respectively, C, D) plane valuation of the field K centered at R. Then the value semigroup S of ν is a finitely generated semigroup of $\mathbb{N}^2$ (respectively, $\mathbb{N}^2$, $\mathbb{R}$) minimally generated by a set $\{\bar{\beta}_i\}_{i=0}^g$ that can be computed from a certain numerical semigroup. The ordering in $\mathbb{N}^2$ is the lexicographical one and in $\mathbb{R}$ the natural one.*

2.2. Order structures

We start by giving the definition of order domain. Some references where this concept is treated are [9,17,7] and [1]. Particularly in [7] the notion of order domain is generalized so that the support semigroup of the corresponding order structure needs not be numerical; this paper also studies the generalization of the theory of Gröbner bases to order domains that begins in [17].

Definition 2.2. Let $<$ be an ordering on the set S. $(S, <)$ is called a well-order (and $<$ a well-ordering) if any non-empty subset of S has a smallest element under $<$.

Let S be as in Definition 2.2, for many properties, S is also required to be a cancellative commutative monoid, which, in the sequel, we shall call *semigroup* (following [7]). It is usual to adjoin an extra element $-\infty$ to S to get the set $S_{-\infty}$ so that $-\infty$ is the minimal element of $S_{-\infty}$. Another useful property of the ordering $<$ is to be *admissible*, i.e. $0 \leqslant \alpha$, for all $\alpha \in S$, and $\alpha + \gamma \leqslant \beta + \gamma$ whenever $\alpha \leqslant \beta$.

Definition 2.3. Let $\mathbb{F}$ be a field, T an $\mathbb{F}$-algebra, and let $(S, <)$ be a well-order. An order function on T is a surjective map $o : T \to S_{-\infty}$ which, for all $f, g \in T$, satisfies the following properties:

- $o(f) = -\infty$ if, and only if, $f = 0$;
- $o(af) = o(f)$ for all nonzero element $a \in \mathbb{F}$;
- $o(f + g) \leqslant \max\{o(f), o(g)\}$;
- If $o(f) < o(g)$ and $0 \neq h \in T$, then $o(fh) < o(gh)$;
- If f and g are nonzero elements and $o(f) = o(g)$, then there exists a nonzero element $a \in \mathbb{F}$ such that $o(f - ag) < o(g)$.

The triple (T, o, S) is called an *order structure* and T an *order domain over* $\mathbb{F}$. An order function such that it also satisfies $o(fg) = o(f) + o(g)$ is called a *weight function*. An order structure (T, o, S) is called *finitely generated* if S is a finitely generated semigroup.

All order domains we shall use in this paper will be with an associated weight function.

2.3. Finitely generated semigroups of order structures given by plane valuations

To start, we recall the following result that follows from [5, Propositions 2.1 and 2.2].

Proposition 2.2. *The value semigroup S of a valuation ν of a field K, centered at R, is a free of torsion, well-ordered semigroup, where the associated order is admissible.*

Furthermore, assume that the canonical embedding of the field $k := R/m$ into the field $K_\nu := R_\nu/m_\nu$ is an isomorphism. Denote by o the mapping $o : K^* \to G$ given by $o(u) = -\nu(u)$ and let $A \subseteq K^*$ be a k-algebra satisfying that $o(A)$ is a free of torsion, well-ordered semigroup, where the associated order is admissible. Then, the mapping $o : A \to o(A) \cup \{-\infty\}$, $o(0) = -\infty$, is a weight function.

As a consequence, from a valuation ν as above, one can obtain order domains with fixed semigroup S if one gets k-algebras A with $o(A) = S$. Since we know the structure of the semigroups of plane valuations, we can try to get suitable algebras A such that the semigroup of the order function given by the valuation is the same as that of the valuation. Let us see how to do it. We start by defining the graded algebra associated with a valuation as in Proposition 2.2. For any $\alpha \in S$, let us consider the ν-ideal of ν in R defined by $P_\alpha := \{f \in R \setminus \{0\} \mid \nu(f) \geqslant \alpha\} \cup \{0\}$ and also the ideal $P_{\alpha^+} := \{f \in R \setminus \{0\} \mid \nu(f) > \alpha\} \cup \{0\}$. Then, the *graded algebra associated with* ν is defined as the k-algebra,

$$\mathrm{gr}_\nu R = \bigoplus_{\alpha \in S} \frac{P_\alpha}{P_{\alpha^+}}.$$

Analogously, associated with an order function $o : T \to S \cup \{-\infty\}$, it can also be defined its graded algebra as $\mathrm{gr}_o T := \bigoplus_{\alpha \in S} O_\alpha / O_{\alpha^-}$, where

$$O_\alpha := \left\{ f \in T \mid o(f) \leqslant \alpha \right\} \cup \{0\} \quad \text{and} \quad O_{\alpha^-} := \left\{ f \in T \mid o(f) < \alpha \right\} \cup \{0\}.$$

In this paper, we shall consider only plane valuations of types B-II-a, C or D. We have already given the reason for this.

Definition 2.4. Let ν be a plane valuation of type B-II-a, C or D of the quotient field K of a local regular Noetherian two-dimensional ring R and centered at R. A set $\{r_i\}_{i \in I}$, where $r_i \in m$, is a generating sequence of ν if, and only if, the k-algebra $\mathrm{gr}_\nu R$ is spanned by the cosets defined by the elements r_i in $\mathrm{gr}_\nu R$.

If S denotes a semigroup and k a field, the semigroup k-algebra of S is the S-graded k-algebra $k[S] := \bigoplus_{\alpha \in S} k[S]_\alpha$, where $k[S]_\alpha := k \cdot \alpha$.

The following result is essential for our purposes and it can be deduced from [5, Theorems 4.1, 5.1 and 5.2].

Theorem 2.1. *Let ν be a valuation of the fraction field K of a two-dimensional Noetherian local regular domain R which is centered at R. Assume that ν is of type B-II-a, C, or D, and let $\{q_i\}_{0 \leqslant i \leqslant g}$ be a minimal generating sequence of ν. Then*

1. *The function o $(= -\nu)$ defined over the k-algebra $\mathrm{gr}_o T$, $T := k[\{q_i^{-1}\}_{0 \leqslant i \leqslant g}] \subseteq K$, is a weight function whose value semigroup is S, the value semigroup of ν.*

2. *The graded algebra associated with* ν *(relative to* R*) and that associated with* o *are isomorphic and both are isomorphic to the* k*-algebra of the semigroup* S, $k[S]$.
3. *Let* $\{\bar{\beta}_i\}_{0 \leqslant i \leqslant g}$ *be a minimal system of generators of the semigroup* S*. Then, there exist unique integer positive numbers* $n_1, \dots, n_{g-1}$ *so that any* $s \in S$ *can be written in a unique way in the form* $s = \sum_{i=0}^{g} a_i \bar{\beta}_i$*, where* $a_i \in \mathbb{N}$ *and* $a_i < n_i$*, for* $1 \leqslant i \leqslant g-1$.
4. *Let* $k[\{X_i\}_{0 \leqslant i \leqslant g}]$ *be the free commutative* k*-algebra of polynomials with indeterminates* $\{X_i\}_{0 \leqslant i \leqslant g}$ *and coefficients over* k*. Then the map* $\psi : k[\{X_i\}_{0 \leqslant i \leqslant g}] \to \mathrm{gr}_\nu R$*, defined by* $\psi(X_i) = q_i + P_{\nu(q_i)^+}$*, is an epimorphism of* k*-algebras.*
5. *For each* $1 \leqslant i \leqslant g-1$*, consider the unique expression*

$$n_i \bar{\beta}_i = \sum_{j=0}^{i-1} \gamma_{ij} \bar{\beta}_j, \tag{1}$$

where the γ_{ij}*'s are nonnegative integers such that* $\gamma_{ij} < n_j$, $j \geqslant 1$*, and the* n_j*'s are those described in item* (3)*. Then the ideal* $\ker \psi$ *is spanned by the set of polynomials* $\mathfrak{G} := \{h_1, \dots, h_{g-1}\}$*, where* $h_i := X_i^{n_i} - \prod_{j=0}^{i-1} X_j^{\gamma_{ij}}$, $1 \leqslant i \leqslant g-1$.

Remark 2.1. On the basis of the isomorphisms of item (2) in Theorem 2.1, it is clear that $o(\psi(X_i))$ is equal to $\bar{\beta}_i$, for $i = 0, \dots, g$.

3. Improved evaluation codes given by plane valuations

Since this paper concerns coding theory, from now on, we assume that the field k is any finite field $\mathbb{F}_q$.

We shall study in this section the improved evaluation codes, introduced in [1], for the case of finitely generated order structures given by plane valuations. For simplicity's sake, we shall suppose that the values n_i, defined by the valuations we shall use, satisfy the inequalities $n_i \leqslant q$.

We assume a basic knowledge of Gröbner bases. As a reference, the reader can consult several sources; we cite for instance [15]. Since it will be useful, we recall the definition of footprint of an ideal of a polynomial ring in several variables, also called "Gröbner éscalier".

Definition 3.1. Let I be an ideal of the polynomial ring $\mathbb{F}_q[\{X_i\}_{0 \leqslant i \leqslant g}]$ and consider a term ordering $\prec$ on it. The *footprint* of I is the set of monomials $\pi \in \mathbb{F}_q[\{X_i\}_{0 \leqslant i \leqslant g}]$ such that π is not a leading monomial of any polynomial in I. We shall denote this set by $\Delta_\prec(I)$.

Our initial purpose will be to compute the footprint of $\ker \psi$ (ideal given in Theorem 2.1). In order to do it, it is convenient to introduce the following notation: for a term $\pi = \prod_{i=0}^{g} X_i^{a_i}$, set $\mathfrak{o}(\pi) := \sum_{i=0}^{g} a_i \bar{\beta}_i$. Furthermore, we shall denote by $\prec_{lex}$ the lexicographical term ordering $\prec_{lex}$ so that $X_0 \prec_{lex} X_1 \prec_{lex} \cdots \prec_{lex} X_g$.

Proposition 3.1. *With the same hypothesis and notation of Theorem* 2.1:

1. $\mathfrak{G}$ *is the reduced Gröbner basis of* $\ker \psi$ *with respect to the term ordering* $\prec_o$ *defined as follows*:

$$\pi_1 \prec_o \pi_2 \quad \textit{if and only if} \quad \begin{cases} \mathfrak{o}(\pi_1) < \mathfrak{o}(\pi_2) & \textit{if } \mathfrak{o}(\pi_1) \neq \mathfrak{o}(\pi_2), \\ \pi_1 \prec_{lex} \pi_2 & \textit{otherwise}. \end{cases}$$

2. *The footprint of* $\ker(\psi)$ *is given by*

$$\Delta_{\prec_o}\big(\ker(\psi)\big) = \left\{ \prod_{i=0}^{g} X_i^{a_i} \;\middle|\; 0 \leqslant a_0, a_g,\ 0 \leqslant a_i < n_i,\ \textit{for } i = 1, \dots, g-1 \right\}.$$

Proof. First, $\prec_o$ is a term ordering because of the admissibility of the order on the semigroup of the valuation ν (see Proposition 2.2). Now it is clear that $\{X_i^{n_i}\}_{1\leqslant i\leqslant g-1}$ is the set of leading monomials of $\mathfrak{G}$, with respect to $\prec_o$, and these terms are relatively prime. These conditions guarantee that $\mathfrak{G}$ is a Gröbner basis of the ideal generated by itself, which is $\ker(\psi)$ due to Theorem 2.1, item (5). $\mathfrak{G}$ is reduced because, again, the maximal terms are prime pairwise and the conditions $\gamma_{ij} < n_j$. This concludes the proof of the first item (1), the second one (2) is a direct consequence of the shape of $\mathfrak{G}$. □

3.1. The improved evaluation codes

To get an evaluation code from a weight function $o : \mathrm{gr}_o T \to S$ as above, one needs an epimorphism of $\mathbb{F}_q$-algebras, $\phi : \mathrm{gr}_o T \to \mathbb{F}_q^n$ and then, the family of evaluation codes is formed by the vector spaces $\{E_\alpha\}_{\alpha\in S}$ defined as

$$E_\alpha = \langle \phi(f) \mid o(f) \leqslant \alpha;\ f \in \mathrm{gr}_o T\rangle_{\mathbb{F}_q},$$

where $\langle L\rangle_{\mathbb{F}_q}$ means the vector space over the field $\mathbb{F}_q$ spanned by the set L.

In [1], a variant of this type of codes (and their duals) is proposed, that we call *improved evaluation codes*. To get them, one must set $\alpha(1) := 0$ and define, recursively, for $2 \leqslant i \leqslant n$ values $\alpha(i) \in S$ which are defined by the fact that each $\alpha(i)$ is the smallest element in S, larger than $\alpha(j)$, $1 \leqslant j \leqslant i-1$, satisfying $E_\alpha \subseteq E_{\alpha(i)}$ and $E_\alpha \neq E_{\alpha(i)}$, for all $\alpha < \alpha(i)$. That is, one selects elements $\alpha(i)$ in S such that the relevant generators to evaluate of the successive evaluation codes $E_{\alpha(i)}$ have weight $\alpha(i)$.

Set $\Delta(\mathrm{gr}_o T, o, \phi) := \{\alpha(1), \alpha(2), \dots, \alpha(n)\}$ and, for each $\alpha(i) \in \Delta(\mathrm{gr}_o T, o, \phi)$, fix an element $f_{\alpha(i)} \in \mathrm{gr}_o T$ such that $o(f_{\alpha(i)}) = \alpha(i)$.

Definition 3.2. For each integer $0 \leqslant \delta \leqslant n$, the *improved evaluation code* $\tilde{E}(\delta)$ is defined as

$$\tilde{E}(\delta) := \langle \phi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(\mathrm{gr}_o T, o, \phi) \text{ and } \sigma(\alpha(i)) \geqslant \delta\rangle_{\mathbb{F}_q},$$

where $\sigma(\alpha(i))$ denotes the cardinality of the set

$$\{\gamma \in \Delta(\mathrm{gr}_o T, o, \phi) \mid \alpha(i) + \beta = \gamma;\ \beta \in \Delta(\mathrm{gr}_o T, o, \phi)\}.$$

Furthermore, the *improved dual evaluation code* $\tilde{C}(\delta)$ will be

$$\tilde{C}(\delta) := \{v \in \mathbb{F}_q^n \mid v \cdot \phi(f_{\alpha(i)}) = 0,\ \text{for all } \alpha(i) \in \Delta(\mathrm{gr}_o T, o, \phi),\ \text{with } \mu(\alpha(i)) < \delta\},$$

$\mu(\alpha(i))$ being the cardinality of the set

$$\{s \in S \mid s + \beta = \alpha(i),\ \text{for some } \beta \in S\}.$$

Clearly, the set $\Delta(\mathrm{gr}_o T, o, \phi)$ is an important object in the construction of the codes E_α and essential for obtaining the improved ones $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$. In the following result, we explicitly describe this set whenever ϕ is the natural evaluation map at all possible points.

First recall that if $f + \ker(\psi) \in k[\{X_i\}_{0\leqslant i\leqslant g}]/\ker(\psi)$ and $p \in V_{\mathbb{F}_q}(\ker(\psi))$, one can evaluate $f + \ker(\psi)$ at p as $(f + \ker(\psi))(p) = f(p)$. Assume $V_{\mathbb{F}_q}(\ker(\psi)) = \{p_1, p_2, \dots, p_n\}$ and set $\varphi : k[\{X_i\}_{0\leqslant i\leqslant g}]/\ker(\psi) \to \mathbb{F}_q^n$ the map $\varphi(f + \ker(\psi)) = (f(p_1), f(p_2), \dots, f(p_n))$.

Proposition 3.2. *Let* $(\mathrm{gr}_o T, o, S)$ *be an order structure as defined in Theorem* 2.1 *given by a plane valuation* ν. *Then,* $\Delta(\mathrm{gr}_o T, o, \varphi)$ *is equal to the set*

$$\Delta(\bar\beta_0, \bar\beta_1, \dots, \bar\beta_g) := \left\{\sum_{i=0}^{g} a_i\bar\beta_i \;\middle|\; 0 \leqslant a_0, a_g < q,\ \textit{and } a_i < n_i,\ \textit{for } 1 \leqslant i \leqslant g-1\right\}.$$

Proof. Set J the ideal in $k[\{X_i\}_{0\leqslant i\leqslant g}]$ defined as the ideal sum of $\ker(\psi)$ and the ideal spanned by the binomials $X_i^q - X_i$, $0\leqslant i\leqslant g$. Following the line of the proof of [1, Proposition 45], it can be shown that

$$\Delta(\operatorname{gr}_o T, o, \varphi) = \{o(\psi(\pi)) \mid \pi \in \Delta_{\prec_o}(J)\}.$$

It is clear that $\Delta_{\prec_o}(J) \subseteq \Delta_{\prec_o}(\ker(\psi))$; taking into account Proposition 3.1, we get

$$\Delta_{\prec_o}(J) \subseteq \left\{\prod_{i=0}^{g} X_i^{a_i} \;\middle|\; 0\leqslant a_0, a_g < q,\ 0\leqslant a_i < n_i,\ \text{for } i=1,\dots,g-1\right\}$$

and then, $\Delta(\operatorname{gr}_o T, o, \varphi) = \Delta(\bar\beta_0, \bar\beta_1, \dots, \bar\beta_g)$. □

Finally, we provide the parameters of the improved evaluation codes above defined.

Theorem 3.1. *Let $\tilde E(\delta)$ and $\tilde C(\delta)$ be the improved evaluation codes given by the map φ attached to an order structure $(\operatorname{gr}_o T, o, S)$ given by a plane valuation ν as in Theorem 2.1. Then, the length of both codes is $q^2\prod_{i=1}^{g-1} n_i$, the minimum distance of both codes is larger than or equal to δ and the dimension of both codes is the cardinality of the set*

$$M(\nu) := \Bigg\{(x_0, x_1, \dots, x_g) \in \mathbb{Z}^{g+1} \;\Bigg|\; 0\leqslant x_0, x_q < q;\ 0\leqslant x_i < n_i,\ 1\leqslant i\leqslant g-1,$$
$$\text{and } (q-x_0)(q-x_g)\prod_{i=1}^{g-1}(n_i - x_i) \geqslant \delta\Bigg\}.$$

Proof. First note that J is a radical ideal [13, p. 250] and, since $\mathbb{F}_q$ is a perfect field, the cardinality of the set $V_{\mathbb{F}_q}(\ker(\psi))$ coincides with that of $\Delta(\operatorname{gr}_o T, o, \varphi)$ (see also [1, Proposition 40]). Therefore, the length of our family of codes is the cardinality of the set $\Delta(\bar\beta_0, \bar\beta_1, \dots, \bar\beta_g)$ (see Proposition 3.2), which equals $q^2\prod_{i=1}^{g-1} n_i$ as a consequence of the fact that all the elements defining the set $\Delta(\bar\beta_0, \bar\beta_1, \dots, \bar\beta_g)$ are different elements in the semigroup S (see (3) of Theorem 2.1).

The minimum distances of the codes are larger than or equal to δ by [1, Theorem 33].

To show that the cardinality of $M(\nu)$ is the dimension of $\tilde E(\delta)$, we only need to observe that $\tilde E(\delta)$ is spanned by the vectors $\varphi(f_{\alpha(i)})$ such that $\sigma(\alpha(i)) \geqslant \delta$ and that $\alpha(i) = \sum_{i=0}^{g} x_i\bar\beta_i$ satisfies that condition if, and only if, $(x_0, x_1, \dots, x_g) \in M(\nu)$. Finally, $\alpha(i) \in \Delta(\bar\beta_0, \bar\beta_1, \dots, \bar\beta_g) = \Delta(\operatorname{gr}_o T, o, \varphi)$ (see proof of Proposition 3.2) and this concludes the proof for $\tilde E(\delta)$. With respect to $\tilde C(\delta)$, the result holds because in [1, Proposition 48] it is proved that the dimensions of $\tilde E(\delta)$ and $\tilde C(\delta)$ coincide. □

Corollary 3.1. *Let $\tilde E_2(\delta)$ and $\tilde C_2(\delta)$ be the improved binary evaluation codes given by the map φ attached to an order structure $(\operatorname{gr}_o T, o, S)$ defined by a plane valuation ν as in Theorem 2.1 such that its corresponding values n_i are equal to 2. Then, the length of both codes is 2^{g+1}, the minimum distance of both codes is larger than or equal to δ and the dimension of both codes is*

$$\binom{g}{0}a(\delta) + \binom{g}{1}a(\delta/2) + \cdots + \binom{g}{g}a(\delta/2^g), \tag{2}$$

where $a(\gamma)$, $\gamma\in\mathbb{Q}$, $\gamma>0$, equals 2 if $\lceil\gamma\rceil = 1$, 1 whenever $\lceil\gamma\rceil = 2$ and 0 otherwise.

Proof. From Theorem 3.1, it is clear that the length of the code is 2^{g+1}, because $q = n_i = 2$ for all index i.

Now, if $\gamma \in \mathbb{Q}$, $\gamma > 0$, denote by $a(\gamma)$ the number of solutions of the inequality $y \geqslant \gamma$, $y \in \{1, 2\}$; the values of the function $a(\gamma)$ are those described in the statement. Fixed a distance δ, to get the dimension of our improved codes, by Theorem 3.1, we must compute the number of solutions $a_{g+1}(\delta)$ of the inequality $(2 - x_0)(2 - x_g)\prod_{i=1}^{g-1}(2 - x_i) \geqslant \delta$, where the values x_i can be either 0 or 1. Setting $2 - x_i := y_i$, the former inequality will be

$$y_0 y_1 \cdots y_g \geqslant \delta, \tag{3}$$

and $y_i \in \{1, 2\}$. If one has a unique variable y, then $a_1(\delta) = a(\delta)$, $a_2(\delta) = a(\delta) + a(\delta/2)$ because one can consider either $y_1 = 1$ and the number of solutions of $y_0 y_1 \geqslant \delta$ will be $a(\delta)$ or $y_1 = 2$ and now we have $a(\delta/2)$ solutions for $y_0 y_1 \geqslant \delta$. Finally the number $a_{g+1}(\delta)$ of solutions of the inequality (3) is the dimension of our improved codes and by induction it follows that it coincides with the value given in (2). □

Remark 3.1. For improved evaluation codes, attached to finitely generated order domains adapted to the scheme of [1, Theorem 42], it holds that the values $\sigma(\alpha)$, for indices α in the semigroup corresponding to the relevant generators to evaluate of the order domain, can be computed from the cardinality of the intersection of certain footprints [1, Appendix A]. We have not used this result to prove the above corollary, however from its proof we do compute that cardinality. Next, we introduce the mentioned intersection set in our situation. With the previous notations consider a term $\pi(a_0, a_1, \ldots, a_g) := \prod_{i=0}^{g} X_i^{a_i} \in k[\{X_i\}_{0 \leqslant i \leqslant g}]$, where $0 \leqslant a_0, a_q < q$; $0 \leqslant a_i < n_i$, $1 \leqslant i \leqslant g - 1$, and define $D(\pi)$ as the cardinality of the set $\Delta_{\prec_o}(\mathfrak{G} \cup \pi) \cap \Delta_{\prec_o}(J)$, where $\mathfrak{G}$ is the set defined in Theorem 2.1 and J the ideal defined in the proof of Proposition 3.2. Therefore, by [1, Appendix A] and the proof and notation of Theorem 3.1, it can be deduced that, if $\alpha(i) = \sum_{i=0}^{g} x_i \bar{\beta}_i \in \Delta(\mathrm{gr}_o T, o, \varphi)$, then

$$D\big(\pi(x_0, x_1, \ldots, x_g)\big) = q^2 \prod_{i=1}^{g-1} n_i - \left[(q - x_0)(q - x_g) \prod_{i=1}^{g-1}(n_i - x_i)\right].$$

4. Example

One of the advantages of the improved codes here studied is that one can directly obtain parameters associated to the codes without actually evaluating at all points in $V_{\mathbb{F}_q}(\ker(\psi))$. Notwithstanding, if one considers a proper subset of $V_{\mathbb{F}_q}(\ker(\psi))$, the relative parameters can be improved. For instance, we can consider the example corresponding to Δ_1 in [6, Example 5.7]. Although, in general, the examples considered in that paper cannot be adapted to the situation described in [1, Theorem 42], the mentioned example can be. The family of dual evaluation codes in [6, Example 5.7], which are defined over the field $\mathbb{F}_7$, has length $n = 10$, and the relative family of parameters $(k/n, d/n)$, k being the dimension and d the minimum distance is

$$\left\{\left(\frac{10}{12}, \frac{2}{12}\right), \left(\frac{9}{12}, \frac{3}{12}\right), \left(\frac{8}{12}, \frac{4}{12}\right), \left(\frac{5}{12}, \frac{5}{12}\right), \left(\frac{3}{12}, \frac{6}{12}\right)\right\}. \tag{4}$$

In our case, $g = 1$ and $\ker(\psi)$ is the zero ideal. Since the field is $\mathbb{F}_7$, the length of the codes is 49 and, by Theorem 3.1, the corresponding family of codes $\tilde{C}(\delta)$ with (estimated) relative distances δ/n near to that of (4) is

$$\left\{\left(\frac{31}{49}, \frac{9}{49}\right), \left(\frac{24}{49}, \frac{13}{49}\right), \left(\frac{19}{49}, \frac{17}{49}\right), \left(\frac{15}{49}, \frac{21}{49}\right), \left(\frac{11}{49}, \frac{25}{49}\right)\right\}.$$

5. Generators of value semigroups of some types of plane valuations

As we said at the end of Section 2.1, we close this paper describing, in a detailed manner, the minimal generating sets of the value semigroups of those valuations we have used. For any numerical semigroup Γ, there exists a germ of plane curve (given by an element in R) whose value semigroup is Γ and conversely, the value semigroup of a germ of curve as above is ever numerical [2, Proposition 5.1.5]. Plane valuations have a deep relation with germs of plane curves. Indeed, valuations of type A are defined by a suitable chosen pencil of germs of plane curves [16]. This makes the semigroup of a type A valuation to be the same as the one of any generator of the mentioned pencil. So, the semigroup S of a plane valuation ν of type A is a numerical semigroup. Assuming that $\{\bar{\beta}_i^*\}_{i=0}^g$ is its minimal set of generators, one can get rational numbers $\beta_i' = m_{i-1}^*/e_{i-1}^*$, $1 \leqslant i \leqslant g$ (see (5) later), that determine together with a positive integer $\bar{\beta}_{g+1}^*$, the structure of the (finite) sequence of quadratic transformations attached to the valuation ν. In fact, the essential information is codified in the Euclidian algorithm of the pairs (m_{i-1}^*, e_{i-1}^*) [16].

Assume that S is the value semigroup of a plane valuation ν of type B-II-a, C or D. Any valuation of these types (in fact, any plane valuation) can be regarded as a limit of a set $\{\nu_j\}_{j\geqslant 1}$ of plane valuations of type A. The difference among distinct types depends on the different ways to take at infinity either the number $\bar{\beta}_{g+1}^*$ or the Euclidean algorithm for the last pair (m_{g-1}^*, e_{g-1}^*) attached to the number β_g'. Next we explain this in more detail, showing how to obtain generators for the value semigroup of the above types of valuations.

It is possible to describe the semigroup S from the numerical semigroup S^* of any valuation ν_j, $j \gg 0$. Let us see how to do it. Consider a minimal set of generators of S^*, $\{\bar{\beta}_i^*\}_{i=0}^r$, and set $e_i^* := \gcd(\bar{\beta}_0^*, \bar{\beta}_1^*, \ldots, \bar{\beta}_i^*)$, $0 \leqslant i \leqslant r$, $n_0 := 1$ and $n_i := e_{i-1}^*/e_i^*$, for $1 \leqslant i \leqslant r$. $e_i^* > 1$ except $e_r^* = 1$. It also holds that $n_i\bar{\beta}_i^* < \bar{\beta}_{i+1}^*$. Now, taking into account also the value $\bar{\beta}_{r+1}^*$, we define the following set of rational numbers $\beta_0' = 1$, and

$$\beta_i' = \frac{\bar{\beta}_i^* - n_{i-1}\bar{\beta}_{i-1}^*}{e_{i-1}^*} + 1, \tag{5}$$

$1 \leqslant i \leqslant r+1$. Due to that ν is a limit of a sequence of type A valuations and since the structure of the resolution process (sequence of quadratic transformations) attached to the valuations ν_j is provided by the continued fraction determined by the previous elements β_i', the semigroup of values of ν will be given by taking at infinity the above continued fractions. We are only interested in certain types of valuations (with finitely generated semigroup), so we have to take at infinity either β_r' (here, the element β_{r+1}' is always equal to 1) or β_{r+1}'. For the sake of homogeneity, we shall put $r = g-1$ if ν is of type B-II-a and $r = g$ otherwise.

– If ν is of type D, we must take at infinity the value r of the continued fraction $\langle a_0; a_1, \ldots, a_{r-1}, a_r\rangle$ of $\beta_g' - 1$ obtaining the continued fraction $\langle a_0; a_1, \ldots, a_{r-1}, \alpha\rangle$ attached with some nonrational real number β_{g+}' given by another nonrational number α. Then S is spanned by a family of real numbers $\{\bar{\beta}_i\}_{i=0}^g$ such that $\bar{\beta}_i = \bar{\beta}_i^*/\bar{\beta}_0^*$, $0 \leqslant i \leqslant g-1$, and

$$\bar{\beta}_g = n_{g-1}\bar{\beta}_{g-1} + \beta_{g+}' \frac{e_{g-1}^*}{e_0^*},$$

formula that comes from (5), after normalizing the values dividing by $\bar{\beta}_0^* = e_0^*$.

– If ν is of type C, we must take at infinity the value a_r of the continued fraction $\langle a_0; a_1, \ldots, a_{r-1}, a_r\rangle$ of $\beta_g' - 1$. This will be done by expressing a_r as the 'quotient' of $(1,0)$ by $(0,1)$. Indeed, to get the elements in $\mathbb{N}^2$, $\{\bar{\beta}_i\}_{i=0}^g$, that generate S, first we must set $\beta_g' = m_{g-1}^*/e_{g-1}^*$, consider the Euclidian algorithm

$$m^*_{g-1} = a_1 q^*_1 + r_1,$$
$$q^*_1 = a_2 q^*_2 + r_2,$$
$$\vdots$$
$$q^*_{r-1} = a_r q^*_r,$$

where $q^*_1 = e^*_{g-1}$. Changing in the above array q^*_{r-1} by $q_{r-1} = (1,0)$ and q^*_r by $q_r = (0,1)$ and doing reverse substitution, we get elements in $\mathbb{N}^2$, q_i and m_{g-1}. Now defining $e_{g-1} := q_1$, and $e_{i-1} = n_i e_i$, we obtain values e_i, $0 \leqslant i \leqslant g-1$. The generators for S will be given by $\bar{\beta}_0 = e_0$, the equalities

$$\bar{\beta}_i - n_{i-1}\bar{\beta}_{i-1} = e_{i-1}\big(\beta'_i - 1\big),$$

whenever $1 \leqslant i < g$ and $\bar{\beta}_g = m_{g-1} + n_{g-1}\bar{\beta}_{g-1} - e_{g-1}$. Notice that all the values in the above equalities are in $\mathbb{N}^2$, except for n_{i-1}, $1 \leqslant i \leqslant g$, which are in $\mathbb{N}$ and $\beta'_i - 1$, $1 \leqslant i < g$, that are in $\mathbb{Q}$.

– Finally, if ν is of type B-II-a, then S is in $\mathbb{N}^2$ and it is spanned by the values $\bar{\beta}_i = (0, \bar{\beta}^*_i)$, $0 \leqslant i \leqslant g-1$, and $\bar{\beta}_g = (1,0)$. This is so since we must take at infinity the expansion of $\beta'_{r+1} - 1$ attached to the value $\bar{\beta}^*_{r+1}$ given in the first paragraph of this section. $\beta'_{r+1} \in \mathbb{N}$ because $e^*_r = 1$ and since we are interested in the values $\bar{\beta}^*_{g+1}$, by simplicity, we express $\beta'_{r+1} = (1,0) - n_r(0, \bar{\beta}^*_r)$ and so (5) happens.

We also give some simple examples to make easier the reading of above paragraphs: from a numerical semigroup spanned by $\bar{\beta}^*_0 = 6$, $\bar{\beta}^*_1 = 9$ and $\bar{\beta}^*_2 = 19$, one can obtain a type D plane valuation whose value semigroup S is generated by $\bar{\beta}_0 = 1$, $\bar{\beta}_1 = 3/2$ and $\bar{\beta}_2 = (1+6e)/(2e)$. Here, we have considered the value $\alpha = e \in \mathbb{R} \setminus \mathbb{Q}$.

From the same numerical semigroup, a type C plane valuation with value semigroup generated by $\bar{\beta}_0 = (2,0)$, $\bar{\beta}_1 = (3,0)$ and $\bar{\beta}_2 = (6,1)$ can be obtained. Indeed, $\beta'_1 = 3/2$, $\beta'_2 = 4/3$, $e^*_0 = 6$, $e^*_1 = 3$, $e^*_2 = 1$, $n_0 = 1$, $n_1 = 2$, $n_2 = 3$ and the Euclidian algorithm

$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1,$$

provides

$$(1,1) = 1 \cdot (1,0) + (0,1)$$
$$(1,0) = \infty \cdot (0,1).$$

Then, $m_1 = (1,1)$ and $e_1 = (1,0)$ which give the mentioned values $\bar{\beta}_i$, $1 \leqslant i \leqslant 2$.

An example of value semigroup of a type B-II-a plane valuation is that spanned by $\bar{\beta}_0 = (0,3)$, $\bar{\beta}_1 = (0,5)$ and $\bar{\beta}_2 = (1,0)$. To see it, it suffices to take at infinity the valuation of type A whose corresponding values $\bar{\beta}^*_i$, $1 \leqslant i \leqslant 2$, are $\bar{\beta}^*_0 = 3$, $\bar{\beta}^*_1 = 5$ and $\bar{\beta}^*_2 = 16$ (recall that the semigroup of values of this last valuation is generated by 3 and 5).

Remark 5.1. We could also describe generators for the remaining types of valuations but we do not include this because we have not used it.

References

[1] H.E. Andersen, O. Geil, Evaluation codes from order domain theory, Finite Fields Appl. 14 (2008) 92–123.
[2] A. Campillo, Algebroid Curves in Positive Characteristic, Lecture Notes in Math., vol. 613, Springer-Verlag, 1980.
[3] F. Delgado, C. Galindo, A. Nuñez, Saturation for valuations on two-dimensional regular local rings, Math. Z. 234 (2000) 519–550.
[4] G.L. Feng, T.R.N. Rao, Decoding of algebraic geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 37–45.
[5] C. Galindo, M. Sanchis, Evaluation codes and plane valuations, Des. Codes Crypt. 41 (2) (2006) 199–219.
[6] C. Galindo, F. Monserrat, δ-Sequences and evaluation codes defined by plane valuations at infinity, Proc. London Math. Soc. 98 (2009) 714–740.
[7] O. Geil, R. Pellikaan, On the structure of order domains, Finite Fields Appl. 8 (2002) 369–396.
[8] S. Greco, K. Kiyek, General elements in complete ideals and valuations centered at a two-dimensional regular local ring, in: Algebra, Arithmetic, and Geometry, with Applications, Springer, 2003, pp. 381–455.
[9] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: Handbook of Coding Theory, vol. 1, 1998, pp. 871–961.
[10] C.D. Jensen, Fast decoding of codes from algebraic geometry, IEEE Trans. Inform. Theory 40 (1994) 223–230.
[11] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose, T. Høholdt, Construction and decoding of a class of algebraic geometric codes, IEEE Trans. Inform. Theory 35 (1989) 811–821.
[12] J. Justesen, K.J. Larsen, H.E. Jensen, T. Høholdt, Fast decoding of codes from algebraic plane curves, IEEE Trans. Inform. Theory 38 (1992) 111–119.
[13] M. Kreuzer, L. Robbiano, Computational Commutative Algebra, Springer, 2000.
[14] J.B. Little, The ubiquity of order domains for the construction of error control codes, Adv. Math. Commun. 1 (2007) 151–171.
[15] T. Mora, Solving Polynomial Equation Systems II: Macaulay's Paradigm and Gröbner Technology, Encyclopedia of Mathematics and Its Applications, vol. 99, Cambridge University Press, 2005.
[16] M. Spivakovsky, Valuations in function fields of surfaces, Amer. J. Math. 112 (1990) 107–156.
[17] M.E. O'Sullivan, New codes for the Berlekamp–Massey–Sakata algorithm, Finite Fields Appl. 7 (2001) 293–317.
[18] A.N. Skorobogatov, S.G. Vlăduţ, On the decoding of algebraic geometric codes, IEEE Trans. Inform. Theory 36 (1990) 1051–1060.
[19] O. Zariski, P. Samuel, Commutative Algebra, vol. II, Springer-Verlag, 1960.