# Evaluation Codes from Order Domain Theory

Henning E. Andersen and Olav Geil
Department of Mathematical Sciences
Aalborg University

*The celebrated Feng-Rao bound estimates the minimum distance of codes defined by means of their parity check matrices. From the Feng-Rao bound it is clear how to improve a large family of codes by leaving out certain rows in their parity check matrices. In this paper we derive a simple lower bound on the minimum distance of codes defined by means of their generator matrices. From our bound it is clear how to improve a large family of codes by adding certain rows to their generator matrices. The new bound is very much related to the Feng-Rao bound as well as to Shibuya and Sakaniwa's bound in [28]. Our bound is easily extended to deal with any generalized Hamming weights. We interpret our methods into the setting of order domain theory. In this way we fill in an obvious gap in the theory of order domains.*

*Keywords: Affine variety code, evaluation code, Feng-Rao bound, footprint, generalized Hamming weight, geometric Goppa code, Gröbner basis, minimum distance, order bound, order domain, well-behaving pair*

## 1 Introduction

In [5] and [6] Feng and Rao introduced a bound on the minimum distance of codes defined by means of their parity check matrices. This bound is known today as the Feng-Rao bound. The Feng-Rao bound is a rather global one. For instance the BCH-bound and the usual bound from algebraic geometry on the minimum distance of duals of one-point geometric Goppa codes can be viewed as being consequences of it. Even from the Feng-Rao bound it is clear how to improve on the latter one. The Feng-Rao bound further allows one to improve on many codes by leaving out certain rows in their parity check matrices without decreasing their designed minimum distance. In particular the Feng-Rao bound gives us a way of constructing improved duals of one-point geometric Goppa codes.

The Feng-Rao bound has been given many interpretations, two of which will be very important to us in this paper. In [16] Høholdt, van Lint and Pellikaan introduced a new type of algebraic structures that are so to speak manufactured to give codes for which the Feng-Rao bound easily applies. These algebraic structures are known today as order domains. By Høholdt et al.'s construction we have a way of generalizing the construction of duals of one-point geometric Goppa codes and improved such ones to algebraic structures of higher transcendence degrees. Further Høholdt et al. showed how to deal with one-point geometric Goppa codes in the language of order domain theory. In particular they gave a simplified proof of the usual bound from algebraic geometry on the minimum distance of one-point geometric Goppa codes. What is obviously missing in the order domain theory is an improved bound on the minimum

distance of one-point geometric Goppa codes, an improved construction of one-point geometric Goppa codes and finally a generalization of the bound and the improved construction to algebraic structures of higher transcendence degrees. In this paper we will solve all these problems in the affirmative. To derive the missing results from order domain theory it proves fruitful to consider first the problems in the most general set-up in which the Feng-Rao bound applies. This set-up was described by Miura in [21] and [22] and by Miura and Matsumoto in [20]. Here no algebraic structure is involved but only a basis for $\mathbb{F}_q^n$. Miura and Matsumoto's description uses besides traditional linear algebra the component wise product of the vectors in $\mathbb{F}_q^n$ and some related concepts. In this language already one bound is known that deals with the minimum distance of codes defined by means of their generator matrix. This is the much too little recognized bound by Shibuya and Sakaniwa in [28]. The bound that we derive in the present paper is very much related to Shibuya and Sakaniwa's bound. In particular their bound can be viewed as a consequence of the bound from the present paper. Also our bound is very much related to the Feng-Rao bound. The proof of our bound however is even simpler than the proof of the Feng-Rao bound. Our bound is easily extended to deal with all the generalized Hamming weights as is the Feng-Rao bound.

The paper is organized as follows. In Section 2 we show how our new bound applies in the case of Reed-Solomon codes. The idea is to give the reader a feeling of the concepts to be introduced more formally in later sections. In Section 3 we give a precise description of our new bound and our new code constructions in Miura and Matsumoto's general set-up of linear codes. In Section 4 we consider the connection to the Feng-Rao bound and in Section 5 we are concerned with the connection to Shibuya and Sakaniwa's bound. Next in Section 6 we translate our findings from Section 3 into the setting of order domain theory. This allows us to deal with the one-point geometric Goppa codes in Section 7. In Section 8 we derive some practical tools for the implementation of our methods in the order domain theoretical set-up. Section 9 contains a number of examples and Section 10 is the conclusion. Finally in Appendix A we establish a connection between our new results and the theory of affine variety codes.

## 2 A motivating example

In this section we derive the well-known minimum distance of the Reed-Solomon codes in an untraditional way. The idea is to give the reader a feeling of the concepts to be introduced more formally in the next section.

**Example 1.** *Let $P_1, \ldots, P_q$ be the elements in the field $\mathbb{F}_q$. Write $n := q$ and consider the evaluation map $ev : \mathbb{F}_q[X] \to \mathbb{F}_q^n$ given by $ev(F) := (F(P_1), \ldots, F(P_n))$. The set*

$$B = \{\boldsymbol{b}_1 = ev(1), \boldsymbol{b}_2 = ev(X), \ldots, \boldsymbol{b}_n = ev(X^{n-1})\}$$

*constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. For $k = 1, \ldots, n$ the*

$[n = q, k]$ *Reed-Solomon code is given by*

$$C_k := span_{\mathbb{F}_q}\{ev(\boldsymbol{b}_i) \mid i = 1, \ldots, k\}.$$

*We now derive the bound* $d(C_k) \geq n - k + 1$ *in an untraditional way. Consider any code word* $\boldsymbol{c} \in C_k$*, say*

$$\boldsymbol{c} = \sum_{t=1}^{i} \alpha_t \boldsymbol{b}_t = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right), \quad \alpha_1, \ldots, \alpha_i \in \mathbb{F}_q, \quad \alpha_i \neq 0 \text{ and } i \leq k. \tag{1}$$

*To estimate the Hamming weight of* $\boldsymbol{c}$ *we will make use of the component wise product on* $\mathbb{F}_q^n$ *given by* $\boldsymbol{e} * \boldsymbol{f} = (e_1 f_1, \ldots, e_n f_n)$*. We have*

$$\begin{array}{rcccl}
\boldsymbol{c} * \boldsymbol{b}_1 & = & ev\left(\sum_{t=1}^{i} \alpha_i X^{t-1}\right) & \in & C_i \backslash C_{i-1} \\
\boldsymbol{c} * \boldsymbol{b}_2 & = & ev\left(\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) X\right) = ev\left(\sum_{t=1}^{i} \alpha_t X^{t}\right) & \in & C_{i+1} \backslash C_i \\
 & \vdots & & & \\
\boldsymbol{c} * \boldsymbol{b}_{n-i+1} & = & ev\left(\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) X^{n-i}\right) = ev\left(\sum_{t=1}^{i} \alpha_t X^{n-i+t-1}\right) & \in & C_n \backslash C_{n-1}
\end{array} \tag{2}$$

*Hence, the vectors* $\boldsymbol{c} * \boldsymbol{b}_1, \boldsymbol{c} * \boldsymbol{b}_2, \ldots, \boldsymbol{c} * \boldsymbol{b}_{n-i+1}$ *are linearly independent and therefore*

$$span_{\mathbb{F}_q}\{\boldsymbol{c} * \boldsymbol{b}_1, \boldsymbol{c} * \boldsymbol{b}_2, \ldots, \boldsymbol{c} * \boldsymbol{b}_{n-i+1}\} \tag{3}$$

*is a space of dimension* $n - i + 1$*. Now denote* $\boldsymbol{e}_1 := (1, 0, \ldots, 0)$*,* $\boldsymbol{e}_2 := (0, 1, 0, \ldots, 0)$*, ...,* $\boldsymbol{e}_n := (0, \ldots, 0, 1)$ *and let* $l$ *be the Hamming weight of* $\boldsymbol{c}$*, say* $\mathrm{Supp}(\boldsymbol{c}) = \{i_1, \ldots, i_l\}$*. But then*

$$span_{\mathbb{F}_q}\{\boldsymbol{c} * \boldsymbol{d} \mid \boldsymbol{d} \in \mathbb{F}_q^n\} = span_{\mathbb{F}_q}\{\boldsymbol{e}_{i_1}, \ldots, \boldsymbol{e}_{i_l}\} \tag{4}$$

*follows immediately. Obviously the* $n-i+1$*-dimensional space in (3) is contained in the* $l$*-dimensional space in (4) and therefore* $w_H(\boldsymbol{c}) = l \geq n - i + 1$ *holds. We have shown*

$$d(C_k) \geq \min\{n - i + 1 \mid i = 1, \ldots, k\} = n - k + 1$$

*and as usual the result* $d(C_k) = n - k + 1$ *now follows from the Singleton bound.*

In the example above we used the algebraic structure of the polynomial ring $\mathbb{F}_q[X]$ heavily. Without this it would have been very difficult for us to conclude the crucial inclusions in (2). Therefore when looking for classes of codes for which the above method can be applied in a manageable way we should look for codes defined from some algebraic structures. Nevertheless, we continue the description of our new bound by considering how it applies in the general case of any linear code. In this general set-up our method is not really manageable but the proof of our bound will be simplified as much as possible. Later in the paper we will see how our new bound applies very natural to the case of codes coming from order domains. In this set-up our bound will be just as manageable as the Feng-Rao bound.

## 3 The new bound

This section contains a description of our new method in the general setting of linear codes. We will see how to deal with not only the minimum distance but along the way with all the generalized Hamming weights. We will use the motivating example from the previous section as a guideline.

Consider the following definition of a linear code.

**Definition 2.** *Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$ and let $G \subseteq B$. We define the $\#G$ dimensional code $C(B, G)$ by $C(B, G) := span_{\mathbb{F}_q}\{\boldsymbol{b} \mid \boldsymbol{b} \in G\}$. The dual code (of dimension $n - \#G$) is denoted $C^{\perp}(B, G)$.*

Our method calls for the following set of spaces.

**Definition 3.** *Let $L_{-1} := \emptyset$, $L_0 := \{\boldsymbol{0}\}$ and $L_l := span_{\mathbb{F}_q}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l\}$ for $l = 1, \ldots, n$.*

We obviously have a chain of spaces $\{\boldsymbol{0}\} = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_{n-1} \subsetneq L_n = \mathbb{F}_q^n$. Hence, we can define a function as follows.

**Definition 4.** *Define $\bar{\rho} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ by $\bar{\rho}(\boldsymbol{v}) = l$ if $\boldsymbol{v} \in L_l \backslash L_{l-1}$.*

Recall from the motivating example in the previous section that given a code word $\boldsymbol{c} \in C(B, G)$, we would like to find as many different numbers $s$ as possible such that a basis element $\boldsymbol{b}_j$ exist with $\boldsymbol{c} * \boldsymbol{b}_j \in L_s \backslash L_{s-1}$. This will allow us to give a good estimate of the Hamming weight of $\boldsymbol{c}$. Expressed in the language of the function $\bar{\rho}$ we look for values $s$ such that a $\boldsymbol{b}_j$ exists with $\bar{\rho}(\boldsymbol{c} * \boldsymbol{b}_j) = s$. In general it is not an easy task to find $\bar{\rho}(\boldsymbol{c} * \boldsymbol{b}_j)$. This is why we now define the concept of well-behaving pairs.

**Definition 5.** *Let $I := \{1, 2, \ldots, n\}$. An ordered pair $(i, j) \in I^2$ is said to be well-behaving (WB) if $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ for all $u$ and $v$ with $1 \leq u \leq i, 1 \leq v \leq j$ and $(u, v) \neq (i, j)$. A little less restrictive an ordered pair $(i, j) \in I^2$ is said to be weakly well-behaving (WWB) if $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_j) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ for $u < i$ and $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ for $v < j$.*

Consider similar to (1) a word

$$\boldsymbol{c} = \sum_{t=1}^{v} \alpha_t \boldsymbol{b}_{i_t}, \text{ with } i_1 < \cdots < i_v \text{ and } \alpha_v \neq 0. \tag{5}$$

If $(i_v, j)$ is WWB we have $\bar{\rho}(\boldsymbol{b}_{i_t} * \boldsymbol{b}_j) < \bar{\rho}(\boldsymbol{b}_{i_v} * \boldsymbol{b}_j)$ for $t = 1, 2, \ldots, v-1$ and therefore we can conclude that

$$\bar{\rho}(\boldsymbol{c} * \boldsymbol{b}_j) = \bar{\rho}\left(\sum_{t=1}^{v} \alpha_t (\boldsymbol{b}_{i_t} * \boldsymbol{b}_j)\right) = \bar{\rho}(\boldsymbol{b}_{i_v} * \boldsymbol{b}_j).$$

So to estimate the number of $s$'s such that a basis element $\boldsymbol{b}_j$ exists with $\bar{\rho}(\boldsymbol{c} * \boldsymbol{b}_j) = s$ we can simply count the size of the following set (here $i$ should be replaced by $i_v$).

**Definition 6.**

$$\Lambda_i \;:=\; \{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \text{ with } \quad (i,j) \text{ } WWB\}$$

**Remark 7.** *If we are given two different numbers $j_1$ and $j_2$ such that both $(i, j_1)$ and $(i, j_2)$ are weakly well behaving, then by the very weakly well behaving property we must have $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_{j_1}) \neq \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_{j_2})$. Hence, counting for a fixed number $i$ the size of the set $\Lambda_i$ is the same as counting the number of weakly well behaving pairs $(i, j)$, $j \in I$.*

We are now in the position that we can state the new bound for the minimum distance of a linear code.

**Theorem 8.** *The minimum distance of $C(B, G)$ satisfies*

$$d(C(B,G)) \;\geq\; \min\{\#\Lambda_i \mid \boldsymbol{b}_i \in G\}$$

*Proof.* Let $\boldsymbol{c} \in C(B,G)\backslash\{\boldsymbol{0}\}$ then $\boldsymbol{c}$ is of the form in (5) with $i_t$ satisfying $\boldsymbol{b}_{i_t} \in G$ for all $t = 1, \ldots, v$. By Definition 6 and the weakly well-behaving property there exists numbers $1 \leq l_1 < \ldots < l_{\#\Lambda_{i_v}} \leq n$ and related numbers $j_1, \ldots, j_{\#\Lambda_{i_v}} \in I$ such that

$$\begin{aligned}
\boldsymbol{c} * \boldsymbol{b}_{j_1} &\in L_{l_1} \backslash L_{l_1 - 1} \\
\boldsymbol{c} * \boldsymbol{b}_{j_2} &\in L_{l_2} \backslash L_{l_2 - 1} \\
&\vdots \\
\boldsymbol{c} * \boldsymbol{b}_{j_{\#\Lambda_{i_v}}} &\in L_{l_{\#\Lambda_{i_v}}} \backslash L_{l_{\#\Lambda_{i_v}} - 1}
\end{aligned}$$

Hence, $\boldsymbol{c} * \boldsymbol{b}_{j_1}, \ldots, \boldsymbol{c} * \boldsymbol{b}_{j_{\#\Lambda_{i_v}}}$ are linearly independent. But then

$$\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{c} * \boldsymbol{b}_{j_1}, \ldots, \boldsymbol{c} * \boldsymbol{b}_{j_{\#\Lambda_{i_v}}}\} \tag{6}$$

is of dimension $\#\Lambda_{i_v}$. As in the motivating example the space

$$\{\boldsymbol{c} * \boldsymbol{d} \mid \boldsymbol{d} \in \mathbb{F}_q^n\} \tag{7}$$

is of dimension equal to the Hamming weight of $\boldsymbol{c}$. The space in (6) is contained in the space (7) and we conclude that the Hamming weight of $\boldsymbol{c}$ must be at least equal to $\#\Lambda_{i_v}$. But then of course also the Hamming weight of $\boldsymbol{c}$ is at least equal to $\min\{\#\Lambda_i \mid \boldsymbol{b}_i \in G\}$. □

As we will see in a moment Theorem 8 can be extended to deal not only with the minimum distance but with all generalized Hamming weights. Also the theorem can sometimes be improved slightly. The small improvement will be of importance when we in a later section compare our bound to the bound by Shibuya and Sakaniwa.

Before giving the extended version of Theorem 8 we remind the reader of the definition of generalized Hamming weights. These where introduced by Wei

in [30] for cryptographic purposes. Recall that the support of a set $S$, $S \subseteq \mathbb{F}_q^n$ is defined by

$$\mathrm{Supp}(S) := \{i \mid c_i \neq 0 \ \text{ for some } \ \boldsymbol{c} = (c_1, \ldots, c_n) \in S\}.$$

The $t$th generalized Hamming weight of a code $C$ is defined by

$$d_t(C) := \min\{\#Supp(S) \mid S \text{ is a linear subcode of } \ C \ \text{ of dimension } \ t\}.$$

The extension of Theorem 8 calls for a definition.

**Definition 9.** *For $\{i_1, \ldots, i_t\} \subseteq I$ define*

$$\bar{\sigma}(i_1, \ldots i_t) \ := \ \# \left( \left( \cup_{s=1}^{t} \Lambda_{i_s} \right) \cup \{i_1, \ldots, i_t\} \right).$$

*In particular, $\bar{\sigma}(i) = \# \left( \Lambda_i \cup \{i\} \right)$.*

The extended version of Theorem 8 is.

**Theorem 10.** *Let $G \subseteq B$ with $\#G = k$ be fixed. For $t = 1, \ldots, k$ the generalized Hamming weight $d_t(C(B, G))$ is at least equal to*

$$\min\{\bar{\sigma}(a_1, a_2, \ldots, a_t) \mid 1 \leq a_1 < \cdots < a_t \leq n \text{ and } \{\boldsymbol{b}_{a_1}, \boldsymbol{b}_{a_2}, \ldots, \boldsymbol{b}_{a_t}\} \subseteq G\}.$$

*In particular the minimum distance of $C(B, G)$ is at least equal to*

$$\min\{\bar{\sigma}(i) \mid \boldsymbol{b}_i \in G\} = \min\{\#(\Lambda_i \cup \{i\}) \mid \boldsymbol{b}_i \in G\}.$$

*Proof.* Denote $G = \{\boldsymbol{b}_{i_1}, \boldsymbol{b}_{i_2}, \ldots, \boldsymbol{b}_{i_k}\}$ where $i_1 < i_2 < \cdots < i_k$ holds. Let $D \subseteq C(B, G)$ be a subspace of dimension $t$, $t \leq k$. Consider basis vectors $\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t$ for $D$

$$\boldsymbol{d}_u = \sum_{s=1}^{k} \alpha_s^{(u)} \boldsymbol{b}_{i_s}, \ u = 1, 2, \ldots, t.$$

We will assume that

$$\max\{s \mid \alpha_s^{(v)} \neq 0\} \neq \max\{s \mid \alpha_s^{(w)} \neq 0\}$$

holds for any $v, w$ with $v \neq w$. If this is not the case from the beginning we can make it hold by performing Gaussian elimination. As by definition

$$\bar{\rho}(\boldsymbol{d}_u) = \max\{i_s \mid \alpha_s^{(u)} \neq 0\}$$

holds the above assumption corresponds to assuming that $\bar{\rho}(\boldsymbol{d}_v) \neq \bar{\rho}(\boldsymbol{d}_w)$ for $v \neq w$. Let $a_u := \bar{\rho}(\boldsymbol{d}_u)$ for $u = 1, 2, \ldots, t$. We observe that if $(a_u, j)$ is WWB for some $j \in \{1, 2, \ldots, n\}$ and $\bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l$ then by the very definition of WWB we have

$$\bar{\rho}(\boldsymbol{d}_u * \boldsymbol{b}_j) = \bar{\rho}\left( \sum_{s=1}^{k} \alpha_s^{(u)} (\boldsymbol{b}_{i_s} * \boldsymbol{b}_j) \right) = \bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l.$$

as well. Hence, the set

$$S \;:=\; \cup_{u=1}^{t}\{\boldsymbol{d}_u * \boldsymbol{b}_j \mid (a_u, j) \text{ is WWB }\}$$

contains at least $\#\left(\cup_{u=1}^{t}\Lambda_{a_u}\right)$ linearly independent vectors. Consider now the numbers $a_u$, $u = 1, \ldots, t$. We have $a_u = \bar{\rho}(\boldsymbol{d}_u) = \bar{\rho}(\boldsymbol{d}_u * (1, 1, \ldots, 1))$ and therefore the set

$$S' \;:=\; (\cup_{u=1}^{t}\{\boldsymbol{d}_u * \boldsymbol{b}_j \mid (a_u, j) \text{ is WWB }\}) \cup \{\boldsymbol{d}_u * (1, 1, \ldots, 1) \mid u = 1, \ldots, t\}$$

contains at least $\#\left(\left(\cup_{u=1}^{t}\Lambda_{a_u}\right) \cup \{a_1, \ldots, a_t\}\right) = \bar{\sigma}(a_1, \ldots, a_t)$ linearly independent vectors. Hence,

$$\bar{\sigma}(a_1, \ldots, a_t) \;\leq\; \dim(\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{f} \mid \boldsymbol{f} \in S'\}). \tag{8}$$

Consider next the set

$$T \;:=\; \{\boldsymbol{d}_u * \boldsymbol{e} \mid u = 1, \ldots, t \;\text{ and }\; \boldsymbol{e} \in \mathbb{F}_q^n\}.$$

The space $\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{f} \mid \boldsymbol{f} \in T\}$ is isomorphic to $\mathbb{F}_q^{\#\mathrm{Supp}(\{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_t\})}$ and as $\mathrm{Supp}(D) = \mathrm{Supp}(\{\boldsymbol{d}_1, \ldots, \boldsymbol{d}_t\})$ we get

$$\#\mathrm{Supp}(D) \;=\; \dim(\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{f} \mid \boldsymbol{f} \in T\}). \tag{9}$$

But $S' \subseteq T$ implying $\dim(\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{f} \mid \boldsymbol{f} \in S'\}) \leq \dim(\mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{f} \mid \boldsymbol{f} \in T\})$ and by use of (8) and (9) we therefore conclude $\bar{\sigma}(a_1, \ldots, a_t) \leq \#\mathrm{Supp}(D)$. The proof is complete. □

Given any fixed value $\delta$ the celebrated Feng-Rao bound tells us how to choose $G$ such that $C^{\perp}(B, G)$ has designed minimum distance at least $\delta$ and is of as large dimension as possible. In a similar manner it is from Theorem 10 obvious given any fixed value $\delta$ how to choose $G$ such that $C(B, G)$ has designed minimum distance at least $\delta$ and is of as large dimension as possible. The improved codes we get in this way are the $\widetilde{\mathcal{E}}(\delta)$ codes below. For use in Section 6 we also define the more naive codes $\mathcal{E}(s)$.

**Definition 11.** *Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$. For $s = 1, 2, \ldots, n$ and $\delta = 0, 1, \ldots, n$ define*

$$\begin{aligned}\mathcal{E}(s) \;&:=\; \mathit{span}_{\mathbb{F}_q}\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_s\}\\ \widetilde{\mathcal{E}}(\delta) \;&:=\; \mathit{span}_{\mathbb{F}_q}\{\boldsymbol{b}_i \mid \bar{\sigma}(i) \geq \delta\}\end{aligned}$$

From our motivating example in Section 2 we see that it is very natural to consider the Reed-Solomon codes as being of the form $\mathcal{E}(s)$. We will see in Section 6 that it is also natural to consider geometric Goppa codes as being of the form $\mathcal{E}(s)$. Furthermore we will see in Section 9 that the class of codes $\widetilde{\mathcal{E}}(\delta)$ contains some well-studied nice codes. We have the following theorem.

**Theorem 12.** *The minimum distance of $\mathcal{E}(s)$ is at least equal to* $\min\{\bar{\sigma}(i) \mid i = 1, \ldots, s\}$. *The minimum distance of $\widetilde{\mathcal{E}}(\delta)$ is at least equal to $\delta$.*

*Proof.* We have $\mathcal{E}(s) = C(B,G)$ with $G = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s\}$ and we have $\widetilde{\mathcal{E}}(\delta) = C(B,G)$ with $G = \{\boldsymbol{b}_i \mid \bar{\sigma}(i) \geq \delta\}$. The result now follows from Theorem 10. □

We conclude this section by noting that Theorem 10 applies in an even more general setting than described above. We put the description of this in the following remark that can easily be skipped at a first reading of the paper.

**Remark 13.** *Recall, that a pair $(i,j)$ is called weakly well-behaving if $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_j) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ as well as $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ holds. However, by inspection of the proofs of Theorem 8 and Theorem 10 it is clear that it is only the first of the two conditions that is of significance for Theorem 8 and Theorem 10 to hold. This suggests that we can introduce an even less restrictive concept that we will call one-way well behaving. Further, from the proofs of Theorem 8 and Theorem 10 it is seen to be of no significance that $\boldsymbol{b}_j$ should be in $B$. Hence, we can consider two bases $B$ and $B'$. The basis $B$ is the one we use for the code construction whereas the basis $B'$ is the one from which we choose the $\boldsymbol{b}_j$'s to be used in the estimation of the minimum distances. Even, it is seen to be of no significance that $B'$ should be a basis of $\mathbb{F}_q^n$ merely as just being some subset of $\mathbb{F}_q^n$. For an outline of these observations we invite the reader to consult [13]. In the case of dual codes $C^{\perp}(B,G)$ the idea of using two bases $B$ and $B'$ has proven fruitful in the study of cyclic codes. It might be that there is also some application of using two basis $B$ and $B'$ in the case of codes $C(B,G)$ as well.*

# 4 The Feng-Rao bound for generalized Hamming weights

The bound in Theorem 8 and Theorem 10 is very much related to the Feng-Rao bound for the codes $C^{\perp}(B,G)$. To see this we will need a few definitions.

**Definition 14.** *For $l = 1, \ldots, n$ let*

$$V_l \;:=\; \{i \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \;\; \textit{for some} \;\; \boldsymbol{b}_j \in B \;\textit{with}\; (i,j) \;\; \textit{WWB}\}$$

*For $\{l_1, l_2, \ldots, l_t\} \subseteq I$ define*

$$\bar{\mu}(l_1, \ldots l_t) \;:=\; \#\left((\cup_{s=1,\ldots,t} V_{l_s}) \cup \{l_1, \ldots, l_t\}\right)$$

*In particular we define*

$$\bar{\mu}(l) \;:=\; \#\left(V_l \cup \{l\}\right)$$

We can now state the Feng-Rao bound for generalized Hamming weights. Our formulation is relatively close to the original formulation by Feng and Rao concerning the minimum distance.

**Theorem 15.** *The $t$th generalized Hamming weight $d_t(C^{\perp}(B,G))$ satisfies*

$$d_t(C^{\perp}(B,G)) \geq \min\{\bar{\mu}(a_1, \ldots, a_t) \mid a_i \neq a_j \textit{ for } i \neq j \textit{ and } \{\boldsymbol{b}_{a_1}, \ldots, \boldsymbol{b}_{a_t}\} \subseteq B \backslash G\}.$$

*In particular*

$$d(C^{\perp}(B,G)) \;\geq\; \min\{\bar{\mu}(a) \mid \boldsymbol{b}_a \in B \backslash G\}.$$

The proof of the above version of the Feng-Rao bound can be found in [13]. The proof there uses many of the same ideas as does the proof of Theorem 10. In the examples at the end of the paper we will see that the two bounds sometimes gives similar results and sometimes they do not.

The similarity between the Feng-Rao bound and the bounds in Theorem 8 and Theorem 10 is almost striking. With the simplicity of the proof of Theorem 8 in mind one may ask why the bound in Theorem 8 has not been discovered simultaneously to or shortly after the Feng-Rao bound. The answer to this question probably is that in most interpretations the Feng-Rao bound is described in the language of the algebraic structures used for the code construction. Hence, the complexity of the algebraic structures used for the code construction may have been an obstacle.

In Section 6 we will need the following codes.

**Definition 16.** *Given the basis* $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ *we define*

$$\begin{aligned} \mathcal{C}(s) &:= C^{\perp}(B,G) \quad \textit{with} \quad G = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s\} \\ \widetilde{\mathcal{C}}(\delta) &:= C^{\perp}(B,G) \quad \textit{with} \quad G = \{\boldsymbol{b}_i \mid \bar{\mu}(i) < \delta\} \end{aligned}$$

It is straightforward to apply the Feng-Rao bound to the codes $\mathcal{C}(s)$ and $\widetilde{\mathcal{C}}(\delta)$. In particular we get $d(\widetilde{\mathcal{C}}(\delta)) \geq \delta$. The codes $\widetilde{\mathcal{C}}(\delta)$ are often called improved dual codes or Feng-Rao improved codes.

## 5 The connection to Shibuya and Sakaniwa's work

In the paper [28] Shibuya and Sakaniwa derived a bound on the minimum distance of $C(B,G)$ codes. This bound has been much too little appreciated in the literature. As we will see below there is a strong connection between Theorem 10 and Shibuya and Sakaniwa's bound. Shibuya and Sakaniwa's bound on the minimum distance of the codes $C(B,G)$ comes out of their extensive work with various coauthors on a bound for generalized Hamming weights of codes $C^{\perp}(B,G)$ ([24],[25], [26], [27], [29]). In the first papers Shibuya, Sakaniwa et al. observed that due to a standard result on generalized Hamming weights once all the generalized Hamming weights of the $C^{\perp}(B,G)$ are estimated by their bound one can easily derive bounds on all the generalized Hamming weights of $C(B,G)$ ([24, Th. 20], [27, Th. 3]). This of course is not a practical method for finding say the minimum distance of $C(B,G)$. However, with some more theory added Shibuya and Sakaniwa in [28] derived the following bound on the minimum distance of the codes $C(B,G)$. Recall, that

$$\Lambda_i = \{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \ \text{ for some } \boldsymbol{b}_j \in B \text{ such that } (i,j) \text{ is WWB}\}.$$

**Theorem 17 (Shibuya, Sakaniwa).** *For given* $B$ *and* $G$ *let for* $i = 1, 2, \ldots, n$, $T_i := \{\nu \mid \boldsymbol{b}_\nu \in B \backslash G\} \backslash \Lambda_i$. *Define* $t(B,G) := \max\{\#T_i \mid \boldsymbol{b}_i \in G\}$. *The minimum distance of* $C(B,G)$ *is at least* $n - k + 1 - t(B,G)$.

Note that $T_i$ relies on the choice of $G$. This means that calculations for one choice of $G$ can not be reused for another choice of $G$. In particular it is not so easy given a $B$ to see what will be the optimal choice of $G$. We now show how Shibuya and Sakaniwa's bound can be viewed as a consequence of Theorem 10.

**Proposition 18.** *The bound on the minimum distance of $C(B, G)$ in Theorem 10 is at least as good as the bound in Theorem 17.*

*Proof.* For $i = 1, 2, \ldots, n$ we have

$$\bar{\sigma}(i) = \#(\Lambda_i \cup \{i\}) \tag{10}$$

The set $T_i$ consist of the basis elements outside $G$ that does not contribute to the counting in (10). Hence, the number of basis elements outside $G$ that contribute to the counting in (10) is $n - k - \#T_i$. For $i$ such that $\boldsymbol{b}_i \in G$ the number of elements in $G$ that contribute to the counting in (10) is at least equal to $\#\{i\} = 1$. All together $n - k + 1 - \#T_i \leq \bar{\sigma}(i)$ holds for all $i$ such that $\boldsymbol{b}_i \in G$. □

The advantages of Theorem 10 in comparison to Shibuya and Sakaniwa's bound are as follows. Firstly, Theorem 10 is much simpler to implement and in the case of the minimum distance the proof of it is almost trivial. Secondly, calculations for one choice of $G$ can be reused for other choices of $G$. As a consequence Theorem 10 allow us (in a very direct way) to construct improved codes $\widetilde{E}(\delta)$. Thirdly, Theorem 10 deals not only with the minimum distance but with any generalized Hamming weights. Finally, by use of Theorem 10 one can define and deal with evaluation codes coming from order domain theory. This will be explored in the next section. Even more, in Section 7 we will see that Theorem 10 allow us to construct improved one-point geometric Goppa codes.

# 6 Codes defined from order domains

In Section 3 and Section 4 we saw how to estimate the parameters of any linear code. For the methods to be really practical we will need bases $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ for $\mathbb{F}_q^n$ for which it is easy to decide if a given ordered pair $(i, j)$ is WB (or WWB) and for which it is easy to calculate $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$. One way of deriving such bases is by using order domain theory. In this section we will give a complete description of how this is done. We will learn that our new bound fills in a major gap in the theory of order domains.

Recall from the motivating example in Section 2 how the Reed-Solomon code can be viewed as being the image of a subspace of the polynomial ring $R = \mathbb{F}_q[X]$ under an evaluation map $\mathrm{ev} : \mathbb{F}_q[X] \to \mathbb{F}_q^n$. Recall also how we in our motivating example used the degree function on $\mathbb{F}_q[X]$ to decide the value of $\bar{\rho}(\boldsymbol{c} * \boldsymbol{b}_j)$ for a number of $\boldsymbol{b}_j$'s. The idea of order domain theory is to generalize this setup to a larger class of algebraic structures called order domains. The corresponding generalization of the degree function is called an order function.

The presentation of order domain theory to be given here mostly relies on [12] where the concepts of an order function and a weight function from [16] are generalized. In our presentation we will consider only order functions that are also weight functions. These seems to be the only order functions that a relevant for coding theoretical purposes. For similar reasons we consider only order domains over finite fields.

**Definition 19.** *Let $R$ be an $\mathbb{F}_q$-algebra and let $\Gamma$ be a subsemigroup of $\mathbb{N}_0^r$ for some $r$. Let $\prec$ be a monomial ordering on $\mathbb{N}_0^r$. A surjective map $\rho : R \to \Gamma_{-\infty} := \Gamma \cup \{-\infty\}$ that satisfies the following six conditions is said to be a weight function*

- (*W*.0) $\rho(f) = -\infty$ *if and only if* $f = 0$
- (*W*.1) $\rho(af) = \rho(f)$ *for all nonzero* $a \in \mathbb{F}_q$
- (*W*.2) $\rho(f+g) \preceq \max\{\rho(f), \rho(g)\}$ *and equality holds when* $\rho(f) \prec \rho(g)$
- (*W*.3) *If* $\rho(f) \prec \rho(g)$ *and* $h \neq 0$, *then* $\rho(fh) \prec \rho(gh)$
- (*W*.4) *If $f$ and $g$ are nonzero and $\rho(f) = \rho(g)$, then there exists a nonzero $a \in \mathbb{F}_q$ such that $\rho(f - ag) \prec \rho(g)$*
- (*W*.5) *If $f$ and $g$ are nonzero then* $\rho(fg) = \rho(f) + \rho(g)$.

*An $\mathbb{F}_q$-algebra with a weight function is called an order domain over $\mathbb{F}_q$. The triple $(R, \rho, \Gamma)$ is called an order structure and $\Gamma$ is called the value semigroup of $\rho$.*

Bases of the following form will play a fundamental role in the code construction.

**Theorem 20.** *Given a weight function then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ constitutes a basis for $R$ as a vector space over $\mathbb{F}_q$. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma := \{f \in R \mid \rho(f) \preceq \gamma\}$.*

A basis $\mathcal{B}$ as above is called a well-behaving basis. Besides the trivial case $R = \mathbb{F}_q$ order domains over $\mathbb{F}_q$ are always of transcendence degree at least 1. Hence, for non-trivial order domains the well-behaving basis $\mathcal{B}$ consists of infinitely many elements. We will always assume that the order domain under consideration is non-trivial and we will always assume that a well-behaving basis $\mathcal{B}$ has been chosen.

**Example 21.** *Consider the quotientring $R := \mathbb{F}_9[X, Y]/I$ where $I$ is the ideal generated by the Hermitian polynomial $X^4 - Y^3 - Y$. It is well-known that the set*

$$\{X^\alpha Y^\beta + I \mid 0 \leq \alpha, 0 \leq \beta < 3\} \tag{11}$$

*constitutes a basis for $R$ as a vectorspace over $\mathbb{F}_9$. We now define $\rho(X^\alpha Y^\beta + I) := \alpha 3 + \beta 4$ for $0 \leq \alpha$ and $0 \leq \beta < 3$. That is, $\rho$ is defined on every element in our basis. By use of the rules* (*W*.0), (*W*.1) *and* (*W*.2) *$\rho$ is extended to a weightfunction on $R$. We have $\Gamma = \langle 3, 4 \rangle$ (here $\langle s_1, \ldots, s_r \rangle$ means the semigroup generated by $s_1, \ldots, s_r$). The basis in (11) is an example of a well-behaving basis for the order domain $R$.*

The maps to be used in the code constructions will be of the following general form.

**Definition 22.** *Let $R$ be an $\mathbb{F}_q$-algebra. A surjective map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if $\varphi$ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$.*

It is now natural to let the elements in the basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ for $\mathbb{F}_q^n$ be of the form $\varphi(f_\lambda)$ for $n$ different values of $\lambda$. The values $\alpha(1), \ldots, \alpha(n)$ in the the next definition will prove to be a clever choice for the $\lambda$'s.

**Definition 23.** *Let $\alpha(1) := \mathbf{0}$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in $\Gamma$ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

The following theorem is easily proven.

**Theorem 24.** *Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be as in Definition 23. The set*

$$B := \{\boldsymbol{b}_1 := \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 := \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n := \varphi(f_{\alpha(n)})\} \tag{12}$$

*constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. For any $\boldsymbol{c} \in \mathbb{F}_q^n$ there exists a unique ordered set $(\beta_1, \beta_2, \ldots, \beta_n)$, $\beta_i \in \mathbb{F}_q$ such that $\boldsymbol{c} = \varphi\left(\sum_{i=1}^n \beta_i f_{\alpha(i)}\right)$. The function $\bar{\rho} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ corresponding to $B$ is given by*

$$\bar{\rho}(\boldsymbol{c}) = \begin{cases} 0 & \text{if } \boldsymbol{c} = 0 \\ \max\{i \mid \beta_i \neq 0\} & \text{otherwise} \end{cases}$$

**Example 25.** *This is a continuation of Example 21. The Hermitian polynomial $X^4 - Y^3 - Y$ has 27 zeros $P_1, \ldots, P_{27}$. We define a morphism $\varphi : R \to \mathbb{F}_9^{27}$ by $\varphi(F(X, Y) + I) := (F(P_1), \ldots, F(P_{27}))$ and get by inspection the values of $\alpha(i)$ and $\boldsymbol{b}_i = \varphi(F(i) + I)$, $i = 1, \ldots, 27$ as described in the table below.*

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha(i)$ | 0 | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| $F(i)$ | 1 | $X$ | $Y$ | $X^2$ | $XY$ | $Y^2$ | $X^3$ | $X^2Y$ | $XY^2$ | $X^4$ | $X^3Y$ | $X^2Y^2$ | $X^5$ | $X^4Y$ | $X^3Y^2$ |

| $i$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha(i)$ | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 28 | 29 | 32 |
| $F(i)$ | $X^6$ | $X^5Y$ | $X^4Y^2$ | $X^7$ | $X^6Y$ | $X^5Y^2$ | $X^8$ | $X^7Y$ | $X^6Y^2$ | $X^8Y$ | $X^7Y^2$ | $X^8Y^2$ |

In the remaining part of this paper we will always assume that the basis $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ is of the form (12). According to our agenda we should now be concerned with studying which ordered pairs $(i, j) \in I^2$ that are well-behaving and we should be concerned with deciding the value $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$. By the following two propositions our basis $B$ is designed in a way that allow us to answer these questions for many choices of $(i, j)$. The results in the two propositions can be found in [21], [22], [20] and [28] for the case of the order domain being of transcendence degree 1 or the order domain being equal to $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$. Here we state the results explicitly and in the more general set-up of all possible weight functions (on non-trivial order domains).

**Proposition 26.** *Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be the basis in (12). If $\alpha(i), \alpha(j)$, $\alpha(l) \in \Delta(R, \rho, \varphi)$ are such that $\alpha(i) + \alpha(j) = \alpha(l)$ then $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l$ and $(i, j) \in I^2$ is WB.*

*Proof.* We first show $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l$. We have

$$
\begin{array}{l}
\alpha(i) + \alpha(j) = \alpha(l) \\
\Downarrow \\
\rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l) \\
\Downarrow \\
f_{\alpha(i)} f_{\alpha(j)} \in R_{\alpha(l)} \text{ and } f_{\alpha(i)} f_{\alpha(j)} \notin R_\gamma \text{ for any } \gamma \prec \alpha(l) \\
\Downarrow \\
\varphi(f_{\alpha(i)} f_{\alpha(j)}) \in \varphi(R_{\alpha(l)}) = L_l \text{ and } \varphi(f_{\alpha(i)} f_{\alpha(j)}) \notin L_w \text{ for any } w < l \\
\Downarrow \\
\varphi(f_{\alpha(i)} f_{\alpha(j)}) \in L_l \backslash L_{l-1} \\
\Downarrow \\
\boldsymbol{b}_i * \boldsymbol{b}_j \in L_l \backslash L_{l-1} \\
\Downarrow \\
\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l.
\end{array}
$$

Next we show that $(i, j)$ is WB. Let $1 \leq u \leq i$, $1 \leq v \leq j$ with $(u, v) \neq (i, j)$. By condition $(W.3)$ in Definition 19 we have $\rho(f_{\alpha(u)} f_{\alpha(v)}) \prec \alpha(l)$. But then by Definition 22 and Definition 23 we have $\boldsymbol{b}_u * \boldsymbol{b}_v = \varphi(f_{\alpha(u)} f_{\alpha(v)}) \in \varphi(R_\gamma) \subseteq L_{l-1}$ for some $\gamma \prec \alpha(l)$. This implies $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_v) \leq l - 1$ and consequently $(\alpha(i), \alpha(j))$ is WB. □

**Proposition 27.** *Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\beta_1 + \beta_2 = \alpha(l)$. Then $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$ holds.*

*Proof.* By definition we have $f_{\beta_1} f_{\beta_2} \in R_{\alpha(l)}$ but $f_{\beta_1} f_{\beta_2} \notin R_\gamma$ for any $\gamma \prec \alpha(l)$. By symmetry it is enough to show that $\beta_1 \in \Delta(R, \rho, \varphi)$. We will assume that this is not the case and arrive at a contradiction. That is, we will assume that there exists $\omega \in \Gamma$ such that $\omega \prec \beta_1$ and $\varphi(f_{\beta_1}) \in \varphi(R_\omega)$. But then there exists $g \in R_\omega$ with $\varphi(g) = \varphi(f_{\beta_1})$ implying that $\varphi(g f_{\beta_2}) = \varphi(f_{\beta_1} f_{\beta_2})$. By $(W.3)$ in Definition 19 and the fact that $\rho(g) \preceq \omega \prec \beta_1$ we have $\rho(g f_{\beta_2}) \prec \rho(f_{\beta_1} f_{\beta_2})$. Hence, there exists $\gamma \prec \alpha(l)$ such that $\varphi(f_{\beta_1} f_{\beta_2}) \in \varphi(R_\gamma)$. This is not possible according to the definition of $\alpha(l)$. □

As we will see in a moment with the above two propositions in hand we can easily estimate the values $\bar{\sigma}(i)$ and $\bar{\mu}(i)$ for $i = 1, \ldots, n$. We will need the following definition.

**Definition 28.** *For $\eta \in \Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define*

$$
\begin{array}{rcl}
M(\eta) & := & \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \eta + \beta = \gamma\} \\
& = & (\eta + \Gamma) \cap \Delta(R, \rho, \varphi)
\end{array}
$$

*where* $\eta+\Gamma$ *means* $\{\eta+\lambda \mid \lambda \in \Gamma\}$. *Let* $\sigma(\eta) := \#M(\eta)$. *For* $\{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R,\rho,\varphi)$ *define* $\sigma(\eta_1, \eta_2, \ldots, \eta_t) := \# \cup_{i=1}^{t} M(\eta_i)$.
*For* $\lambda \in \Gamma$ *define*

$$N(\lambda) \quad := \quad \{(\alpha,\beta) \in \Gamma^2 \mid \alpha+\beta = \lambda\}.$$

*Let* $\mu(\lambda) := \#N(\lambda)$ *if* $N(\lambda)$ *is a finite set and* $\mu(\lambda) = \infty$ *if not. For* $\{\lambda_1, \ldots, \lambda_t\} \subseteq \Gamma$ *define* $\mu(\lambda_1, \ldots, \lambda_t) := \#\left(\cup_{i=1}^{t} N(\lambda_i)\right)$ *if* $\cup_{i=1}^{t} N(\lambda_i))$ *is a finite set and* $\mu(\lambda_1, \ldots, \lambda_t) = \infty$ *if not.*

The $N$ and $\mu$ notion is a slightly modification of the notion in [16][Def. 4.8] whereas the $M$ and $\sigma$ notion is new.

**Proposition 29.** *Consider the set* $\Delta(R,\rho,\varphi) = \{\alpha(1), \ldots \alpha(n)\}$ *and the corresponding basis* $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. *For* $i = 1, \ldots, n$ *we have* $\bar{\sigma}(i) \geq \sigma(\alpha(i))$ *and* $\bar{\mu}(i) \geq \mu(\alpha(i))$. *In larger generality for* $\{a_1, \ldots, a_t\} \subseteq I$ *we have* $\bar{\sigma}(a_1, \ldots, a_t) \geq \sigma(\alpha(a_1), \ldots, \alpha(a_t))$ *and* $\bar{\mu}(a_1, \ldots, a_t) \geq \mu(\alpha(a_1), \ldots, \alpha(a_t))$.

*Proof.* By Proposition 26 and Proposition 27 we have for $i = 1, \ldots, n$

$$\Lambda_i \supseteq \{s \mid \alpha(s) \in M(\alpha(i))\} \quad \text{and} \quad \mathrm{V}_i \supseteq \{s \mid \alpha(s) \in N(\alpha(i))\}.$$

Further $\alpha(i) \in M(\alpha(i))$ follows from the fact that $\mathbf{0} \in \Delta(R,\rho,\varphi)$ and that $\alpha(i) + \mathbf{0} = \alpha(i)$. Therefore $\Lambda_i \cup \{i\} = \Lambda_i$. Similarly $\mathrm{V}_i \cup \{i\} = \mathrm{V}_i$. All together

$$\Lambda_i \cup \{i\} \supseteq \{s \mid \alpha(s) \in M(\alpha(i))\} \quad \text{and} \quad \mathrm{V}_i \cup \{i\} \supseteq \{s \mid \alpha(s) \in N(\alpha(i))\}.$$

The theorem follows. □

**Example 30.** *This is a continuation of Example 21 and Example 25. To estimate* $\bar{\sigma}(21)$ *we first observe that* $\alpha(21) = 23$. *We then look for values* $s, t$ *in* $\Delta(R,\rho,\varphi)$ *such that* $23+s = t$. *We get* $23+0 = 23$, $23+3 = 26$, $23+6 = 29$ *and* $23+9 = 32$. *Hence,* $\sigma(\alpha(21)) = 4$ *and from Proposition 29 we get* $\bar{\sigma}(21) \geq 4$.

Recall, that we in Section 3 introduced the codes $\mathcal{E}(s)$ and the improved codes $\widetilde{\mathcal{E}}(\delta)$. Similar in Section 4 we introduced the codes $\mathcal{C}(s)$ and the improved codes $\widetilde{\mathcal{C}}(\delta)$. We now consider their counter parts in the order domain theoretical set-up.

**Definition 31.** *Consider the set* $\Delta(R,\rho,\varphi) = \{\alpha(1), \ldots \alpha(n)\}$ *and the corresponding basis* $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. *Define*

$$\begin{aligned}
E(\lambda) &:= \varphi(R_\lambda) \\
&= C(B,G) \quad \textit{where} \quad G = \{\boldsymbol{b}_i \mid \alpha(i) \leq \lambda\} \\
\widetilde{E}(\delta) &:= \mathit{span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R,\rho,\varphi) \textit{ and } \sigma(\alpha(i)) \geq \delta\} \\
&= C(B,G) \quad \textit{where} \quad G = \{\boldsymbol{b}_i \mid \sigma(\alpha(i)) \geq \delta\} \\
C(\lambda) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_\gamma) = 0 \textit{ for all } \gamma \preceq \lambda\} \\
&= C^{\perp}(B,G) \quad \textit{where} \quad G = \{\boldsymbol{b}_i \mid \alpha(i) \leq \lambda\} \\
\widetilde{C}(\delta) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \textit{ for all } \alpha(i) \in \Delta(R,\rho,\varphi) \textit{ with } \mu(\alpha(i)) < \delta\} \\
&= C^{\perp}(B,G) \quad \textit{where} \quad G = \{\boldsymbol{b}_i \mid \mu(\alpha(i)) < \delta\}
\end{aligned}$$

The following Theorem is an easy consequence of the theory developed so far.

**Theorem 32.** *The minimum distances of the codes in Definition 31 are bounded by*

$$\begin{aligned} d(E(\lambda)) &\geq \min\{\sigma(\eta) \mid \eta \in \Delta(R,\rho,\varphi), \eta \preceq \lambda\} \qquad (13)\\ d(\widetilde{E}(\delta)) &\geq \delta.\\ d(C(\lambda)) &\geq \min\{\mu(\eta) \mid \lambda \prec \eta, \eta \in \Delta(R,\rho,\varphi)\}\\ &\geq \min\{\mu(\eta) \mid \lambda \prec \eta\}\\ d(\widetilde{C}(\delta)) &\geq \delta. \end{aligned}$$

*More generally the* `t`*th generalized Hamming weights (*$t$ *being at most equal to the dimension of the code) satisfy*

$$\begin{aligned} d_t(E(\lambda)) &\geq \min\{\sigma(\eta_1,\eta_2,\ldots,\eta_t) \mid \{\eta_1,\eta_2,\ldots,\eta_t\} \subseteq \Delta(R,\rho,\varphi)\\ &\qquad \eta_i \neq \eta_j \text{ for } i \neq j, \eta_s \preceq \lambda \text{ for } s = 1,\ldots,t\} \qquad (14)\\ d_t(\widetilde{E}(\delta)) &\geq \min\{\sigma(\eta_1,\eta_2,\ldots,\eta_t) \mid \{\eta_1,\eta_2,\ldots,\eta_t\} \subseteq \Delta(R,\rho,\varphi)\\ &\qquad \eta_i \neq \eta_j \text{ for } i \neq j, \sigma(\eta_s) \geq \delta \text{ for } s = 1,\ldots,t\}. \qquad (15)\\ d_t(C(\lambda)) &\geq \min\{\mu(\lambda_1,\ldots,\lambda_t) \mid \lambda_i \succ \lambda, \lambda_i \in \Delta(R,\rho,\varphi) \text{ for } i = 1,\ldots,t\}\\ &\geq \min\{\mu(\lambda_1,\ldots,\lambda_t) \mid \lambda_i \succ \lambda \text{ for } i = 1,\ldots,t\}\\ d_t(\widetilde{C}(\delta)) &\geq \min\{\mu(\lambda_1,\ldots,\lambda_t) \mid \mu(\lambda_i) \geq \delta, \lambda_i \in \Delta(R,\rho,\varphi) \text{ for } i = 1,\ldots,t\}\\ &\geq \min\{\mu(\lambda_1,\ldots,\lambda_t) \mid \mu(\lambda_i) \geq \delta \text{ for } i = 1,\ldots,t\} \end{aligned}$$

It is obvious that with respect to the above bounds the $\widetilde{C}(\delta)$ construction is an improvement to the $C(\lambda)$ construction and the $\widetilde{E}(\delta)$ construction is an improvement to the $E(\lambda)$ construction. The result concerning $d(C(\lambda))$ and $d(\widetilde{C}(\delta))$ is known as the order bound and comes from [16]. The result concerning $d_t(C(\lambda))$ is from [14] and the result concerning $d_t(\widetilde{C}(\delta))$ is from [13]. The results concerning $E(\lambda)$ and $\widetilde{E}(\lambda)$ are new and explains the title of the present paper. It should be mentioned that Shibuya and Sakaniwa in [28] translates their bound into the setting of codes coming from $C_{ab}$ curves and codes coming from Garcia and Stichtenoth's tower in [7].

**Example 33.** *This is a continuation of Example 21, Example 25 and Example 30. In the table below we list all the values* $\sigma(\alpha(i))$, $i = 1,\ldots,27$.

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha(i)$ | 0 | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| $\sigma(\alpha(i))$ | 27 | 24 | 23 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 |

| $i$ | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha(i)$ | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 28 | 29 | 32 |
| $\sigma(\alpha(i))$ | 10 | 9 | 8 | 7 | 6 | 6 | 4 | 3 | 4 | 3 | 2 | 2 | 1 |

*Hence, $\mathcal{E}(21) = E(23)$ has parameters $n = 27, k = 21, d \geq 4$ and $\mathcal{E}(22) = E(24)$ has parameters $n = 27, k = 22, d \geq 3$. But $\widetilde{\mathcal{E}}(4) = \widetilde{E}(4)$ has parameters $n = 27, k = 22, d \geq 4$ and is therefore indeed an improved code. The three estimations on the minimum distances are known to be sharp.*

In the next section we will recall the well-known fact that every one-point geometric Goppa code can be described as an $E(s)$ code related to an order domain of transcendence degree 1, and we will show by a very easy argument that our new bound is an improvement to the usual bound from algebraic geometry.

# 7 Improved one-point geometric Goppa codes

The following example is well-known. Actually it was one of the main reasons for introducing order domains in the first place.

**Example 34.** *Let $\mathcal{P}$ be a rational place in an algebraic function field $\mathcal{F}$ of one variable and let $v_{\mathcal{P}}$ be the valuation corresponding to $\mathcal{P}$. Then $R := \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ is an order domain with a weight function given by $\rho(x) = -v_{\mathcal{P}}(x)$ for any $x \in R$.*

Hence, it is clear that the one-point geometric Goppa codes are codes $E(\lambda)$ defined from order domains with a weight function with a numerical value semigroup $\Gamma$. In the same way of course the duals of one-point geometric Goppa codes are codes $C(\lambda)$ defined from order domains with a weight function with a numerical value semigroup $\Gamma$. It is well-known that the order bound is an improvement to the Goppa bound for the duals of one-point geometric Goppa codes (see [16][Th. 5.24]). Consequently the corresponding codes $\widetilde{C}(\delta)$ becomes improvements to the duals of one-point geometric Goppa codes.

We now show by a rather easy argument that our bound for the minimum distance of the one-point geometric Goppa code $E(\lambda)$ is an improvement to the usual bound from algebraic geometry. Consequently, the corresponding codes $\widetilde{E}(\lambda)$ can be viewed as being improved one-point geometric Goppa codes. From [16][Lem. 5.15] we have the following lemma.

**Lemma 35.** *Let $\Gamma$ be a numerical semigroup with finitely many gaps. That is, let $\mathbb{N}_0 \backslash \Gamma$ be a finite set. Assume $i \in \Gamma$. Then the number of elements of $\Gamma \backslash (i + \Gamma)$ is equal to $i$.*

The well-known Goppa bound for the one-point geometric Goppa code $E(\lambda)$ says $d(E(\lambda)) \geq n - \lambda$. For comparison, our new bound (13) states

$$d(E(\lambda)) \geq \min\{\#((i + \Gamma) \cap \Delta(R, \rho, \varphi)) \mid i \in \Gamma, i \leq \lambda\}.$$

As by Lemma 35 we have

$$\#((i + \Gamma) \cap \Delta(R, \rho, \varphi)) \geq n - i$$

with equality if and only if $\Gamma\backslash(i+\Gamma) \subseteq \Delta(R,\rho,\varphi)$ it is clear that our bound is as good and sometimes better than the Goppa bound. In particular for $\lambda$ being of a high value compared to $n$ the new bound will often be much better than the Goppa bound. We have proved the last part of the following proposition.

**Proposition 36.** *Any one-point geometric Goppa code is of the form $E(\lambda)$ in Definition 31 and the bound (13) is an improvement to the Goppa bound.*

For comparison, as already mentioned Shibuya et al. in [28] only show that their bound is an improvement to the Goppa bound in the case of codes defined from $C_{ab}$ curves and in the case of some codes coming from Garcia and Stichtenoth's tower in [7].

# 8 The Gröbner basis approach

In Section 6 we described the main tools needed to deal with codes coming from order domains. Important ingredients were the well-behaving basis $\mathcal{B} = \{f_\lambda \mid \rho(f_\lambda) = \lambda\}_{\lambda\in\Gamma}$, the morphism $\varphi : R \to \mathbb{F}_q^n$ and the set $\Delta(R,\rho,\varphi)$. Here $\Delta(R,\rho,\varphi) = \{\alpha(1),\ldots,\alpha(n)\}$ where $\alpha(1) = 0$ and where $\alpha(i)$, $i = 2,\ldots,n$ is defined to be the smallest element in $\Gamma$ that is greater than $\alpha(1),\alpha(2),\ldots,\alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma \prec \alpha(i)$. With these ingredients in hand we constructed the basis $B = \{\boldsymbol{b}_1 = \varphi(f_{\alpha(1)}),\ldots,\boldsymbol{b}_n = \varphi(f_{\alpha(n)})\}$ which is very suitable for the code construction. For small code lengths it will normally be an easy task to find the set $\Delta(R,\rho,\varphi)$ by using standard linear algebra methods. However, for larger code lengths we will need some more sophisticated machinery.

Recall from [12] that an order domain is called finitely generated if it possesses a weight function with a finitely generated value semigroup $\Gamma$. One of the very nice things about order domain theory is the fact that any finitely generated order domain over $\mathbb{F}_q$ can be described as a quotient ring $R = \mathbb{F}_q[X_1,\ldots,X_m]/I$. Furthermore the description only relies on some not too complicated Gröbner basis theory. In this section we will see that the very same Gröbner basis theoretical methods will allow us to find $\Delta(R,\rho,\varphi)$ and thereby also the basis $B$ in a rather simple way whenever $\varphi$ is the most natural chosen evaluation map. We start our study by considering some basic terminology from Gröbner basis theory. We will assume that the reader is familiar with the concept of a monomial ordering, with the definition of a Gröbner basis and with the division algorithm for polynomials in more variables. We will differ slightly from the traditional notion by defining for any monomial ordering $\emptyset$ to be a Gröbner basis for the zero ideal $I = \{0\}$. The following concept will be used extensively throughout the later sections.

**Definition 37.** *Denote by $\mathcal{M}(X_1,X_2,\ldots,X_m)$ the set of monomials in $X_1$, $X_2$, $\ldots$, $X_m$. Given a monomial ordering $\prec$ on $\mathcal{M}(X_1,X_2,\ldots,X_m)$ and an*

*ideal* $L \subseteq \mathbb{F}[X_1, \ldots, X_m]$ *the footprint*[1] *of* $L$ *is the set*

$$\Delta_\prec(L) := \{M \in \mathcal{M}(X_1, \ldots, X_m) \mid M \text{ is not a leading monomial of any polynomial in } L\}.$$

The following proposition from [3][Pro. 4 in Paragraph 5.3] will be one of our main tools.

**Proposition 38.** *Consider any field* $\mathbb{F}$ *and let* $L \subseteq \mathbb{F}[X_1, \ldots, X_m]$ *be an ideal. Then* $\{M + L \mid M \in \Delta_\prec(L)\}$ *is a basis for* $\mathbb{F}[X_1, \ldots, X_m]/L$ *as a vectors pace over* $\mathbb{F}$*.*

Another useful tool is the following proposition known as the footprint-bound. From [3][§5.3, Pro. 8] and [4][Pro. 2.7] we have.

**Proposition 39.** *If* $\Delta_\prec(L)$ *is finite then the size of the variety* $\mathbb{V}_\mathbb{F}(L)$ *is bounded by*

$$\#\mathbb{V}_\mathbb{F}(L) \leq \#\Delta_\prec(L). \tag{16}$$

*If* $L$ *is a radical ideal and* $\mathbb{F}$ *is algebraically closed then equality holds in (16). As a consequence equality holds when* $\mathbb{F} = \mathbb{F}_q$*,* $L \subseteq \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ *and* $X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m \in L$*.*

The footprint can only in rare cases be read directly of the polynomials defining the ideal $L$. However, we can always extend the set of defining polynomials to a Gröbner basis by using Buchgberger's well-known algorithm and thereby find the footprint. We now introduce the particular type of monomial orderings that will be important for us. They are the generalized weighted degree orderings. The class of generalized weighted degree orderings is indeed a large class. Actually any monomial ordering can be described as a generalized weighted degree ordering. Nevertheless, the following definition will prove to be very useful.

**Definition 40.** *Given weights* $w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^r \backslash \{\mathbf{0}\}$ *let* $\mathbb{N}_0^r$ *be ordered by some fixed monomial ordering* $\prec_{\mathbb{N}_0^r}$ *and let* $\prec_\mathcal{M}$ *be a fixed monomial ordering on* $\mathcal{M}(X_1, X_2, \ldots, X_m)$*. The weights extends to a monomial function* $w : \mathcal{M}(X_1, X_2, \ldots, X_m) \to \mathbb{N}_0^r$ *by* $w(X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m}) = \sum_{i=1}^m \alpha_i w(X_i)$*. For a monomial* $M$ *we call* $w(M)$ *the weight of* $M$*. We define the weighted degree* $wdeg(F)$ *of a polynomial* $F$ *to be the highest weight (with respect to* $\prec_{\mathbb{N}_0^r}$*) that appears as a weight of a monomial in the support of* $F$*. Now the generalized weighted degree ordering* $\prec_w$ *induced by* $w$*,* $\prec_{\mathbb{N}_0^r}$ *and* $\prec_\mathcal{M}$ *is the monomial ordering defined as follows. Given* $M_1, M_2 \in \mathcal{M}(X_1, X_2, \ldots, X_m)$ *then* $M_1 \prec_w M_2$ *if and only if one of the following two conditions holds:*

*(1)* $w(M_1) \prec_{\mathbb{N}_0^r} w(M_2)$ *(2)* $w(M_1) = w(M_2)$ *and* $M_1 \prec_\mathcal{M} M_2$*.*

We are now in the position where we can give the useful description from [12][Th. 9.1 and Th. 10.4] of finitely generated order domains.

[1]The name "footprint" was suggested by D. Blahut in 1991. The footprint was previously called the delta-set, the excluded point set and other things (see [15]).

**Theorem 41.** *Let $\prec_w$ be a generalized weighted degree ordering and assume that $I \subset \mathbb{F}[X_1, X_2, \ldots, X_m]$ is an ideal with a Gröbner basis $\mathcal{G}$ with respect to $\prec_w$. Suppose that the elements of the footprint $\Delta_{\prec_w}(I)$ have mutually distinct weights and that every element of $\mathcal{G}$ has exactly two monomials of highest weight (with respect to $\prec_{\mathbb{N}_0^r}$) in its support. Then $R = \mathbb{F}[X_1, X_2, \ldots, X_m]/I$ is an order domain with a weight function defined as follows. Given a nonzero $f \in \mathbb{F}[X_1, X_2, \ldots, X_m]/I$ write $f = F + I$ where $F \in span_{\mathbb{F}}\{M \mid M \in \Delta_{\prec_w}(I)\}$. We have $\rho(f) = wdeg(F)$ and $\rho(0) = -\infty$.*
*Any finitely generated order domain can be described as above.*

**Example 42.** *In this example we show how the order domain and weight function described in Example 21 can be easily explained in the language of Theorem 41. The generalized weighted degree ordering $\prec_w$ to be used is the one with weights $w(X) = 3$ and $w(Y) = 4$. The monomial ordering $\prec_{\mathbb{N}_0}$ is of course the unique monomial ordering $<$ on $\mathbb{N}_0$ and as ordering $\prec_{\mathcal{M}}$ on $\mathcal{M}(X, Y)$ we choose the lexicographic ordering with $X \prec_{\mathcal{M}} Y$. The resulting ordering $\prec_w$ can be shown to give us the footprint*

$$\Delta_{\prec_w}(I) = \{X^\alpha Y^\beta \mid 0 \leq \alpha, 0 \leq \beta < 3\}.$$

*Now the footprint satisfies the condition in Theorem 41 and so does the Hermitian polynomial. Hence, a weight function is given exactly as we described it in Example 21. The well-behaving basis (11) is found by using Proposition 38 on the above footprint.*

According to our agenda we now choose a morphism on the order domain $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$. The most obvious choice of morphism is the evaluation map based on the entire affine variety $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$. In other words the morphism $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(F + I) := (F(P_1), \ldots, F(P_n))$. As we will see in a moment it will be an easy task to derive the corresponding set $\Delta(R, \rho, \varphi)$ for this particular choice of $\varphi$. We will need a single definition.

**Definition 43.** *Given an ideal $I \subseteq \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ write*

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

The following method to derive $\Delta(R, \rho, \varphi)$ was stated in [21][Lem. 6.2] and [23][p. 1402] (both in Japanese) for the case of the valuesemigroup $\Gamma$ being numerical. That is, for the case $\Gamma \subseteq \mathbb{N}_0$. A version considering the general case $\Gamma \subseteq \mathbb{N}_0^r$ for any $r$ was presented in the abstract [8], but no proof was included.

**Proposition 44.** *Consider an order structure $(R, \rho, \Gamma)$ that is described as in Theorem 41. Let $\varphi$ be the morphism $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(F + I) := (F(P_1), F(P_2), \ldots, F(P_n))$ where $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$. We have*

$$\Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}. \tag{17}$$

*Proof.* One of the conditions in Theorem 41 is that the weights of the monomials in $\Delta_{\prec_w}(I)$ are all different. As $I \subseteq I_q$ implies $\Delta_{\prec_w}(I_q) \subseteq \Delta_{\prec_w}(I)$ the weights of all the monomials in $\Delta_{\prec_w}(I_q)$ are also different. Hence, the size of $\{w(M) \mid$

$M \in \Delta_{\prec_w}(I_q)\}$ equals the size of $\#\Delta_{\prec_w}(I_q)$ which in turn equals $n$ by the last part of Proposition 39. As clearly $\#\Delta(R,\rho,\varphi) = n$ we conclude that the sets on the two sides of (17) are of the same size. The proposition therefore will be proven if we can show that $\alpha(s) \in \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$ for $s = 1, 2, \ldots, n$. Consider a fixed $\alpha(s) \in \Delta(R,\rho,\Gamma)$ and let $f \in R$ be such that $\rho(f) = \alpha(s)$. By the construction in Theorem 41 we can write $f = F + I$ where $F = \sum_{i=1}^{t} \eta_i M_i$ where $t \geq 1$, where $M_i \in \Delta_{\prec_w}(I)$, $\eta_i \in \mathbb{F}_q \backslash \{0\}$ for $i = 1, 2, \ldots, t$, where $w(M_t) \prec_{\mathbb{N}_0^r} w(M_{t-1}) \prec_{\mathbb{N}_0^r} \cdots \prec_{\mathbb{N}_0^r} w(M_1)$ and where $\alpha(s) = \rho(f) = w(M_1)$. Let $\mathcal{G}'$ be a Gröbner basis for $I_q$ with respect to $\prec_w$. We now reduce $F$ modulo $\mathcal{G}'$ using the division algorithm for polynomials and get a remainder $\sum_{i=1}^{l} \beta_i N_i$ where $N_i \in \Delta_{\prec_w}(I_q)$, $\beta_i \in \mathbb{F}_q \backslash \{0\}$ for $i = 1, 2, \ldots, l$ and where $w(N_l) \prec_{\mathbb{N}_0^r} w(N_{l-1}) \prec_{\mathbb{N}_0^r} \cdots \prec_{\mathbb{N}_0^r} w(N_1)$. We have $F - \sum_{i=1}^{l} \beta_i N_i \in I_q$ and as $\mathbb{V}_{\mathbb{F}_q}(I_q) = \mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ holds we get $\varphi(F - \sum_{i=1}^{l} \beta_i N_i + I) = \mathbf{0}$. We conclude

$$\varphi(f) = \varphi(F + I) = \varphi(F - (F - \sum_{i=1}^{l} \beta_i N_i) + I) = \varphi(\sum_{i=1}^{l} \beta_i N_i + I). \tag{18}$$

Note that $\varphi(f)$ is nonzero by the definition of $\alpha(s)$. Therefore (18) implies that $\sum_{i=1}^{l} \beta_i N_i \neq 0$. This fact and the fact that $\Delta_{\prec_w}(I_q) \subseteq \Delta_{\prec_w}(I)$ implies

$$\rho(\sum_{i=1}^{l} \beta_i N_i + I) = w(N_1).$$

Next we observe that by the nature of the division algorithm and by the definition of $\prec_w$ we have $\mathrm{wdeg}(F) \succeq_{\mathbb{N}_0^r} \mathrm{wdeg}(\sum_{i=1}^{l} \beta_i N_i)$. This is the same as saying

$$\alpha(s) = \rho(f) \succeq_{\mathbb{N}_0^r} w(N_1) = \rho(\sum_{i=1}^{l} \beta_i N_i) + I) \tag{19}$$

By the definition of $\Delta(R,\rho,\varphi)$, we have $\varphi(R_\lambda) \subsetneq \varphi(R_{\alpha(s)})$ for all $\lambda \prec_{\mathbb{N}_0^r} \alpha(s)$. In particular this implies that $\varphi(g) \neq \varphi(f)$ for any $g \in R$ with $\rho(g) \prec_{\mathbb{N}_0^r} \rho(f)$. But then by (18) we must have equality in (19). Consequently, $\alpha(s) = w(N_1) \in \Delta_{\prec_w}(I_q)$ holds and we are through. □

**Remark 45.** *It is shown in [1] that a result similar to the one in Proposition 44 holds for a more general class of morphisms. Namely whenever $\varphi(F+I)$ equals $(F(Q_1), \ldots, F(Q_{n'}))$ for a subvariety $\{Q_1, \ldots, Q_{n'}\} \subseteq \mathbb{V}_{\mathbb{F}_q}(I_q)$. This observation in combination with the methods of the present paper is then used to derive improved bounds on punctured codes coming from the norm-trace curve. As any finite set of points constitutes a variety the observation in [1] gives a general way of dealing with punctured codes.*

**Example 46.** *This is a continuation of Example 42. One can show*

$$\Delta_{\prec_w}(I_q) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 9, 0 \leq \beta < 3\}.$$

*Hence, by Proposition 47 we get $\Delta(R,\rho,\varphi) = \{w(X^\alpha Y^\beta) \mid 0 \leq \alpha < 9, 0 \leq \beta < 3\}$. By inspection this gives us exactly the basis $B$ that we derived in*

*Example 25. The footprint is particular simple in the sense that it so to speak constitutes a box. By inspection it is seen that as a consequence*

$$\mu(\rho(X^{\alpha}Y^{\beta}+I)) = \sigma(\rho(X^{8-\alpha}Y^{2-\beta}+I))$$

*holds for any $\alpha, \beta$ with $X^{\alpha}Y^{\alpha}$ in the footprint. Therefore in particular the Feng-Rao bound gives us the same estimate for the minimum distance of the code $C(\alpha(s))$ as does our new bound for the minimum distance of the code $E(\alpha(n-s))$, $s = 1, \ldots, n-1$. Further the dimension of $\widetilde{C}(\delta)$ equals the dimension of $\widetilde{E}(\delta)$ for all choices of $\delta$. The similarity between the Feng-Rao bound and our new bound not only holds for the minimum distance, but can be seen to hold for all the generalized Hamming weights from this example.*

Consider any order domain $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ described as in Theorem 41. The following Proposition states that a result similar to the one in Example 46 holds whenever the footprint $\Delta_{\prec_w}(I_q)$ is an $m$-dimensional box.

**Proposition 47.** *Let $R$ be an order domain over $\mathbb{F}_q$ described as in Theorem 41. Let $\mathbb{V}_{\mathbb{F}_q}(I_q) = \{P_1, P_2, \ldots, P_n\}$ and consider the evaluation map $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(F+I) = (F(P_1), F(P_2), \ldots, F(P_n))$. Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be defined accordingly. If $\Delta_{\prec_w}(I_q)$ is of the form*

$$\Delta_{\prec_w}(I_q) = \{X_1^{\beta_1} X_2^{\beta_2} \ldots X_m^{\beta_m} \mid \beta_1 \leq \gamma_1, \beta_2 \leq \gamma_2, \ldots, \beta_m \leq \gamma_m\} \tag{20}$$

*for some $(\gamma_1, \gamma_2, \ldots, \gamma_m) \in \mathbb{N}_0^m$ then*

$$\mu(\rho(X_1^{\beta_1} \cdots X_m^{\beta_m} + I)) = \sigma(\rho(X_1^{\gamma_1 - \beta_1} \cdots X_m^{\gamma_m - \beta_m} + I)) \tag{21}$$

*holds for any $X_1^{\beta_1} \cdots X_m^{\beta_m} \in \Delta(I_q)$. More generally for any $s$, $1 \leq s < n$ the codes $C(\alpha(s))$ and $E(\alpha(n-s))$ are of the same dimension and the Feng-Rao bound gives us exactly the same estimations on the generalized Hamming weights of $C(\alpha(s))$ as does our new bound on the generalized Hamming weights of $E(\alpha(n-s))$. Also for any $\delta$ the dimension of $\widetilde{C}(\delta)$ equals the dimension of $\widetilde{E}(\delta)$ and for any $t$ at most equal to the dimension of $\widetilde{C}(\delta)$ the Feng-Rao bound gives us exactly the same estimations on the $t$th generalized Hamming weights of $\widetilde{C}(\delta)$ as does our new bound on the $t$th generalized Hamming weights of $\widetilde{E}(\delta)$.*

*Proof.* We only show (21) and leave the remaining part of the proof for the reader. Consider $\alpha(l) \in \Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$. By assumption there exist $\omega_1, \omega_2, \ldots, \omega_m \in \mathbb{N}_0$ with $\omega_1 \leq \gamma_1, \omega_2 \leq \gamma_2, \ldots, \omega_m \leq \gamma_m$ such that $w(X_1^{\omega_1} X_2^{\omega_2} \cdots X_m^{\omega_m}) = \alpha(l)$. Also by assumption

$$w(X_1^{\gamma_1 - \omega_1} X_2^{\gamma_2 - \omega_2} \cdots X_m^{\gamma_m - \omega_m}) \in \Delta(R, \rho, \varphi).$$

Hence, if we write $\alpha_{\max} := w(X_1^{\gamma_1} X_2^{\gamma_2} \cdots X_m^{\gamma_m})$ then we have $\alpha(l) \in \Delta(R, \rho, \varphi)$ if and only if $\alpha_{\max} - \alpha(l) \in \Delta(R, \rho, \varphi)$. Moreover by the very definition of $\mu$ and $\sigma$ (20) implies that for all $\alpha(l) \in \Delta(R, \rho, \varphi)$ we have $\mu(\alpha(l)) = \sigma(\alpha_{\max} - \alpha(l))$. □

**Remark 48.** *In Remark 45 we noted that Proposition 44 can be modified to deal with punctured codes. In a similar manner one can modify Proposition 47 to deal with punctured codes.*

The next section includes examples where (20) is satisfied but also an example illustrating that if $R$ and $\varphi$ are given as in Proposition 47, but (20) is not satisfied then it may happen that the dimensions of the codes $\widetilde{E}(\delta)$ and $\widetilde{C}(\delta)$ are not the same for almost all choices of $\delta \in \{1, 2, \ldots, n\}$. We will describe two types of algebraic structures where not only (20) is satisfied but actually $\widetilde{E}(\delta) = \widetilde{C}(\delta)$ holds for all $\delta \in \{1, 2, \ldots, n\}$.

# 9 Examples

In this section we make extensive use of most of the theory developed so far. Rather than reintroducing the notation we invite the reader to revisit if necessary Proposition 39, Definition 40, Theorem 41, Proposition 44 and Proposition 47 before continuing. In the following we will use the notation $\langle \cdots \rangle$ in two meanings. Firstly, given $F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ by $\langle F_1, \ldots, F_s \rangle$ we denote the ideal generated by the polynomials $F_1, \ldots, F_s$. Secondly, given elements $w_1, \ldots, w_m \in \mathbb{N}_0^r$ by $\langle w_1, \ldots, w_m \rangle$ we denote the semigroup generated by $w_1, \ldots, w_m$.

**Example 49.** *Let $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z \rangle \subseteq \mathbb{F}_{16}[X, Y, Z]$. Define the generalized weighted degree ordering $\prec_w$ on $\mathcal{M}(X, Y, Z)$ as follows. Consider weights $w(X) = 16, w(Y) = 20, w(Z) = 25 \in \mathbb{N}_0$. Let $\prec_{\mathbb{N}_0}$ be the usual (and unique) monomial ordering on $\mathbb{N}_0$ and let $\prec_{\mathcal{M}}$ be the lexicographic ordering on $\mathcal{M}(X, Y, Z)$ given by $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z$. With respect to the resulting ordering $\prec_w$ $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z\}$ is a Gröbner basis and by inspection it is seen that the conditions in Theorem 41 are satisfied. By Theorem 41 we therefore get a weight function*

$$\rho : R := \mathbb{F}_{16}[X, Y, Z]/I \to \langle 16, 20, 25 \rangle \cup \{-\infty\}.$$

*Also the set $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z, X^{16} + X, Y^{16} + Y, Z^{16} + Z\}$ constitutes a Gröbner basis with respect to $\prec_w$ and therefore by the last part of Proposition 39 the variety $\mathbb{V}_{\mathbb{F}_{16}}(I_{16})$ is of size equal to $\#\Delta_{\prec_w}(I_{16}) = 256$. Let $\varphi$ be the affine variety map $\varphi : R \to \mathbb{F}_{16}^{256}$ given by $\varphi(f) = (f(P_1), f(P_2), \ldots, f(P_{256}))$ where $\{P_1, P_2, \ldots, P_{256}\} = \mathbb{V}_{\mathbb{F}_{16}}(I_{16})$. As $\Delta_{\prec_w}(I_{16}) = \{X^a Y^b Z^c \mid 0 \leq a < 16, 0 \leq b < 4, 0 \leq c < 4\}$ the condition in (20) of Proposition 47 is satisfied and therefore the dimension of $\widetilde{C}(\delta)$ equals the dimension of $\widetilde{E}(\delta)$ for all $\delta = 1, 2, \ldots, 256$. In Figure 1 we plot the (estimated) parameters of the codes $\widetilde{E}(\delta)$. For the $E(\lambda)$ codes we plot the usual Goppa bound (old bound) as well as the improved bound from the present paper (new bound).*

**Example 50.** *Let $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z, Z^5 + U^4 + U^2 \rangle \subseteq \mathbb{F}_{16}[X, Y, Z, U]$ (note the term $U^2$). Define the generalized weighted degree ordering $\prec_w$ on $\mathcal{M}(X, Y, Z, U)$ as follows. Consider weights $w(X) = 64, w(Y) = 80, w(Z) = 100, w(U) = 125 \in \mathbb{N}_0$. Let $\prec_{\mathbb{N}_0}$ be the usual (and unique) monomial ordering on $\mathbb{N}_0$ and let $\prec_{\mathcal{M}}$ be the lexicographic ordering on $\mathcal{M}(X, Y, Z, U)$ given by $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z \prec_{\mathcal{M}} U$. The conditions in Theorem 41 are satisfied with the Gröbner basis $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z, Z^5 + U^4 + U^2\}$. We therefore get a*

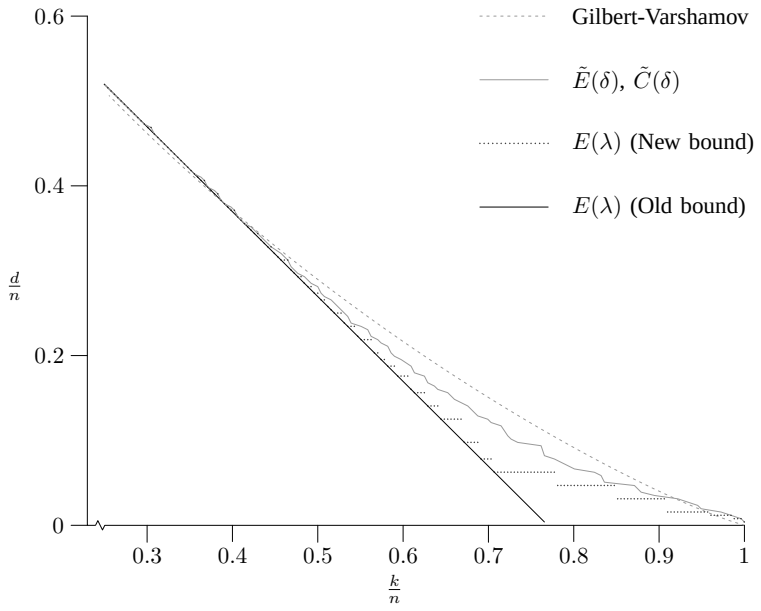


Figure 1:

*weight function*

$$\rho : R := \mathbb{F}_{16}[X, Y, Z, U]/I \to \langle 64, 80, 100, 125\rangle \cup \{-\infty\}.$$

*According to our agenda we should next derive a footprint for* $I_{16}$*. By the use of Buchberger's algorithm we get a reduced Gröbner basis with* 21 *polynomials. Due to lack of space we list here only their leading monomials*

$$\{Y^4, Z^4, U^4, X^{10}Y^2Z^2, X^5Y^2ZU^2, X^{10}ZU^2, X^5Y^2Z^3, X^{10}Z^3, X^{10}Y^3, X^{15},$$
$$XY^3Z^3U^2, X^6Y^3U^2, X^{11}U^2, X^6Z^2U^2, X^6Y^3Z^2, X^{11}Y, X^{11}Z, X^6YZU^2,$$
$$X^6YZ^3, X^{10}Y^2U^2, X^5YZ^2U^2\}.$$

*By definition of a Gröbner basis the footprint of* $I_{16}$ *consists of the monomials that are not divisible of any of the above* 21 *monomials. The footprint is found to be of size* $n = 512$ *and we therefore have a morphism* $\varphi : R \to \mathbb{F}_{16}^{512}$ *for the code construction. It is clear that the footprint does not satisfy the conditions in (20). That is, it does not have the shape of a box. Therefore it should come as no surprise that the codes* $\widetilde{C}(\delta)$ *and the codes* $\widetilde{E}(\delta)$ *perform quite differently. In Figure 2 we plot the estimated performance of the codes* $\widetilde{E}(\delta)$ *and* $\widetilde{C}(\delta)$*. It is clear that for values of* $k/n$ *smaller than approximately* 0.2 *the codes* $\widetilde{E}(\delta)$ *are the best whereas for larger values the codes* $\widetilde{C}(\delta)$ *are the best. Finally in Figure 2 we plot the usual Goppa bound (old bound) for the* $E(\lambda)$ *codes versus the improved bound from the present paper (new bound).*

**Example 51.** *In this example we assume that the reader is familiar with Buchberger's algorithm. In particular the reader is assumed to be familiar with the concept of an* $S$*-polynomial. Let*

$$H_1(X, Y, Z, U) := X^q + YZ^q - Y^qZ - X,$$

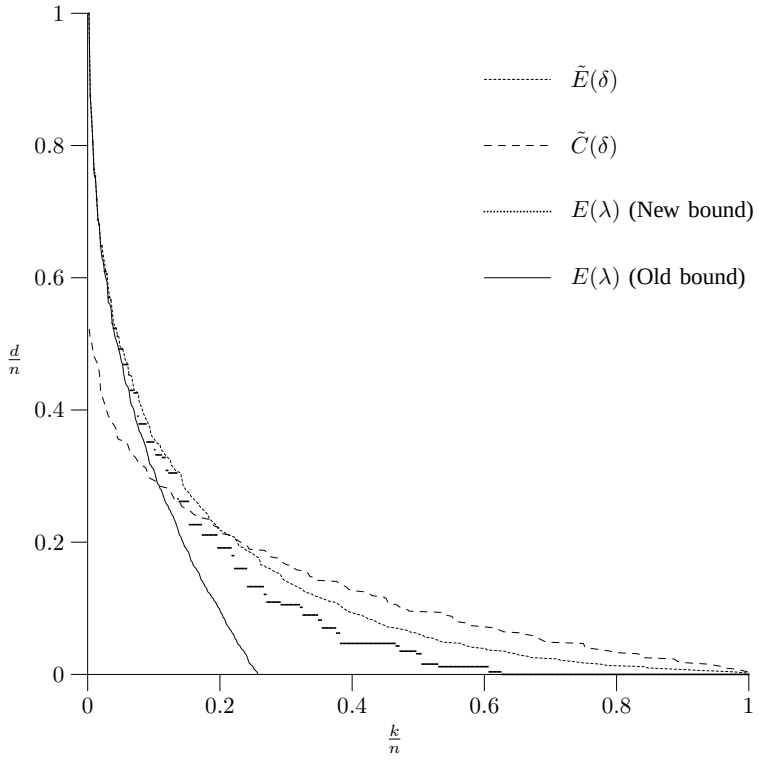
1
0.8
0.6
0.4
0.2
0
$\frac{d}{n}$
0
0.2
0.4
0.6
0.8
1
$\frac{k}{n}$
$\tilde{E}(\delta)$
$\tilde{C}(\delta)$
$E(\lambda)$ (New bound)
$E(\lambda)$ (Old bound)

Figure 2:

$$H_2(X,Y,Z,U) := U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U$$

*where* $a, b \in \mathbb{F}_q$. *Consider* $I := \langle H_1(X,Y,Z,U), H_2(X,Y,Z,U)\rangle \subseteq \mathbb{F}_{q^2}[X,Y,Z,U]$ *and define the generalized weighted degree ordering* $\prec_w$ *on* $\mathcal{M}(X,Y,Z,U)$ *as follows. Consider weights* $w(X) = (q,1), w(Y) = (0,q), w(Z) = (q,0), w(U) = (q+1,0) \in \mathbb{N}_0^2$ *and let* $\prec_{\mathbb{N}_0^2}$ *be any fixed monomial ordering on* $\mathbb{N}_0^2$ *that satisfies* $(q^2+q,0) \succ_{\mathbb{N}_0^2} (q^2,q), (q,q^2), (0,q^2+q)$. *Finally let* $\prec_{\mathcal{M}}$ *be any fixed monomial ordering on* $\mathcal{M}(X,Y,Z,U)$ *that satisfies* $X^q \succ_{\mathcal{M}} YZ^q$ *and* $U^q \succ_{\mathcal{M}} Z^{q+1}$. *The leading monomial of* $H_1$ *is* $X^q$ *and the leading monomial of* $H_2$ *is* $U^q$. *Hence, the two leading monomials are relatively prime. By a standard result in Gröbner basis theory this implies that* $\{H_1(X,Y,Z,U), H_2(X,Y,Z,U)\}$ *constitutes a Gröbner basis. It is easily shown that the remaining conditions in Theorem 41 are satisfied. From Theorem 41 we get a weight function*

$$\rho : R := \mathbb{F}_{q^2}[X,Y,Z,U]/I \to \langle (q,1),(0,q),(q,0),(q+1,0)\rangle \cup \{-\infty\}.$$

*We next want to use Buchberger's algorithm to establish that*

$$\mathcal{G}' = \{H_1(X,Y,Z,U), H_2(X,Y,Z,U), X^{q^2} - X, Y^{q^2} - Y, Z^{q^2} - Z, U^{q^2} - U\}$$

*constitutes a Gröbner basis for* $I_{q^2}$. *In the following* $K(X,Y,Z,U) \to L(X,Y,Z,U)$ *means that the polynomial* $K(X,Y,Z,U)$ *is reduced to the polynomial* $L(X,Y,Z,U)$ *modulo* $\mathcal{G}'$ *(using the operations that is allowed in Buchberger's algorithm). We have*

$$\begin{aligned}
& S(H_2, U^{q^2} - U) \\
= \;& (U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U)(U^q)^{q-1} - (U^{q^2} - U) \\
\to \;& (-Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U)^q(-1)^{q-1} + U \\
= \;& -Z^{q^2}Z^q + aX^{q^2} - aY^{q^2}Z^q + bY^{q^2}Y^q + U^q + U \\
\to \;& -Z^{q+1} + aX - aYZ^q + bY^{q+1} + U^q + U \\
\to \;& -a(X^q + YZ^q - aY^qZ - X) \\
\to \;& 0.
\end{aligned}$$

*The remaining S-polynomials are easily seen to reduce to* 0. *Hence, we actually have a Gröbner basis and*

$$\Delta_{\prec_w}(I_q) = \{X^\alpha Y^\beta Z^\gamma U^\delta \mid \alpha, \delta < q \quad \textit{and} \quad \beta, \gamma < q^2\}.$$

*The footprint is of size* $q^6$ *and our methods therefore give codes of length* $n = q^6$. *We next note that again the conditions in (20) of Proposition 47 are satisfied and therefore the dimension of* $\widetilde{C}(\delta)$ *equals the dimension of* $\widetilde{E}(\delta)$ *for all* $\delta = 1, 2, \ldots, q^6$. *In Figure 3 we plot the estimated performance of the codes* $\widetilde{E}(\delta)$ *and* $\widetilde{C}(\delta)$ *from the present example in the case* $\mathbb{F}_{q^2} = \mathbb{F}_{64}$. *These are of length* $n = 262144$. *The hyperbolic codes* $Hyp_{64}(s,3)$ *and the generalized Reed-Muller codes* $RM_{64}(s,3)$ *are of the same length, but according to Figure 3 they do not perform nearly as good as the codes from the present example.*

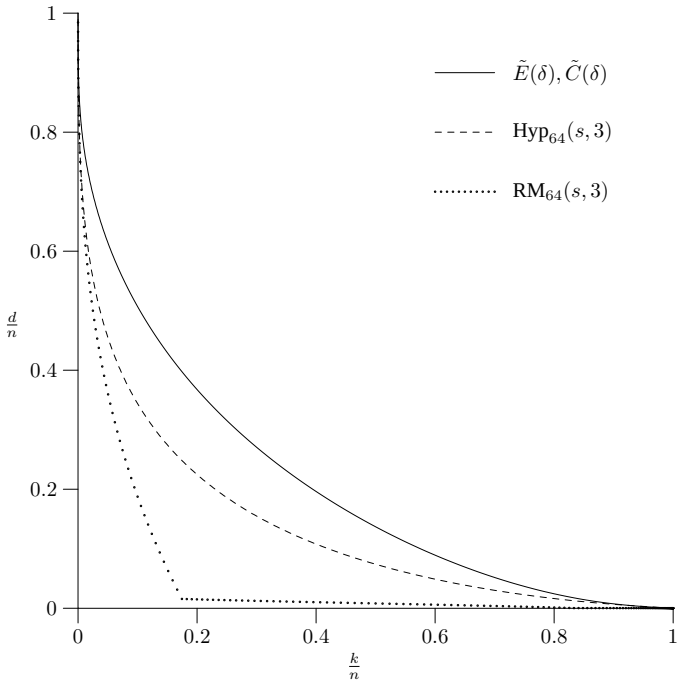


Figure 3:

**Example 52.** *In this example we consider the order domain* $R := \mathbb{F}_q[X_1, \ldots, X_r]$. *There exists infinitely many different weight function on this algebraic structure but we will only be concerned with a particular one. Let* $\prec_{\mathbb{N}_0^r}$ *be the generalized weighted degree lexicographic ordering on* $\mathbb{N}_0^r$ *given by the weights* $w((a_1, \ldots, a_r)) = \sum_{i=1}^r a_i$ *and by the rule*

$$(1, 0, \ldots, 0) \prec_{\mathbb{N}_0^r} (0, 1, 0 \ldots, 0) \prec_{\mathbb{N}_0^r} \cdots \prec_{\mathbb{N}_0^r} (0, \ldots, 0, 1).$$

*Define the weight function* $\rho : \mathbb{F}_q[X_1, \ldots, X_r] \to \mathbb{N}_0^r$ *by* $\rho(X_1^{a_1} \cdots X_r^{a_r}) = (a_1, \ldots, a_r)$. *Consider the set of points* $\mathbb{F}_q^r = \{P_1, \ldots, P_{q^r}\}$ *and let a morphism* $\varphi : R \to \mathbb{F}_q^{q^r}$ *be given by* $\varphi(F) := (F(P_1), \ldots, F(P_{q^r}))$. *We have*

$$\Delta(R, \rho, \varphi) = \{(a_1, \ldots, a_r) \mid 0 \leq a_i < q,\ i = 1, \ldots, r\}$$

*and for any* $(a_1, \ldots, a_r) \in \Delta(R, \rho, \varphi)$ *we get*

$$V_{(a_1,\ldots,a_r)} = \{(e_1, \ldots, e_r) \mid 0 \leq e_i \leq a_i\ i = 1, \ldots, r\} \tag{22}$$

$$\Lambda_{(a_1,\ldots,a_r)} = \{(e_1, \ldots, e_r) \mid a_i \leq e_i \leq q - 1\ i = 1, \ldots, r\}. \tag{23}$$

*The generalized Reed-Muller code is the code* $RM_q(s, r) = \{\varphi(F) \mid deg(F) \leq s\}$ *and it is well-known that*

$$(RM_q(s, r))^{\perp} = RM_q(r(q - 1) - s - 1, r) \tag{24}$$

*holds. One of the motivations for introducing order domains in the first place is the fact that the generalized Reed-Muller code can be understood as being a code*

*$C(\lambda)$ defined from the order domain in this example. More precisely from (24) we have $(RM_q(s,r))^{\perp} = C((0,\ldots,0,s))$. But what is even more obvious is that $RM(s,r) = E((0,\ldots,0,s))$ holds. From (22) and (23) is is clear that our new bound gives exactly the same estimates for the generalized Reed-Muller codes as does the Feng-Rao bound. In [14] it was shown that the Feng-Rao bound is tight in the case of the generalized Hamming weights of generalized Reed-Muller codes. It follows immediately that also are our new bound. The improved codes $\widetilde{C}(\delta)$ are known as hyperbolic codes and the improved codes $\widetilde{E}(\delta)$ are the Massey-Costello-Justesen codes so named in [17] with a reference to [18]. By (22) and (23) these are of the same dimension. Actually, in a pure Gröbner basis theoretical set-up it was shown in [10] that $\widetilde{C}(\delta) = \widetilde{E}(\delta)$ and that the Feng-Rao bound gives the true minimum distance. Consequently also our new bound gives the true minimum distances of the hyperbolic codes.*

We conclude this section by mentioning without a proof that the construction of Hermitian codes in Example 33 is easily generalized to deal with the case of codes coming from any norm-trace curve $X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y$. The constructions satisfies the condition (20) in Proposition 47. Actually it is even known that the corresponding $C(s)$ codes can also be described as $E(s)$ codes and that $\widetilde{C}(\delta) = \widetilde{E}(\delta)$ holds. Furthermore it is known that one gets the actual minimum distances of the above codes by applying the Feng-Rao bound or similarly our new bound. For more details see [9]. In [2] it was shown that the Feng-Rao bound gives the actual generalized Hamming weights of the Hermitian codes. It follows that also our new bound would produce the actual generalized Hamming weights of the Hermitian codes.

## 10 Conclusion

In this paper we have derived a Feng-Rao type bound for the minimum distance of codes defined by means of their generator matrix. From our bound it is clear how to construct improved codes. In particular it is clear how to construct improved one-point geometric Goppa codes. Our new bound is easily extended to deal with any generalized Hamming weights. When translated into the setting of order domain theory our new bound becomes rather manageable. In particular it becomes obvious how to generalize the construction of (improved) one-point geometric Goppa codes to algebraic structures of higher transcendence degree. It remains to consider other implementations of our bound than the order domain theoretical one. Also it remains to find a decoding method for the new improved code constructions. It would be obvious to try to modify the Guruswami-Sudan algorithm for one-point geometric Goppa codes to deal with the new improved one-point geometric Goppa codes.

## A A pure Gröbner basis theoretical approach

In the paper [10] the hyperbolic codes were studied from a pure Gröbner basis theoretical point of view. Similarly, in the paper [9] one-point geometric Goppa

codes as well as improved such ones from the norm-trace curve were studied by means of pure Gröbner basis theoretical methods. It is possible to generalize the methods from [10] and [9] to deal with any order domain. Actually, the method can be seen as a consequence of our new bound on the minimum distance. The following definition plays a fundamental role.

**Definition 53.** *Assume a description of an order domain $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ is given as in Theorem 41. Let $\{F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m)\}$ be the Gröbner basis from Theorem 41 for $I$ with respect to $\prec_w$. For $i = 1, \ldots, s$ we let $B_i$ be a difference between the two monomials of highest weight in $F_i$. Finally for all $M \in \Delta_{\prec_w}(I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle)$ we define*

$$D(M) := \#(\Delta_{\prec_w}(\langle B_1, \ldots, B_s, M \rangle) \cap \Delta_{\prec_w}(I_q)).$$

Assume an order domain $R$ with corresponding weight function $\rho$ is described as a quotient ring $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ by the construction in Theorem 41. Consider the variety $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and let as in Section 8 the morphism $\varphi$ be given by

$$\varphi(F + I) := (F(P_1), \ldots, F(P_n)) \tag{25}$$

From Proposition 44 in Section 8 we have

$$\Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}.$$

In this appendix we will show that for all $\lambda \in \Delta(R, \rho, \varphi)$ we have $\sigma(\lambda) = n - D(M)$ where $M \in \Delta_{\prec_w}(I_q)$ is the unique element satisfying $w(M) = \lambda$. From this result it follows immediately that all the statements in Section 8 concerning the minimum distance of codes $C(B, G)$ can be rephrased with $\sigma(\lambda)$ replaced by $n - D(M)$. This observation may serve as a guideline and as a tool in the future work on codes defined by use of pure Gröbner basis theoretical methods. In the following we will assume that the reader is familiar with Buchberger's algorithm.

We will need three lemmas.

**Lemma 54.** *$\{B_1, \ldots, B_s\}$ is a Gröbner basis with respect to $\prec_w$.*

*Proof.* According to Buchberger's algorithm it is enough to show that $S(B_i, B_j)$ rem $\{B_1, \ldots, B_s\} = 0$ for all pairs $(i, j)$. Consider any fixed pair $(i, j)$. We now perform the following procedure. We first calculate $rb(1) := S(B_i, B_j)$ and $rf(1) := S(F_i, F_j)$. Then, as long as $rf(l) \neq 0$ and $rb(l)$ is a polynomial we choose a leading monomial $\mathrm{lm}(F_s)$ $(= \mathrm{lm}(B_s))$ such that $\mathrm{lm}(F_s) \mid \mathrm{lm}(rf(l))$ and define

$$\begin{aligned} rb(l+1) &:= rb(l) - \frac{\mathrm{lc}(rb(l))}{\mathrm{lc}(B_s)} \frac{\mathrm{lm}(rb(l))}{\mathrm{lm}(B_s)} B_s \\ rf(l+1) &:= rf(l) - \frac{\mathrm{lc}(rf(l))}{\mathrm{lc}(F_s)} \frac{\mathrm{lm}(rf(l))}{\mathrm{lm}(F_s)} F_s. \end{aligned}$$

As $\{F_1, \ldots, F_s\}$ is truly a Gröbner basis we know that it is always possible to find an $F_s$ as above until the procedure stops either because $rf(l) = S(F_i, F_j)$ rem $\{F_1, \ldots, F_s\} = 0$ or because $rb(l)$ is not a polynomial. Denote by $e$ the value of $l$ for which the procedure stops. We will show $rb(e) = rf(e) = 0$. We claim that at any step in the procedure either (Inv.1) or (Inv.2) below holds.

(Inv.1) There exist monomials $T_1, T_2$, $T_1 \succ_w T_2$,
scalars $a, b \in \mathbb{F}_q \backslash \{0\}$, $p \in \{-1, 1\}$
and a polynomial $G \in \mathbb{F}_q[X_1, \ldots, X_m]$ with $\mathrm{wdeg}(G) \prec_{\mathbb{N}_0^r} \mathrm{wdeg}(T_1)$
such that $rb(l) = p(T_1 - T_2)$ and $rf(l) = aT_1 + bT_2 + G$

(Inv.2) $rb(l) = rf(l) = 0$

By simple inspection it is seen that for $l = 1$ the above holds. Now any $rf(l)$ must be either zero or must be of the form described in (Inv.1). This is seen as follows. By induction there can in $rf(l)$ be at most two monomials of highest weight. Assume there is an $rf(l)$ with only one monomial of highest weight. But then also $rf(l)$ rem $\{F_1, \ldots, F_s\}$ will have only one monomial of highest weight. This is a contradiction as $rf(l)$ rem $\{F_1, \ldots, F_s\} = 0$ and therefore $rf(l)$ is either zero or is of the form in (Inv.1). With this fact in mind it is now by inspection seen that if (Inv.1) holds in step $l$ then either (Inv.1) or (Inv.2) holds in step $l + 1$. In particular $rb(l)$ is always a polynomial. Therefore at the end of the procedure we must have $rb(l) = 0$ implying $S(B_i, B_j)$ rem $\{B_1, \ldots, B_s\} = 0$ and we are through. □

**Lemma 55.** *The restriction of the map $w : \mathcal{M}(X_1, \ldots, X_m) \to \Gamma$ to $\Delta_{\prec_w}(\langle B_1, \ldots, B_s \rangle)$ is a bijection.*

*Proof.* By assumption $\{F_1, \ldots, F_s\}$ is a Gröbner basis with respect to $\prec_w$. From Lemma 54 we know that also $\{B_1, \ldots, B_s\}$ is a Gröbner basis with respect to $\prec_w$. By the very construction of $B_i$ we have $\mathrm{lm}(B_i) = \mathrm{lm}(F_i)$, $i = 1, \ldots, s$ and it therefore follows from the definition of a Gröbner basis that $\Delta_{\prec_w}(\langle B_1, \ldots, B_s \rangle) = \Delta_{\prec_w}(\langle F_1, \ldots, F_s \rangle)$ holds. From the very construction of the order domain and the weight function in Theorem 41 we know that the restriction of $w : \mathcal{M}(X_1, \ldots, X_m) \to \Gamma$ to $\Delta_{\prec_w}(\langle F_1, \ldots, F_s \rangle)$ is a bijection. But then also is the restriction of $w$ to $\Delta_{\prec_w}(\langle B_1, \ldots, B_s \rangle)$ a bijection. □

**Lemma 56.** *Let $M \in \Delta_{\prec_w}(I_q)$ and write $\lambda = w(M)$. We have*

$$w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M \rangle)\right) = \Gamma \backslash (\lambda + \Gamma). \tag{26}$$

*Proof.* We first show that the left hand side of (26) is contained in the right hand side. By Lemma 55 the restriction of $w$ to $\Delta_{\prec_w}(\langle B_1 \ldots, B_s \rangle)$ is surjective. We conclude that

$$\{w(MM') \mid M' \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s \rangle)\} = \lambda + \Gamma. \tag{27}$$

Next, $w(MM') = w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\})$ and from (27) we conclude

$$\{w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\}) \mid M' \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s \rangle)\} = \lambda + \Gamma. \tag{28}$$

Note that

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$$

and that

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \langle B_1, B_2, \ldots, B_s, M\rangle.$$

In particular

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \notin \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)$$

and we conclude

$$\begin{aligned} MM' \text{ rem } \quad & \{B_1, B_2, \ldots, B_s\} \\ & \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \backslash \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle). \end{aligned} \tag{29}$$

Comparing (28) and (29) we have

$$\lambda + \Gamma \subseteq w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \backslash \Delta_{\prec_w}(\langle B_1, B_2, \ldots, M\rangle)\right).$$

The fact that the restriction of $w$ to $\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$ is injective now implies

$$w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle\right) \subseteq \Gamma \backslash (\lambda + \Gamma).$$

We have shown that the left hand side of (26) is contained in the right hand side.

Next we prove that the right hand side of (26) is contained in the left hand side. We start by considering what can happen when we use Buchberger's algorithm to extend $\{B_1, B_2, \ldots, B_s, M\}$ to a Gröbner basis with respect to $\prec_w$. As $\{B_1, \ldots, B_s\}$ is known to be a Gröbner basis we need not consider the S-polynomials $S(B_i, B_j)$. Hence, at the beginning of the algorithm the only S-polynomials to be considered are the $S$-polynomials $S(B_i, M)$. These polynomials are monomials and they either reduces to 0 modulo $\{B_1, B_2, \ldots, B_s, M\}$ or reduces to a monomial of weight $\lambda + w'$, where $w' \in w(\mathcal{M}(X_1, X_2, \ldots, X_m)) = \Gamma$. Hence, every polynomial adjoined to the basis at the beginning of Buchberger's algorithm is a monomial with weight in $\lambda + \Gamma$. Assume $\widetilde{M}$ is such a monomial. The S-polynomial $S(B_i, \widetilde{M})$ is a monomial that either reduces to 0 or reduces to a monomial $\hat{M}$ of weight $w(\hat{M}) = w(\widetilde{M}) + w'' = \lambda + w' + w''$ with $w'' \in w(\mathcal{M}(X_1, X_2, \ldots, X_m)) = \Gamma$. That is, $S(B_i, \widetilde{M})$ is a monomial that either reduces to 0 or reduces to a monomial $\hat{M}$ with weight in $\lambda + \Gamma$. As the S-polynomial of two monomials is 0, by induction every polynomial added to the basis $\{B_1, \ldots, B_s\}$ throughout Buchberger's algorithm is a monomial with weight in $\lambda + \Gamma$. It follows that every monomial $N$, $N \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \backslash \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)$ has weight in $\lambda + \Gamma$. As the restriction of $w$ to $\Delta_{\prec_w}(\langle B_1, \ldots, B_s\rangle)$ is surjective we conclude $w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle\right) \supseteq \Gamma \backslash (\lambda + \Gamma)$. □

**Proposition 57.** *Let $\varphi$ be as in (25). For $\lambda \in \Delta(R, \rho, \varphi)$ we have $\sigma(\lambda) = n - D(M)$ where $M \in \Delta_{\prec_w}(I_q)$ is the (unique) element satisfying $w(M) = \lambda$.*

*Proof.* The proof use extensively the fact that the restriction of $w$ to $\Delta_{\prec_w}(I_q)$ is injective. From Lemma 56 we get that

$$\begin{aligned} &\Delta_{\prec_w}(\langle B_1, \ldots, B_s, M\rangle) \cap \Delta_{\prec_w}(I_q) \\ &\qquad = \{M \in \Delta_{\prec_w}(I_q) \mid w(M) \notin \lambda + \Gamma\}. \end{aligned} \tag{30}$$

By Definition 28 for $\lambda \in \Delta(R, \rho, \varphi)$ we have

$$\begin{aligned} \sigma(\lambda) &= \#\{\alpha \in \Delta(R, \rho, \varphi) \mid \alpha \in \lambda + \Gamma\} \\ &= \#\{M \in \Delta_{\prec_w}(I_q) \mid w(M) \in \lambda + \Gamma\}. \end{aligned} \tag{31}$$

Comparing (30) and (31) we get

$$\sigma(\lambda) = \#\Delta_{\prec_w}(I_q) - \#(\Delta_{\prec_w}(\langle B_1, \ldots, B_s, M\rangle) \cap \Delta_{\prec_w}(I_q)) = n - D(M).$$

□

# References


[1] H. E. Andersen, On puncturing of codes from Norm-Trace curves, to appear in *Finite Fields and their Applications*.

[2] A. I. Barbero and C. Munuera, The Weight Hierarchy of Hermitian Codes, *SIAM J. Discrete Math.*, **13**, 79-104.

[3] D. Cox, J. Little and D. O'Shea, "Ideals, Varieties, and Algorithms, 2nd ed.," Springer, Berlin, 1997.

[4] D. Cox, J. Little and D. O'Shea, "Using Algebraic Geometry," Springer, Berlin, 1998.

[5] 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.

[6] G.-L. Feng and T.R.N. Rao, Improved Geometric Goppa Codes, Part I:Basic theory, *IEEE Trans. Inform. Theory*, **41**, (1995), 1678-1693.

[7] A. Garcia and H. Stichtenoth, A Tower of Artin-Schreier Extensions of Function Fields, Attaining the Drinfeld-Vladut Bound, *Invent. Math.*, **121**, no. 2, (1995), 211-222.

[8] O. Geil, Codes from Order Domains, Proc. of 2001 IEEE International Symposium on Inform. Theory, Washington, USA, June 24-29, 2001, 308.

[9] O. Geil, On Codes From Norm-Trace Curves, *Finite Fields and their Applications*, **9**, (2003), 351-371.

[10] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci. 2227*, (S. Bozta, I. Sphparlinski, Eds.), Springer, Berlin, 2001, 159-171.

[11] O. Geil and T. Høholdt, On Hyperbolic Type Codes, Proc. of 2003 IEEE International Symposium on Inform. Theory, Yokohama, Japan, June 29-July 4, 2003, 331.

[12] O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields and their Applications*, **8**, (2002), 369-396.

[13] O. Geil and C. Thommesen, On the Feng-Rao Bound for Generalized Hamming Weights, Proc. AAECC-16, *Lecture Notes in Comput. Sci. 3857*, (M. Fossorier, H. Imai, S. Lin and A. Poli, Eds.), Springer, Berlin, 2006, 295-306

[14] P. Heijnen and R. Pellikaan, Generalized Hamming Weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory*, **44**, (1998), 181-196

[15] T. Høholdt, On (or in) Dick Blahut's 'footprint', in "Codes, Curves and Signals," (A. Vardy, Ed.), Kluwer Academic, Norwell, MA, 1998, 3-9.

[16] T. Høholdt, J. van Lint and R. Pellikaan, Algebraic Geometry Codes, Chapter 10 in "Handbook of Coding Theory," (V.S. Pless and W.C. Huffman, Eds.), vol. 1, Elsevier, Amsterdam, 1998, 871-961.

[17] G. Kabatiansky, Two Generalizations of Product Codes, *Proc. of Academy of Science USSR, Cybernetics and Theory of Regulation*, **232**, vol. 6, (1977), 1277-1280 (in Russian).

[18] J. Massey, D. J. Costello and J. Justesen, Polynomial Weights and Code Constructions, *IEEE Trans. Inf. Theory*, **19** (1973), 101-110.

[19] R. Matsumoto, Miura's Generalization of One-Point AG codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization, *IEICE Trans. Fundamentals,* **E82-A**, no. 10 (1999), 2007-2010.

[20] R. Matsumoto and S. Miura, On the Feng-Rao Bound for the $\mathcal{L}$-Construction of Algebraic Geometry Codes, *IEICE Trans. Fundamentals,* **E83-A**, no. 5 (2000), 923-927.

[21] S. Miura, Ph.D. thesis, Univ. Tokyo, May 1997, (in Japanese).

[22] S. Miura, Linear Codes on Affine Algebraic Varieties, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1386-1397 (in Japanese).

[23] S. Miura, Linear Codes on Affine Algebraic Curves, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1398-1421 (in Japanese).

[24] T. Shibuya, J. Mizutani, K. Sakaniwa, On generalized Hamming Weights of codes constructed on Affine algebraic sets, Proc. AAECC-12, *Lecture Notes in Computer Science*, **vol. 1255**, Springer-Verlag, (1997), 311-320.

[25] T. Shibuya, J. Mizutani, K. Sakaniwa, On generalized Hamming Weights of codes constructed on Affine algebraic sets, *IEICE Trans. Fund.*, **E81-A** (1998), 1979-1989.

[26] T.Shibuya and K. Sakaniwa, Lower bound on generalized Hamming weights in terms of a notion af well-behaving, Proc. ISIT 1998, Cambridge, USA, (1998), 96.

[27] T. Shibuya, R. Hasagawa, K. Sakaniwa, A Lower Bound for Generalized Hamming Weights and a Condition for $t$-th Rank MDS, *IEICE Trans. Fund.*, **E82-A**, (1999), 1090-1101.

[28] T. Shibuya and K. Sakaniwa, A Dual of Well-Behaving Type Designed Minimum Distance, *IEICE Trans. Fund.*, **E84-A**, (2001), 647-652.

[29] T. Shibuya and K. Sakaniwa, A note on a Lower Bound for General Hamming Weights, *IEICE Trans. Fund.*, **E84-A**, (2001), 3138-3145.

[30] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inf. Theory*, **37**, (1991), 1412-1418.