AALBORG UNIVERSITY

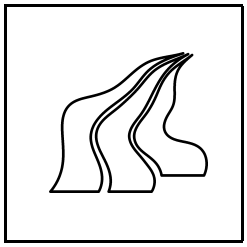
The Missing Evaluation Codes from Order Domain Theory

by

Henning E. Andersen and Olav Geil

June 2004 R-2004-17

Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G ▪ DK - 9220 Aalborg Øst ▪ Denmark
Phone: +45 96 35 80 80 ▪ Telefax: +45 98 15 81 29
URL: www.math.aau.dk/research/reports/reports.htm



ISSN 1399–2503 ▪ On-line version ISSN 1601–7811

The Missing Evaluation Codes from Order Domain Theory

Henning E. Andersen and Olav Geil
Department of Mathematics, Aalborg University,
Fredrik Bajersvej 7G, DK-9220 Aalborg Ø, Denmark
E-mail addresses: henning@math.auc.dk, olav@math.auc.dk

Abstract

The Feng-Rao bound gives a lower bound on 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. Actually our result not only deals with the minimum distance but gives lower bounds on any generalized Hamming weight. 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. The improved codes from the present paper are not in general equal to the Feng-Rao improved codes but the constructions are very much related.

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

I. Introduction

In [3] Feng and Rao showed how to estimate the minimum distance of a large class of algebraically defined codes by considering certain relations between the rows in the corresponding parity check matrices. This result is known today as the Feng-Rao bound. Using the bound Feng and Rao were able to improve a large class of well-known codes by leaving out certain rows in the corresponding parity check matrices.

To deal with the above mentioned code constructions, Høholdt, van Lint and Pellikaan in [14] and [15] introduced the concept of an order function acting on what is known today as an order domain ([12]). Then they reformulated the most important results by Feng and Rao in this new setting. Their code constructions includes the set of duals of one-point geometric Goppa codes, the set of Feng-Rao improved such ones, the set of generalized Reed-Muller codes and the set of Feng-Rao improved such ones (the hyperbolic codes). It should be mentioned that independently of Høholdt et al. Miura in [20] and [21] derived many of the same results. Regarding codes defined by means of their generator matrices, Høholdt et al. in [15] only considered the one-point geometric Goppa codes. More precisely, they showed how to prove the Goppa bound without the use of the Riemann-Roch theorem. One of the nice things about order domains is that they can be understood without the use of algebraic geometry. More precisely, it was shown in [20], [22], [23] and [12] how Gröbner basis theory plays a fundamental role in the theory of order domains.

In [20] and [21] Miura observed that the results by Feng and Rao can be obtained by using only linear algebra. In particular one can view the Feng-Rao bound as a bound on the minimum distance of any linear code (with known parity check matrix). Furthermore it was shown in [19] how to improve the Feng-Rao bound slightly in this general set-up. In the present paper we will initially take the general

point of view on the Feng-Rao bound from [19]. Later we will translate our findings into the frame work of order domain theory.

What is obviously missing in the above description is a Feng-Rao type bound on the minimum distance of codes which are not defined on the basis of parity check matrices but are defined on the basis of generator matrices. This question was treated by Shibuya and Sakaniwa in [25] where they use the theory of generalized Hamming weights to translate the Feng-Rao bound for the codes defined by means of parity check matrices into a bound for the codes defined by means of generator matrices. The bound derived in this way is of a much more complicated form than the Feng-Rao bound and the problem of improving the codes by using the information from the bound is not so easy. Furthermore, the proof of the bound by Shibuya and Sakaniwa is rather complicated.

In this paper we derive a new and very simple bound on the minimum distance of codes defined by means of their generator matrices. Our bound is of a form very similar to the Feng-Rao bound and in particular from our bound it is obvious how to improve the codes. The proof of the new bound is trivial and our result is at least as good as the result by Shibuya and Sakaniwa. Furthermore our bound not only deals with the minimum distance but actually gives lower bounds on any generalized Hamming weights of the considered codes. We show how to deal with the new bounds and the new code construction from an order domain theoretical point of view. We give some very concrete results on how to deal with the code construction in the case of affine variety codes[1] defined from order domains and we derive some results concerning the connection between the Feng-Rao improved codes and the new improved codes. Also we show how to understand our new bound and code construction from a Gröbner basis theoretical point of view. For the case of one-point geometric Goppa codes our bound can easily be shown to be an improvement of the usual bound from algebraic geometry and in many cases we are able to improve substantial on the one-point geometric Goppa code construction. In this way we improve the results in [25] where it was shown that their bound is at least as good as the usual bound from algebraic geometry for the case of one-point geometric Goppa codes from C_{ab} curves. Our new construction and our new bounds can be viewed as a generalization of the recent Gröbner basis theoretical descriptions in [9] and [8] concerning Reed-Muller codes, hyperbolic codes and codes from norm-trace curves. For these codes our bounds are tight.

The paper is organized as follows. In Section II we are concerned with the general set-up from [19]. Here we introduce our new bound on any linear code defined by means of a generator matrix and relate the new bound to the Feng-Rao bound and the bound by Shibuya and Sakaniwa. In Section III we describe the relevant concepts from order domain theory and show how to translate our findings from Section II into the language of order domain theory. In Section IV we treat the connection to the theory of one-point geometric Goppa codes. In Section V we are concerned with affine variety codes from order domains. Section V includes a description of order domains from a Gröbner basis theoretical point of view. Section VI contains some examples of codes and Section VII is the conclusion. In Appendix A we deal with the connection between the construction of the present paper and the recent Gröbner basis theoretically defined constructions from [9] and [8].

II. The new Feng-Rao type bound

We start by introducing some terminology from [19]. To ease the comparison with the results in [25] we will mainly use the notation from there.

[1] So named in [4].

Definition 1: Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$ and consider $G \subseteq B$. We define the $k = \#G$ dimensional code $C(B,G)$ by $C(B,G) := \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{b} \mid \boldsymbol{b} \in G\}$. We denote the dual code by $C^{\perp}(B,G)$.

The following definition plays a central role for the bounds on the minimum distances of the above codes.

Definition 2: For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n), \boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ define the component-wise (or Schur or Hadamard) product $\boldsymbol{u} * \boldsymbol{v} := (u_1v_1, u_2v_2, \ldots, u_nv_n)$. Let $\boldsymbol{b}_0 := \boldsymbol{0} \in \mathbb{F}_q^n$ and define $L_l := \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_l\}$ for $l = 0, \ldots, n$ and $L_{-1} := \emptyset$.

We obviously have a chain of spaces $\{\boldsymbol{0}\} = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_{n-1} \subsetneq L_n = \mathbb{F}_q^n$ and $\dim(L_i) = i$ holds for $i = 0, 1, \ldots, n$. Next we recall the concept of a well-behaving ordered pair. The function $\bar{\mu}$ below is well-known whereas the function $\bar{\sigma}$ is new.

Definition 3: Define $\bar{\rho} : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ by $\bar{\rho}(\boldsymbol{v}) = l$ if $\boldsymbol{v} \in L_l \backslash L_{l-1}$. 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 $(u,v) \neq (i,j)$. 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 $v < j$. For $\{l_1, l_2, \ldots, l_t\} \subseteq I$ and $\{i_1, i_2, \ldots, i_t\} \subseteq I$ define[2]

$$\begin{aligned}
\bar{\mu}(l_1, l_2 \ldots l_t) &:= \#\cup_{s=1,\ldots,t}\{(i,j) \in I^2 \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l_s \text{ and } (i,j) \text{ is WWB }\} \\
\bar{\sigma}(i_1, i_2 \ldots i_t) &:= \#\cup_{s=1,\ldots,t}(\{l \in I \mid \bar{\rho}(\boldsymbol{b}_{i_s} * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \\
&\qquad \text{such that } (i_s, j) \text{ is WWB}\} \cup \{i_s\}).
\end{aligned}$$

We now state the celebrated Feng-Rao bound in the general version from [19].

Theorem 1 (Feng-Rao) The minimum distance of $C^{\perp}(B,G)$ is at least equal to $\min\{\bar{\mu}(i) \mid \boldsymbol{b}_i \in B\backslash G\}$.

A lower bound on the generalized Hamming weights of the codes $C^{\perp}(B,G)$ can be found in [24]. This bound, however, is not nearly as simple as the one we are going to present for the codes $C(B,G)$. In Definition 4 below we give the formal definition from [26] of the generalized Hamming weights. Recall, that for every $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ the set $\mathrm{Supp}(\boldsymbol{v}) := \{i \mid v_i \neq 0\}$ is called the support of $\boldsymbol{v}$ and in general for any subset $A \subseteq \mathbb{F}_q^n$ the set $\mathrm{Supp}(A) := \cup_{\boldsymbol{v} \in A}\mathrm{Supp}(\boldsymbol{v})$ is called the support of A.

Definition 4: Consider a k dimensional code C. For $t = 1, 2, \ldots, k$ the tth generalized Hamming weight is

$$d_t(C) := \min\{\#\mathrm{Supp}(D) \mid D \text{ is a } t \text{ dimensional subcode of } C\}.$$

We next state the new Feng-Rao type bound on the generalized Hamming weights of the code $C(B,G)$.

Theorem 2: 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

$$\min\{\bar{\sigma}(a_1, a_2, \ldots, a_t) \mid a_i \neq a_j \text{ for } i \neq j \text{ and } \{\boldsymbol{b}_{a_1}, \boldsymbol{b}_{a_2}, \ldots, \boldsymbol{b}_{a_t}\} \subseteq G\}.$$

[2]We note that writing WWB rather than only WB in the definition of $\bar{\mu}$ and $\bar{\sigma}$ strengthens the results to be presented in this paper. This is due to the fact that an ordered pair that is WB is of course also WWB.

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

$$\begin{aligned}\min\{\bar{\sigma}(i) \mid \boldsymbol{b}_i \in G\} &= \min\{\#\left(\{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \right. \\ &\qquad \left. \text{such that } (i,j) \text{ is WWB}\} \cup \{i\}\right) \mid \boldsymbol{b}_i \in G\}.\end{aligned}$$

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 $D \subseteq G$ be a subspace of dimension t, $t \leq k$. Consider basis vectors $\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t$ for D

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

By a standard linear algebra result we may without loss of generality 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 $v \neq w$. 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 $\bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l$ (equivalent to saying $\boldsymbol{b}_{a_u} * \boldsymbol{b}_j \in L_l \backslash L_{l-1}$) then by the very definition of WWB we have

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

Hence, the set

$$S := (\cup_{u=1}^{t} \{\boldsymbol{d}_u * \boldsymbol{b}_j \mid (a_u, j) \text{ is WWB }\}) \cup \{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t\} \tag{1}$$

contains at least

$$\begin{aligned}&\#\left((\cup_{u=1,2,\ldots,t} \{l \in I \mid \bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \right. \\ &\qquad \left. \text{such that } (a_u, j) \text{ is WWB}\}) \cup \{a_1, a_2, \ldots, a_t\}\right) \\ = \ &\bar{\sigma}(a_1, a_2, \ldots, a_t)\end{aligned}$$

linearly independent vectors. But the support of S is equal to the support of $\{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t\}$ which in turn is equal to the support of D. Hence, the size of the support of D is at least $\bar{\sigma}(a_1, a_2, \ldots, a_t)$.

■

It is now obvious how to optimize the choice of G to obtain the best codes with respect to the above bound. These are the $\tilde{E}(\delta)$ codes below. For use in Section III we also define the more naive codes $E(s)$.

Definition 5: 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

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

Theorem 3: The minimum distance of $E(s)$ is at least equal to $\min\{\bar{\sigma}(i) \mid i = 1, \ldots, s\}$. The minimum distance of $\tilde{E}(\delta)$ is at least equal to δ.

Proof: By Theorem 2 ■

In Appendix A it is shown that the hyperbolic codes (improved generalized Reed-Muller codes) and the improved one-point geometric Goppa codes from norm-trace curves described in [8] are special examples of the codes $\tilde{E}(\delta)$ of the present paper. Also it is shown that the bounds in Theorem 3 are tight for the Reed-Muller codes, the hyperbolic codes, the one-point geometric Goppa codes from norm-trace curves and for the improved one-point geometric Goppa codes from norm-trace curves. We conclude this section by relating the result in Theorem 2 to the result by Shibuya and Sakaniwa in [25]. Their result is as follows.

Theorem 4 (Shibuya, Sakaniwa) For given B and G let for $i = 1, 2, \ldots, n$

$$\begin{aligned}\mathcal{B}'_i \;:=\; \{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \;\text{ for some } \boldsymbol{b}_j \in B \\ \text{such that } (i,j) \text{ is WWB}\}\end{aligned}$$

and $\mathcal{B}_i := \{\nu \mid \boldsymbol{b}_\nu \in B \backslash G\} \backslash \mathcal{B}'_i$. Define $t(B,G) := \max\{\#\mathcal{B}_i \mid \boldsymbol{b}_i \in G\}$. The minimum distance of $C(B,G)$ is at least $n - k + 1 - t(B,G)$.

Proposition 1: The bound on the minimum distance of $C(B,G)$ in Theorem 2 is at least as good as the bound in Theorem 4.

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

$$\bar{\sigma}(i) = \#(\mathcal{B}'_i \cup \{i\}) \tag{2}$$

The set $\mathcal{B}_i$ consist of the basis elements outside G that does not contribute to the counting in (2). Hence, the number of basis elements outside G that contribute to the counting in (2) is $n - k - \#\mathcal{B}_i$. For i such that $\boldsymbol{b}_i \in G$ the number of elements in G that contribute to the counting in (2) is at least equal to $\#\{i\} = 1$. All together $n - k + 1 - \#\mathcal{B}_i \leq \bar{\sigma}(i)$ holds for all i such that $\boldsymbol{b}_i \in G$. ■

III. Codes defined from order domains

In the previous section 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 $(\boldsymbol{b}_i, \boldsymbol{b}_j)$ is WB (or WWB) and to calculate $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$. This is where order domain theory comes into action. The presentation of order domain theory to be given in this paper mostly relies on [12] where the concepts of an order function and a weight function from [15] are generalized.

Recall, that if Γ is a set and $\prec$ is a total ordering on Γ then $(\Gamma, \prec)$ is called a well-order if every non empty subset of Γ has a smallest element with respect to $\prec$. Given a well-order $(\Gamma, \prec)$ we adjoin an element $-\infty$ to Γ to get $\Gamma_{-\infty} := \Gamma \cup \{-\infty\}$. The ordering $\prec$ extends to an ordering on $\Gamma_{-\infty}$ by the rule $-\infty \prec \gamma$ for all $\gamma \in \Gamma$. Clearly $(\Gamma_{-\infty}, \prec)$ is a well-order. The following definition corresponds to [12][Def. 2.1] (with the little change that in this paper we require an order function to be surjective).

Definition 6: Let $(\Gamma, \prec)$ be a well-order. Let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra (see [2][p. 36]). A surjective map $\rho : R \to \Gamma_{-\infty}$ that satisfies the following five conditions is called an order function.

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

We call (R, ρ, Γ) an order structure and R an order domain (over $\mathbb{F}$).

The order function being surjective ensures the existence of sets of the form $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$. From [12][Def. 3.1 and Pro. 3.2] we have

Theorem 5: Given an order structure (R, ρ, Γ) 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 $\mathbb{F}$. For any $f = c_{\gamma_1} f_{\gamma_1} + \cdots + c_{\gamma_d} f_{\gamma_d}$ with $c_{\gamma_1}, \ldots, c_{\gamma_d} \in \mathbb{F}_q \backslash \{0\}$ $\rho(f) = \max_\prec\{\gamma_1, \ldots, \gamma_d\}$ holds. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma := \{f \in R \mid \rho(f) \preceq \gamma\}$ as a vector space over $\mathbb{F}$.

From [12][Def. 3.1 and Pro. 3.3] we have

Definition 7: The set $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ in Theorem 5 is called a well-behaving basis (for R).

Besides the trivial case $R = \mathbb{F}$ order domains are always of transcendence degree at least 1. Hence, for non-trivial order domains the well-behaving basis $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ consists of infinitely many elements. In this paper we will always assume that the order domain under consideration is non-trivial. The following well-known concept will help us construct the finite bases B needed in the code constructions from the previous section.

Definition 8: Let R be an $\mathbb{F}_q$-algebra. A map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$.

To derive the finite bases B we will just need the following definition.

Definition 9: Let 0 be the smallest element of Γ and define $\alpha(1) := 0$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ 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 6: Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be as in Definition 9. The set

$$B := \{\boldsymbol{b}_1 := \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 := \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n := \varphi(f_{\alpha(n)})\} \tag{3}$$

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

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

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 (3). According to our agenda we should now be concerned with studying which ordered pairs $(i, j) \in I^2$ that are well-behaving. The following two propositions will give us precisely the information that we need. The results described in these propositions can be found in [20], [21], [19] and [25] 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 explicit and for all non-trivial order domains.

Proposition 2: Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be the basis in (3). If $\alpha(i), \alpha(j), \alpha(l) \in \Delta(R, \rho, \varphi)$ are such that $\rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l)$ 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

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

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 $(O.3)$ in Definition 6 we have $\rho(f_{\alpha(u)} f_{\alpha(v)}) \prec \alpha(l)$. But then by Definition 8 and Definition 9 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 3: Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$. 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 $(O.3)$ in Definition 6 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 $\alpha(l)$. ■

We are now in the position that we can give a simple description of the codes $C^\perp(B, G)$ and $C(B, G)$ related to order domains. To this end consider Definition 10 and Definition 11 below. Here the N and μ

notation is a slightly modification of the notation in [15][Def. 4.8], whereas the M and σ notation is new.

Definition 10: For $\lambda \in \Gamma$ define

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

Define $\mu(\lambda) := \#N(\lambda)$ if $N(\lambda)$ is finite and $\mu(\lambda) = \infty$ if not. For $\eta \in \Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define

$$M(\eta) := \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi)\} \text{ with } \rho(f_\eta f_\beta) = \gamma\}$$

and $\sigma(\eta) := \#M(\eta)$.

Definition 11: Let $t \leq n$ and $\{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi)$. Define $\sigma(\eta_1, \eta_2, \ldots, \eta_t) := \# \cup_{i=1}^{t} M(\eta_i)$.

The codes are now defined as follows.

Definition 12: Consider a well-behaving basis $\{f_\lambda \mid \rho(f_\lambda) = \lambda\}_{\lambda \in \Gamma}$ for an order structure (R, ρ, Γ) over $\mathbb{F}_q$. Let φ be a morphism as in Definition 8 and let $B = \{\boldsymbol{b}_1 = \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 = \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n = \varphi(f_{\alpha(n)})\}$ as in (3). Define

$$\begin{aligned}
C(\lambda) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\} \\
&= (\varphi(R_\lambda))^\perp \\
\tilde{C}(\delta) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \text{ for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\} \\
E(\lambda) &:= \varphi(R_\lambda) \\
\tilde{E}(\delta) &:= \operatorname{span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \text{ and } \sigma(\alpha(i)) \geq \delta\}
\end{aligned}$$

The result concerning $C(\lambda)$ and $\tilde{C}(\delta)$ in the next theorem is from [15]. The result concerning $C(\lambda)$ is known as the order bound. The remaining results are new.

Theorem 7: The minimum distance of $C(\lambda)$ and $\tilde{C}(\delta)$ satisfy

$$\begin{aligned}
d(C(\lambda)) &\geq \min\{\mu(\eta) \mid \lambda \prec \eta, \eta \in \Delta(R, \rho, \varphi)\} &(4)\\
&\geq \min\{\mu(\eta) \mid \lambda \prec \eta\} &(5)\\
d(\tilde{C}(\delta)) &\geq \delta. &(6)
\end{aligned}$$

The tth generalized Hamming weight of $E(\lambda)$ and $\tilde{E}(\delta)$ (t being at most equal to the dimension of the code) satisfies

$$\begin{aligned}
d_t(E(\lambda)) \geq \min\{&\sigma(\eta_1, \eta_2, \ldots, \eta_t) \mid \{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi) \\
&\eta_i \neq \eta_j \text{ for } i \neq j, \eta_s \preceq \lambda \text{ for } s = 1, \ldots, t\} &(7)\\
d_t(\tilde{E}(\delta)) \geq \min\{&\sigma(\eta_1, \eta_2, \ldots, \eta_t) \mid \{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi) \\
&\eta_i \neq \eta_j \text{ for } i \neq j, \sigma(\eta_s) \geq \delta \text{ for } s = 1, \ldots, t\}. &(8)
\end{aligned}$$

In particular

$$\begin{aligned}
d(E(\lambda)) &\geq \min\{\sigma(\eta) \mid \eta \in \Delta(R, \rho, \varphi), \eta \preceq \lambda\} &(9)\\
d(\tilde{E}(\delta)) &\geq \delta. &(10)
\end{aligned}$$

Proof: Using the notation from Definition 3 and Definition 10 and the results from Proposition 2 and Proposition 3 we verify that $\bar{\mu}(i) \geq \mu(\alpha(i))$. To see that also $\bar{\sigma}(i) \geq \sigma(\alpha(i))$ we note that by [12][Pro. 2.5] the following holds. If the smallest element in Γ is denoted 0 then the elements in R that satisfy $\rho(f) = 0$ are precisely the elements in $\mathbb{F}_q \backslash \{0\}$. Hence, by condition $(O.1)$ in Definition 6 we have $\rho(f_0 f_\gamma) = \gamma$ for all $\gamma \in \Gamma$ and therefore by Proposition 2 and Proposition 3 $\bar{\sigma}(i) \geq \sigma(\alpha(i))$ holds. The theorem now follows by applying Theorem 1 and Theorem 2. ■

It is obvious that with respect to the above bounds the $\tilde{C}(\delta)$ construction is an improvement to the $C(\lambda)$ construction and the $\tilde{E}(\delta)$ construction is an improvement to the $E(\lambda)$ construction. In Section IV we will recall the well-known fact that every one-point geometric Goppa code can be described as an $E(\lambda)$ code related to an order domain of transcendence degree 1, and we will show by a very easy argument that the bound (9) is an improvement to the usual bound from algebraic geometry.

We conclude this section by discussing the concept of a weight function. It is well-known that the order function ρ induces a binary operation on Γ by $\rho(f) + \rho(g) = \rho(fg)$. This turns Γ into a semigroup called the value semigroup of ρ. The order structure (R, ρ, Γ) is called finitely generated if the value semigroup is finitely generated. Whenever an order structure (R, ρ, Γ) is finitely generated then by [12][Cor. 5.7] we may without loss of generality assume that the order function is a weight function as in the following definition.

Definition 13: Let $\prec$ be a monomial ordering on $\mathbb{N}_0^r$ and let $+$ be the ordinary $+$ extended with the rule $-\infty + a = a + (-\infty) = -\infty + (-\infty) = -\infty$. Let R be an $\mathbb{F}$-algebra. A weight function on R is an order function $\rho : R \to \Gamma \cup \{-\infty\} \subseteq \mathbb{N}_0^r \cup \{-\infty\}$ such that

$$(O.5) \quad \rho(fg) = \rho(f) + \rho(g) \quad \text{for all } f, g \in R.$$

The calculation of the values of the functions μ and σ becomes much easier whenever ρ is not just an order function but merely a weight function. We have

$$\begin{aligned} N(\lambda) &= \{(\alpha, \beta) \in \Gamma^2 \mid \alpha + \beta = \lambda\} \\ M(\eta) &= \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \eta + \beta = \gamma\} \\ &= (\eta + \Gamma) \cap \Delta(R, \rho, \varphi) \end{aligned} \tag{11}$$

where $\eta + \Gamma$ means $\{\eta + \lambda \mid \lambda \in \Gamma\}$.

IV. Improved one-point geometric Goppa codes

In this section we will see how to construct improved one-point geometric Goppa codes and we will see how to improve on the Goppa bound. The following example is well-known (see [15][Ex. 3.8] and [18][Th. 1]).

Example 1: Consider a curve $\mathcal{X}$ with a single place $\mathcal{P}_{-\infty}$ at infinity. Let $\nu_{\mathcal{P}_{-\infty}}$ denote the discrete valuation corresponding to the place $\mathcal{P}_{-\infty}$. Let R be any subring of the union of $\mathcal{L}$-spaces corresponding to $\mathcal{P}_{-\infty}$. That is, let $R \subseteq \cup_{i=0}^{\infty} \mathcal{L}(i\mathcal{P}_{-\infty})$. Then R is an order domain with a weight function given by $\rho(f) = -\nu_{\mathcal{P}_{-\infty}}(f)$. It is well-known that all weight functions with a numerical value semigroup are of the form described in this example.

From Example 1 it is clear that the one-point geometric Goppa codes are precisely the codes $E(\lambda)$

defined from order structures with a weight function with a numerical value semigroup. In the same way of course the duals of one-point geometric Goppa codes are precisely the codes $C(\lambda)$ defined from order structures with a weight function with a numerical value semigroup. By [15][Th. 5.24] the bound (5) and thereby also (4) are improvements to the Goppa bound for the duals of one-point geometric Goppa codes. Clearly, the corresponding codes $\tilde{C}(\delta)$ become improvements to the duals of one-point geometric Goppa codes.

By using the following lemma from [15][Lem. 5.15] we now give an easy proof that also the bound (9) is an improvement to the Goppa bound for the one-point geometric Goppa codes. It follows that the codes $\tilde{E}(\delta)$ can be viewed as improved one-point geometric Goppa codes.

Lemma 1: Let Γ be a numerical semigroup with finitely many gaps. Let $i \in \Gamma$. Then the number of elements of $\Gamma \backslash (i + \Gamma)$ is equal to i.

Now the Goppa bound for the one-point geometric Goppa code $E(\lambda)$ says $d(E(\lambda)) \geq n - \lambda$. For comparison, by (11) the bound (9) states

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

By Lemma 1 we have

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

with equality if and only if $\Gamma \backslash (i + \Gamma) \subseteq \Delta(R, \rho, \varphi)$. In particular for λ being of a high value compared to n the just mentioned condition for equality often turns out not be fulfilled and the new bound will be an improvement to the Goppa bound. We have proved the last part of the following proposition.

Proposition 4: Any one-point geometric Goppa code is of the form $E(\lambda)$ in Definition 12 and the bound (9) is an improvement to the Goppa bound.

For comparison, Shibuya et al. in [25] only show that their bound (Theorem 4) 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 [5]. In Section VI we shall demonstrate that the new bound (9) can be much better than the Goppa bound and that the new construction $\tilde{E}(\delta)$ can be much better than traditional one-point geometric Goppa code.

V. The Gröbner basis approach

In this section we shall see how to easily construct order domains and related codes by the use of Gröbner basis theoretical methods. We start by introducing some concepts from Gröbner basis theory.

Definition 14: 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[3] of L is the set

$$\begin{aligned} \Delta_{\prec}(L) \;:=\; \{&M \in \mathcal{M}(X_1, X_2, \ldots, X_m) \mid M \\ &\text{is not a leading monomial of any polynomial in } L\}. \end{aligned}$$

[3]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 [13]).

The following well-known proposition (for a reference, see [1][Pro. 4 in Paragraph 5.3]) explains why footprints are interesting.

Proposition 5: Let $L \subseteq \mathbb{F}[X_1, \ldots, X_m]$ be any 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 $\mathbb{F}$.

The first part of the following proposition is a corollary to Proposition 5. It is known as the footprint bound. A proof of the proposition below can be found in [1][Pro. 8] and [2][Pro. 2.7].

Proposition 6: If $\Delta_\prec(L)$ is finite then the size of the variety $\mathbb{V}_\mathbb{F}(L)$ is bounded by

$$\#\mathbb{V}_\mathbb{F}(L) \leq \#\Delta_\prec(L). \tag{12}$$

If L is a radical ideal then equality holds in (12). In particular equality holds when $L \subseteq \mathbb{F}_q[X_1, X_2, \ldots, X_m]$ and $X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m \in L$.

We will need the following generalization from [12][Def. 9.2] of the usual weighted degree lexicographic ordering.

Definition 15: 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 $\mathrm{wdeg}(F)$ 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 $M_1 \prec_\mathcal{M} M_2$.

The next theorem characterizes all finitely generated order structures. Note that in particular (R, ρ, Γ) is finitely generated if ρ is a weight function with a numerical value semigroup. It corresponds to [12][Th. 9.1 and Th. 10.4].

Theorem 8: Let $I \subset \mathbb{F}[X_1, X_2, \ldots, X_m]$ be an ideal with Gröbner basis $\mathcal{B}$ with respect to $\prec_w$ (see Definition 15). Suppose that the elements of the footprint $\Delta_{\prec_w}(I)$ have mutually distinct weights and that every element of $\mathcal{B}$ 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 $F \in \mathrm{span}_\mathbb{F}\{M \mid M \in \Delta_{\prec_w}(I)$. We have $\rho(f) = \mathrm{wdeg}(F)$ and $\rho(0) = -\infty$.
On the other hand if (R, ρ, Γ) is a finitely generated order structure then after having embedded Γ into $\mathbb{N}_0^r$ one can up to isomorphism describe R as above. In this way the original order function on R becomes a weight function (described as above).

Not only have we by the above theorem a simple way of describing order domains but also by Proposition 7 below we have a simple way of actually constructing the corresponding codes. We will need

the following definition.

Definition 16: 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 result was treated in [20][Sec. 5.4] and [22][p. 147] (both in Japanese) for the case of $w(X_1), w(X_2), \ldots, w(X_m) \in \mathbb{N}_0$. Here we consider the general case (this result was included without a proof in the abstract [6]).

Proposition 7: Let (R, ρ, Γ) be an order structure described as in Theorem 8. Consider the affine variety $\mathbb{V}_{\mathbb{F}_q}(I) = \mathbb{V}_{\mathbb{F}_q}(I_q) = \{P_1, P_2, \ldots, P_n\}$. The affine variety map $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(F + I) := (F(P_1), F(P_2), \ldots, F(P_n))$ is a morphism as in Definition 8. Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be given as in Definition 9. We have

$$\Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}. \tag{13}$$

Proof: Clearly φ is well-defined and satisfies the conditions in Definition 8. This establish the first result.
By Proposition 6 the two sets in (13) are of the same size. Hence, we will be through 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 8 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 $\mathcal{B}'$ be a Gröbner basis for I_q with respect to $\prec_w$. We now reduce F modulo $\mathcal{B}'$ using the division algorithm ([1][Sec. 2, Par. 3]) 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 therefore

$$\varphi(f) = \varphi(F + I) = \varphi(\sum_{i=1}^{l} \beta_i N_i + I). \tag{14}$$

Note that as $\varphi(f)$ by the very definition of $\alpha(s)$ is nonzero (14) 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 very 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

$$\alpha(s) \succeq_{\mathbb{N}_0^r} w(N_1). \tag{15}$$

Comparing (14) and (15) and using the definition of $\alpha(s)$ gives $\alpha(s) = w(N_1) \in \Delta_{\prec_w}(I_q)$. ■

The following proposition gives some simple conditions under which the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ defined by use of the affine variety map in Proposition 7 are of the same dimension.

Proposition 8: Let R be an order domain described as in Theorem 8. 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

$$\Delta_{\prec_w}(I_q) = \{X_1^{\beta_1} X_2^{\beta_2} \ldots X_m^{\beta_m} \mid \beta_1 \leq \gamma_1, \beta_2 \leq \gamma_2, \ldots, \beta_m \leq \gamma_m\} \tag{16}$$

for some $(\gamma_1, \gamma_2, \ldots, \gamma_m) \in \mathbb{N}_0^m$ then for any $\delta \in \{1, 2, \ldots, n\}$ we have

$$\#\{i \in \{1, 2, \ldots, n\} \mid \sigma(\alpha(i)) = \delta\} = \#\{i \in \{1, 2, \ldots, n\} \mid \mu(\alpha(i)) = \delta\}. \quad (17)$$

Proof: 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 μ and σ (16) implies that for all $\alpha(l) \in \Delta(R, \rho, \varphi)$ we have $\mu(\alpha(l)) = \sigma(\alpha_{\max} - \alpha(l))$. ∎

Clearly, if R and φ are given as in Proposition 8 and if (16) is satisfied then the dimensions of the related codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ will be the same. The next section includes examples where (16) is satisfied but also an example illustrating that if R and φ are given as in Proposition 8, but (16) is not satisfied then it may happen that the dimensions of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ are not the same for almost all choices of $\delta \in \{1, 2, \ldots, n\}$. In the Appendix A two types of algebraic structures are described where not only (16) is satisfied but actually $\tilde{E}(\delta) = \tilde{C}(\delta)$ holds for all $\delta \in \{1, 2, \ldots, n\}$.

VI. Examples

In this section we make extensive use of the notation from Definition 15, Theorem 8 and Proposition 7.

Example 2: Let $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z \rangle \subseteq \mathbb{F}_{16}[X, Y, Z]$. Define the weighted degree lexicographic 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 $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z$. Using Theorem 8 we get a weight function

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

By Proposition 6 the variety $\mathbb{V}_{\mathbb{F}_{16}}(I_{16})$ is of size equal to $\#\Delta_{\prec_w}(I_{16}) = 256$. Let φ 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 (16) of Proposition 8 is satisfied and therefore the dimension of $\tilde{C}(\delta)$ equals the dimension of $\tilde{E}(\delta)$ for all $\delta = 1, 2, \ldots, 256$. In Figure 1 we plot the (estimated) parameters of the codes $\tilde{E}(\delta)$. 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 3: In [10] and [11] the parameters of the codes $\tilde{C}(\delta)$ coming from repeated tensor products of the Hermitian order domain were considered. The footprint $\Delta_{\prec_w}(I_q)$ involved in the construction of the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ from the (single) Hermitian order domain satisfies the condition in (16) of Proposition 8. It follows immediately that the footprints involved in the construction of the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ from repeated tensor products of Hermitian order domains also satisfy the condition in (16) of Proposition 8. Hence, the estimates in [10] of the parameters of the codes $\tilde{C}(\delta)$ from repeated tensor products also holds for the corresponding codes $\tilde{E}(\delta)$.

Example 4: Consider the order domain $R := \mathbb{F}_{16}[X, Y, Z, U]/I$ where $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z, Z^5 + U^4 + U^2 \rangle$ (note the term U^2). The construction of codes from this order domain does not

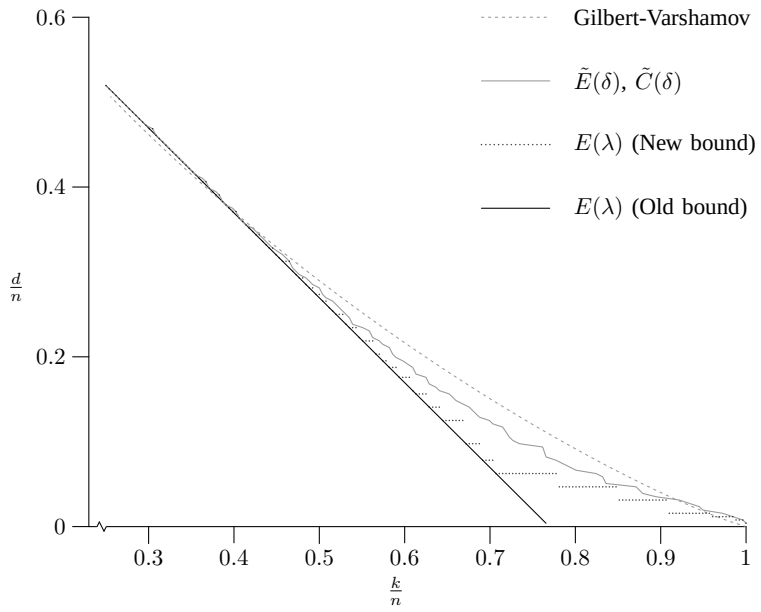


Fig. 1.

satisfy the condition in (16) of Proposition 8. In Figure 2 we plot the estimated performance of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$. It is clear that for values of k/n smaller than approximately 0.2 the codes $\tilde{E}(\delta)$ are the best whereas for larger values the codes $\tilde{C}(\delta)$ 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 5: In the technical report [7][Ex. 12] it was shown that $\mathbb{F}_{q^2}[X,Y,Z,U]/I$ where

$$I := \langle X^q + YZ^q - Y^qZ - X, U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U \rangle$$

and where $a, b \in \mathbb{F}_q$ is an order domain with a weight function given as follows. Define weights

$$\begin{array}{ll} w(X) = (q,1) & w(Y) = (0,q) \\ w(Z) = (q,0) & w(U) = (q+1,0) \end{array}$$

Define $\prec_{\mathbb{N}_0^2}$ such that $(q,q^2) \prec_{\mathbb{N}_0^2} (q^2,q)$ and such that

$$(q^2,q),(q,q^2),(0,q^2+q) \prec_{\mathbb{N}_0^2} (q^2+q,0).$$

Finally define $\prec_{\mathcal{M}}$ such that $YZ^q \prec_{\mathcal{M}} X^q$, $Z^{q+1} \prec_{\mathcal{M}} U^q$ and apply Theorem 8. It was shown in [7][Ex. 12] that

$$\Delta_{\prec_w}(I_{q^2}) = \{X^aY^bZ^cU^d \mid a,d < q \text{ and } b,c < q^2\}.$$

This footprint satisfies the condition in (16) of Proposition 8. Hence, the dimension of the code $\tilde{E}(\delta)$ equals the dimension of the code $\tilde{C}(\delta)$ for all choices of δ and the codes are of length $n = (q^2)^3 = q^6$. In Figure 3 we plot the estimated performance of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ form the present example in the case $\mathbb{F}_{q^2} = \mathbb{F}_{64}$. These are of length $n = 262144$. The hyperbolic codes $\mathrm{Hyp}_{64}(s,3)$ and the generalized Reed-Muller codes $\mathrm{RM}_{64}(s,3)$ are of the same length, but according to Figure 3 they do not perform nearly as good as the codes from the present example.

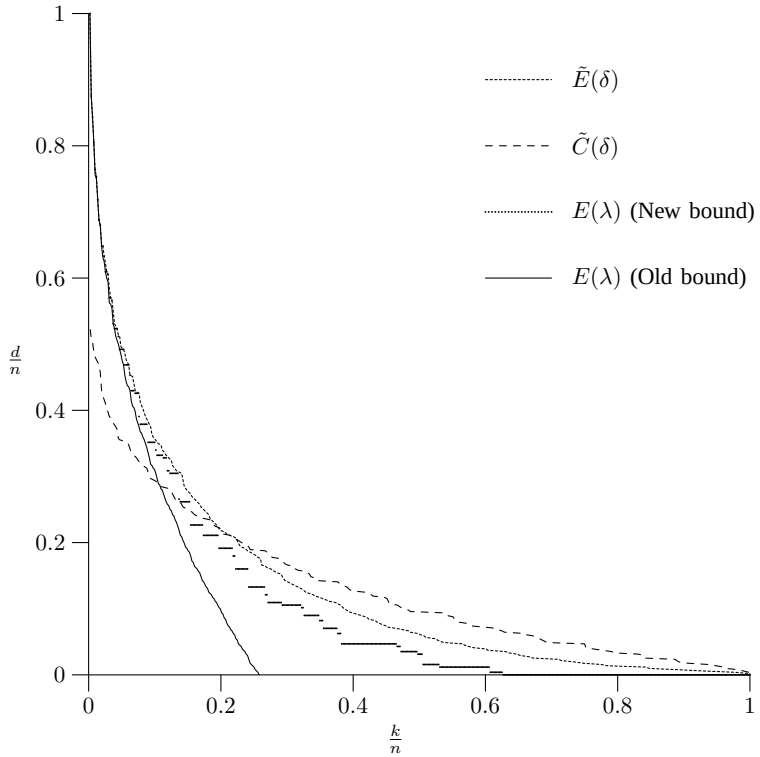

1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1
$\frac{d}{n}$
$\frac{k}{n}$
$\tilde{E}(\delta)$
$\tilde{C}(\delta)$
$E(\lambda)$ (New bound)
$E(\lambda)$ (Old bound)

Fig. 2.

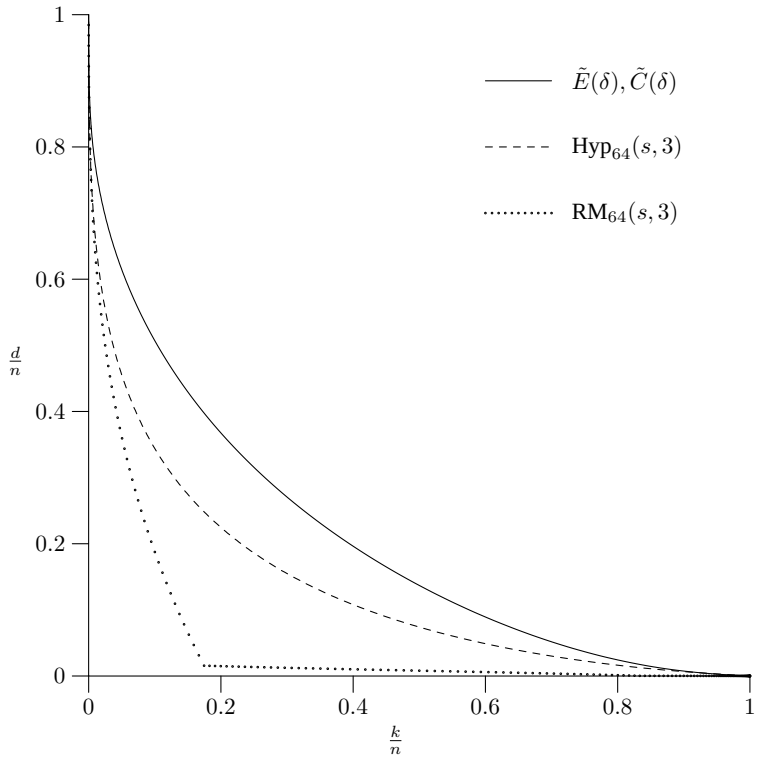

1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1
$\frac{d}{n}$
$\frac{k}{n}$
$\tilde{E}(\delta), \tilde{C}(\delta)$
$\text{Hyp}_{64}(s,3)$
$\text{RM}_{64}(s,3)$

Fig. 3.

VII. Conclusion

In this paper we have presented the missing evaluation codes from order domain theory and we have studied various features of these new codes. It remains to derive decoding algorithms for the new codes. It would be obvious to try to investigate if it is possible to modify the Guruswami-Sudan algorithm for one-point geometric Goppa codes to deal with the new improved one-point geometric Goppa codes. In the light of the relatively simple bound on the generalized Hamming weights for the codes $C(B,G)$ of this paper it would be obvious to try to derive a simpler bound on the generalized Hamming weights for the codes $C^{\perp}(B,G)$ than the ones that can be found in the literature.

Appendix

I. A pure Gröbner basis theoretical approach

In [9] and [8] some concrete improved code constructions were given in the language of Gröbner basis theory. These code constructions heavily rely on the footprint bound (Proposition 6). To establish the connection between the results in [9] and [8] and the results in the present paper consider the following generalization of the function D from [9][p. 160] and [8][Def. 3].

Definition 17: Assume a description of a finitely generated order domain is given as in Theorem 8. Write

$$\mathcal{B} = \{F_1(X_1, X_2, \ldots, X_m), F_2(X_1, X_2, \ldots, X_m), \ldots, F_s(X_1, X_2, \ldots, X_m)\}$$

and let for $i = 1, 2, \ldots, s$, B_i be a difference between the two monomials of highest weight in F_i. For all $M \in \Delta_{\prec_w}(I_q = I + \langle X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m\rangle)$ define

$$D(M) := \#(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle) \cap \Delta_{\prec_w}(I_q)). \tag{18}$$

By use of Gröbner basis theoretical arguments we can show how to generalize the results from [9] and [8] to a construction of improved codes from any order domain. The function D from Definition 17 plays a fundamental role in this construction. However, our construction turns out to be just the code construction $\tilde{E}(\delta)$ from the present paper by Proposition 9 below. More general the following result together with Theorem 7 may serve as a guideline for the future work on constructing improved codes by the use of Gröbner basis theoretical methods.

Proposition 9: Let $M \in \Delta_{\prec_w}(I_q)$ and $\rho(M+I) = \lambda$ (that is, $w(M) = \lambda$). We have $\sigma(\lambda) = n - D(M)$.

Proof: We first note that $\{B_1, B_2, \ldots, B_s\}$ is a Gröbner basis for $\langle B_1, B_2, \ldots, B_s\rangle$ with respect to $\prec_w$ and that

$$\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) = \Delta_{\prec_w}(\langle F_1, F_2, \ldots, F_s\rangle)$$

holds. The first fact can be shown by considering what takes place in Buchberger's algorithm (see [1]) and the last fact is obvious. By the conditions in Theorem 8 the restriction of the map

$$w : \mathcal{M}(X_1, X_2, \ldots, X_m) \to \Gamma$$

to $\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$ is a bijective map. The proposition will follow from (11) and Proposition 7 if we can show that

$$w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)\right) = \Gamma \backslash (\lambda + \Gamma). \tag{19}$$

We first show that the left hand side of (19) is contained in the right hand side. We have

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

$$\Downarrow$$

$$\{w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\}) \mid M' \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)\} = \lambda + \Gamma \tag{20}$$

Here, MM' rem $\{B_1, B_2, \ldots, B_s\}$ means the remainder of MM' after division with $\{B_1, B_2, \ldots, B_s\}$ and the implication follows from the fact $w(MM') = w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\})$. 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

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \backslash \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle). \tag{21}$$

Comparing (20) and (21) we have

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

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

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

Next we prove that the right hand side of (19) 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 $\prec_w$. Consider the S-polynomials (see [1]) $S(B_i, M)$. These polynomials (actually monomials) either reduces to 0 modulo $\{B_1, B_2, \ldots, B_s, M\}$ or reduces to a monomial of weight $\lambda + w'$, where $w' \in w(\mathcal{M}(X_1, X_2, \ldots, X_m)) = \Gamma$. The S-polynomial of two monomials in turn is 0. Hence, by induction every new polynomial adjoined to the basis in a given step of 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 $\lambda + \Gamma$. We conclude $w\left(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle\right) \supseteq \Gamma \backslash (\lambda + \Gamma)$ ■

As already mentioned the function $D(M)$ plays a fundamental role in [9] where the generalized Reed-Muller codes and the hyperbolic codes[4] (improved generalized Reed-Muller codes) are studied. The function also plays a fundamental role in [8] where one-point geometric Goppa codes and improved one-point geometric Goppa codes from norm-trace curves $X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y$ over $\mathbb{F}_{q^r}$ are studied (including improved Hermitian codes). Using Proposition 6 the authors of the above mentioned two papers derive improved code constructions for the considered algebraic structures that by the use of Proposition 9 can be shown to be identical to the improved code constructions from the present paper. Also bounds similar to (9) and (10) are described for the considered algebraic structures. Moreover these bounds are shown to be tight. Hence, our bounds (9) and (10) are known to be tight for some relatively large classes of codes. The code constructions in the two papers satisfy the conditions in Proposition 8. Moreover, it was shown it both papers that actually $\tilde{E}(\delta) = \tilde{C}(\delta)$ holds for all choices of $\delta \in \{1, 2, \ldots, n\}$ for the considered algebraic structures.

[4]The name hyperbolic code comes from [15]. In [16] Kabatiansky studied the very same codes. He calls the codes Massey-Costello-Justesen codes with at reference to [17].

References

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

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

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

[4] J. Fitzgerald and R. F. Lax, Decoding Affine Variety Codes Using Gröbner Bases, *Designs, Codes and Cryptography*, **13**, **2**, (1998), 147-158.

[5] 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.

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

[7] O. Geil, On The Construction of Codes from Order Domains, Technical report R-00-2013, Department of Mathematical Sciences, Aalborg University, 2000.

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

[9] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci. 2227*, Springer, Berlin, 2001, 159-171.

[10] 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.

[11] O. Geil and T. Høholdt, On Hyperbolic Type Codes, Technical report, to appear.

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

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

[14] T. Høholdt, J. van Lint and R. Pellikaan, Order Functions and Evaluation Codes, Proc. AAECC-12, *Lecture Notes in Comput. Sci. 1255*, Springer, Berlin, 1997, 138-150.

[15] 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.

[16] 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).

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

[18] 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.

[19] 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.

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

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

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

[23] R. Pellikaan, On the existence of order functions, *Journal of Statistical Planning and Inference,* **94**, no. 2 (2001), 287-301.

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

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

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