Algebraic geometry codes from order domains

Olav Geil
Department of Mathematical Sciences
Aalborg University

Abstract

In this tutorial we introduce order domains and study the related codes. Special attention is given to the one-point geometric Goppa codes. We show how Gröbner basis theory helps us constructing order domains as well as helps us dealing with the related codes.

1 Introduction

The theory of order domains is a relatively new key object in the study of algebraic geometry codes. It provides us with a simplified understanding of more well established results and gives rise to new findings and constructions. By use of the theory one can give a simple proof of the usual bounds from algebraic geometry on the minimum distance of one-point geometric Goppa codes $C_{\mathcal{L}}(D, m\mathcal{P})$ and $C_{\Omega}(D, m\mathcal{P})$. In a Feng-Rao type manner it is often possible to improve on the above bounds and using the improved information one can then construct improved codes. Furthermore, order domain theory gives us an easy way of generalizing the concept of one-point geometric Goppa codes to algebraic structures of higher transcendence degree. The very definition of order domains finally implies that the Berlekamp-Massey-Sakata decoding algorithm can be easily applied to any of the above codes for which a parity check matrix description is given.
Order domain codes can be viewed as generalizations of Reed-Solomon codes. Recall that Reed-Solomon codes are defined from the polynomial ring $R = \mathbb{F}_q[X]$. Denoting $\mathbb{F}_q = \{P_1, \ldots, P_q\}$ the Reed-Solomon code with parameters $[n = q, k, d = n - k + 1]$ (here of course $k \leq q$ must hold) is

$$\{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < k\} = \{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < n - k\}^{\perp}.$$

The parameters of the Reed-Solomon code are easily demonstrated by using the fact that a polynomial of degree t can have at most t zeros. From an order domain perspective $R = \mathbb{F}_q[X]$ is an order domain and the degree function $\rho : \mathbb{F}_q[X] \rightarrow \mathbb{N}_0 \cup \{-\infty\}$, $\rho(F(X)) = \deg(F)$ is a weight function. The codes are defined by using the map $\varphi : \mathbb{F}_q[X] \rightarrow \mathbb{F}_q^n$, $\varphi(F(X)) = (F(P_1), \ldots, F(P_n))$ and the parameters can be found by studying the properties of ρ and φ.
The next most simple examples of order domain codes are the Hermitian codes, the improved Hermitian codes, the generalized Reed-Muller codes and the improved generalized Reed-Muller codes known as hyperbolic codes. Throughout the paper we will investigate the behavior of these codes and the nature of the

algebraic structures used for their construction. The idea is to make it easier for the reader to grasp the general theory of order domains.
The paper is organized as follows. In Section 2 we explain what is an order domain with a weight function. Then in Section 3 we introduce codes defined from order domains and estimate their parameters. Section 4 is concerned with one-point geometric Goppa codes. In Section 5 we show how to easily construct order domains by use of Gröbner basis methods, and in Section 6 we see how Gröbner basis theory helps us construct the corresponding codes. Finally, in Section 7 we briefly discuss the connection to valuation theory. Being a tutorial the paper contains only known results. Our presentation mostly relies on [12], [15], [9] and [2].

2 Order domains with weight functions

We start our treatment of weight functions by considering in detail the Hermitian order domain.

Example 1 Consider the Hermitian polynomial $X^{q+1} - Y^q - Y$ and let I be the ideal $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y]$. The Hermitian order domain is $R = \mathbb{F}_{q^2}[X, Y]/I$. As will be shown in Example 9 of Section 5 one possible basis for R as a vector space over $\mathbb{F}_{q^2}$ is $\mathcal{B} = \{X^i Y^j + I \mid 0 \leq i, 0 \leq j < q\}$. Denote by $\mathcal{M}(X, Y)$ the monomials in X and Y and define a function $w : \mathcal{M}(X, Y) \to \mathbb{N}_0$ by $w(X^i Y^j) = iq + j(q+1)$. The value $w(X^i Y^j)$ will be called the weight of $X^i Y^j$. We observe that the restriction of w to $\{X^i Y^j \mid 0 \leq i, 0 \leq j < q\}$ is injective. Therefore w induces a bijective map $\rho : \mathcal{B} \to \langle q, q+1 \rangle$ by $\rho(X^i Y^j + I) = w(X^i Y^j)$. Here, $\langle q, q+1 \rangle$ denotes the numerical semigroup generated by q and $q+1$. As $\mathcal{B}$ is a basis it is clear that any element $f \in R$ can be uniquely described as $f = F(X, Y) + I$ where every monomial $X^i Y^j$ in the support of $F(X, Y)$ satisfies $0 \leq i$, $0 \leq j < q$. This unique polynomial will be called the canonical representative of f. Given a description $F'(X, Y) + I$ not of this form we can substitute repeatedly any occurrences of Y^q with $X^{q+1} - Y$ and thereby eventually get a description $F(X, Y) + I$ of the desired form. We can now extend ρ to a function on R. Let $F(X, Y)$ be the canonical representative of f, we define $\rho(0 + I) = -\infty$ and

$$\rho(f) = \max\{w(M) \mid M \text{ is in the support of } F(X, Y)\}$$

when $F(X, Y) \neq 0$. Observe, that $F(X, Y)$ either is 0 or has precisely one monomial of highest weight in its support. Given two nonzero elements $f_1 = F_1(X, Y) + I$, $f_2 = F_2(X, Y) + I$ where $F_1(X, Y)$ respectively $F_2(X, Y)$ is the canonical representative of f_1 respectively f_2 we conclude that there will be exactly one monomial in $G'(X, Y) = F_1(X, Y)F_2(X, Y)$ of highest weight and this highest weight equals $\rho(f_1) + \rho(f_2)$. Substituting in $G'(X, Y)$ repeatedly any occurrences of Y^q with $X^{q+1} - Y$ will as mentioned above eventually give a description $G(X, Y) + I$ of $G'(X, Y) + I$ such that every monomial $X^i Y^j$ in $G(X, Y)$

satisfies $0 \leq i$, $0 \leq j < q$. The crucial observation now is that by induction at any step in this reduction the derived polynomial will have exactly one monomial in its support of highest weight and this weight equals

$$\max\{w(M) \mid M \text{ is in the support of } F_1(X,Y)F_2(X,Y)\} = \rho(f_1) + \rho(f_2).$$

The above observation follows from the fact that the polynomial $X^{q+1} - Y$ replacing Y^q has exactly one monomial in its support of highest weight and from the fact that this weight equals $w(Y^q)$. As a consequence of the above observation we get the nice result $\rho(f_1 f_2) = \rho(f_1) + \rho(f_2)$.

The function $\rho : R \to \langle q, q+1\rangle \cup \{-\infty\}$ described in Example 1 is an instance of a weight function. Keeping this in mind should make it easier to understand the general definition of a weight function. We will need the concept of a well-behaving basis.

Definition 1 *Let k be a field and let R be a k-algebra. Let $\Gamma \subseteq \mathbb{N}_0^r$ be a semigroup and assume $<_{\mathbb{N}_0^r}$ is a term ordering on $\mathbb{N}_0^r$. Given a basis $\mathcal{B}$ for R and a bijective map $\rho : \mathcal{B} \to \Gamma$ we will write $\mathcal{B} = \{f_\lambda \mid \lambda \in \Gamma\}$ (with the underlying assumption that $\rho(f_\lambda) = \lambda$) and for all $\lambda \in \Gamma$ define $R_\lambda = Span_k\{f_\gamma \mid \gamma \leq_{\mathbb{N}_0^r} \lambda\}$. We also define $R_{-\infty} = \{0\}$. The ordered basis $\mathcal{B}$ is called a well-behaving basis if for all $\lambda, \gamma \in \Gamma$ we have $f_\lambda f_\gamma \in R_{\lambda+\gamma}$ but $f_\lambda f_\gamma \notin R_\delta$ for any $\delta <_{\mathbb{N}_0^r} \lambda + \gamma$.*

The basis $\mathcal{B}$ from Example 1 clearly satisfies the conditions of Definition 1 and is therefore a well-behaving basis. Just as was the case in Example 1 the ordered basis from Definition 1 induces a map $\rho : R \to \Gamma \cup \{-\infty\}$. We have

Definition 2 *Let $\mathcal{B} = \{f_\lambda \mid \lambda \in \Gamma\}$ be a well-behaving basis. If $f = 0$ we define $\rho(f) = -\infty$. For nonzero f we consider the expansion $f = \sum_{i=1}^t k_i f_{\lambda_i}$, $k_i \in k\backslash\{0\}$ for $i = 1, \ldots, t$ and $\lambda_i \neq \lambda_j$ for $i \neq j$. We then define $\rho(f) = \max\{\lambda_i \mid i = 1, \ldots, t\}$. A function ρ defined in this way is called a weight function.*

Remark 1 *It is not hard to show that Definition 2 is equivalent to the following characterization. Let $<_{\mathbb{N}_0^r}$ be a term ordering on $\mathbb{N}_0^r$ and let Γ, $\Gamma \subseteq \mathbb{N}_0^r$ be a semigroup. For all $\lambda \in \Gamma$ define $\lambda + (-\infty) = -\infty$. A surjective map $\rho : R \to \Gamma \cup \{-\infty\}$ is called a weight function if for all $f, g, h \in R$ we have*

(W.0) $\rho(f) = -\infty \Leftrightarrow f = 0$

(W.1) $\rho(af) = \rho(f)$ *for all* $a \in k \backslash \{0\}$

(W.2) $\rho(f+g) \leq_{\mathbb{N}_0^r} \max\{\rho(f), \rho(g)\}$

(W.3) $\rho(fg) = \rho(f) + \rho(g)$

(W.4) *If* f *and* g *are nonzero and* $\rho(f) = \rho(g)$ *then there exists a nonzero* $a \in k$ *such that* $\rho(f - ag) <_{\mathbb{N}_0^r} \rho(g)$

Remark 2 *Weight functions are special cases of order functions. The general definition of order functions ([9, Def. 2.1]) calls for the following changes in the characterization in Remark 1. We start by replacing* $(\Gamma \subseteq \mathbb{N}_0^r, <_{\mathbb{N}_0^r})$ *by any well-order* $(\Gamma, <_\Gamma)$*. Then we replace (W.3) with*

$$\textit{(O.3)} \quad \textit{If } \rho(f) <_\Gamma \rho(g) \quad \textit{and} \quad h \neq 0 \quad \textit{then} \quad \rho(fh) <_\Gamma \rho(gh).$$

A k*-algebra with an order function is called an order domain (over* k*).*

Remark 3 *The original definition of an order function in [12, Def. 3.4] is a little less general than the definition in [9]. More precisely it is in [12] required that* $\Gamma \subseteq \mathbb{N}_0$ *and therefore automatically* $<_\Gamma$ *becomes the usual ordering* $<$ *on* $\mathbb{N}_0$*. For a weight function to be an order function under this description one must require that the ordering* $<_{\mathbb{N}_0^r}$ *on* $\mathbb{N}_0^r$ *is isomorphic to the ordering* $<$ *on* $\mathbb{N}_0$*. We will see later in the paper that mapping to* $\mathbb{N}_0^r$ *rather than just to* $\mathbb{N}_0$ *gives us a method for dealing with order domains of transcendence degree more than one.*

In Section 5 we will observe that all order functions relevant in coding theory are actually weight functions. Although Definition 1 and Definition 2 are not very involved they will be general enough to help us construct quite a large class of algebraic geometry codes. The following example describes the algebraic structure needed in the construction of one-point geometric Goppa codes.

Example 2 Let $\mathcal{P}$ be a rational place in an algebraic function field 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 $x \in R$.

The next example describes the algebraic structures needed in the construction of generalized Reed-Muller codes and hyperbolic codes.

Example 3 Let $R = \mathbb{F}_q[X_1, \ldots, X_m]$ and fix any term ordering $<_{\mathbb{N}_0^m}$ on $\mathbb{N}_0^m$. Define a weight function $\rho : R \to \mathbb{N}_0^m \cup \{-\infty\}$ as follows. We have $\rho(0) = -\infty$

and for nonzero $F(X_1, \ldots, X_m)$ we have

$$\rho(F(X_1, \ldots, X_m)) = \max\{(\alpha_1, \ldots, \alpha_m) \mid X_1^{\alpha_1} \cdots X_m^{\alpha_m} \text{ is in the support of } F(X_1, \ldots, X_m)\}.$$

Here max is taken with respect to the ordering $<_{\mathbb{N}_0^m}$.An obvious choice of a well-behaving basis is $\mathcal{B} = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1, \ldots, 0 \leq i_m\}$. For $m \geq 2$ there are infinitely many term orderings on $\mathbb{N}_0^m$ and therefore a polynomial ring in more variables possesses infinitely many weight functions.

The construction of order domains and weight functions in Example 1 and Example 3 was not very involved whereas the construction in Example 2 relies on algebraic function field theory or algebraic geometry. Later in this paper we present a method for constructing order domains and weight functions by use of only simple Gröbner basis theoretical methods. The construction is very similar to the one in Example 1 and deals with any weight function for which the semigroup Γ is finitely generated. The Gröbner basis construction provides us in particular with much more sophisticated examples of order domains of higher transcendence degree than the one in Example 3. However, before continuing our study of order domains we should get involved with the codes. This is done in the next section.

3 Codes from order domains

With a reference to [12, p. 873] by an algebraic geometry code we mean a code that is defined from an algebraic geometry structure by use of some kind of evaluation map[1]. We now consider algebraic geometry codes related to order domains over finite fields $\mathbb{F}_q$. As we will see this set of codes contains in particular one-point geometric Goppa codes. We start by recalling that the component wise product in $\mathbb{F}_q^n$ is given by $(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$. With this product $\mathbb{F}_q^n$ becomes an $\mathbb{F}_q$-algebra. For the code constructions we consider any map φ of the following type.

Definition 3 *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 φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ holds for all $f, g \in R$.*

Example 4 By using the fact that α^{q+1} is the norm map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and by using the fact that $\alpha^q + \alpha$ is the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ the zeros of the Hermitian polynomial $X^{q+1} - Y^q - Y$ can be determined. There are $n = q^3$ of

[1]In recent literature the name geometric Goppa code is often replaced with the name algebraic geometric code. Hence, algebraic geometry codes and algebraic geometric codes are not the same and the word AG-code should be used with caution.

them. Hence, if $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}(X,Y)$ then the variety $\mathcal{V}_{\mathbb{F}_{q^2}}(I)$ consists of q^3 points, say $P_1, \ldots, P_{q^3}$. The evaluation map $\varphi : R = \mathbb{F}_{q^2}[X,Y]/I \to \mathbb{F}_{q^2}^n$ given by $\varphi(F(X,Y)+I) = (F(P_1), \ldots, F(P_{q^3}))$ is a morphism of $\mathbb{F}_{q^2}$-algebras. Recall from the previous section, that $\mathcal{B} = \{X^iY^j + I \mid 0 \leq i, 0 \leq j < q\}$ is a well-behaving basis for the Hermitian order domain. The most natural codes from the Hermitian order domains are the one-point geometric Goppa codes

$$\begin{aligned} E(s) &= \varphi(R_s) = \mathrm{Span}_{\mathbb{F}_{q^2}}\{\varphi(X^iY^j + I) \mid 0 \leq i, 0 \leq j < q, w(X^iY^j) \leq s\} \\ C(s) &= (E(s))^{\perp} \end{aligned}$$

In the remainder of this section let R be an order domain with a weight function $\rho : R \to \Gamma \cup \{-\infty\}$, $\Gamma \subseteq \mathbb{N}_0^r$ and let $\varphi : R \to \mathbb{F}_q^n$ be a morphism between $\mathbb{F}_q$ algebras. Consider the following very general problem. Let $\mathcal{B} = \{f_\lambda \mid \lambda \in \Gamma\}$ be a well-behaving basis and consider a subset $\mathcal{B}' \subseteq \mathcal{B}$. We would like to know what is the minimum distance of $\mathrm{Span}_{\mathbb{F}_q}\{\varphi(f) \mid f \in \mathcal{B}'\}$ and what is the minimum distance of $\left(\mathrm{Span}_{\mathbb{F}_q}\{\varphi(f) \mid f \in \mathcal{B}'\}\right)^{\perp}$. As we shall demonstrate the semigroup Γ holds a lot of information about these questions. The information even suggests clever ways of choosing $\mathcal{B}'$. We start our investigation by stating some useful lemmas and propositions.

Definition 4 *For $\lambda \in \Gamma$ define*

$$N(\lambda) = \{\eta \in \Gamma \mid \exists \beta \in \Gamma \quad \textit{with} \quad \eta + \beta = \lambda\} \quad \textit{and} \quad \mu(\lambda) = \#N(\lambda).$$

Remark 4 *In [12, Def. 4.8] $N(\lambda)$ is defined slightly differently and $\#N(\lambda)$ is called $\nu(\lambda)$. To apply the definition in [12] to the weight functions described in the present paper we must require that the well-order $(\mathbb{N}_0^r, <_{\mathbb{N}_0^r})$ is isomorphic to the well-order $(\mathbb{N}_0, <)$. In other words, for every nonzero $\lambda \in \Gamma$ there exists a maximal element $\gamma \in \Gamma$ for which $\gamma <_{\mathbb{N}_0^r} \lambda$ holds. We then have $\nu(\gamma) = \mu(\lambda)$. The main motivation for using Definition 4 rather than [12, Def. 4.8] is that in this way $N(\lambda)$ and therefore also the size of it becomes independent on the term ordering on $\mathbb{N}_0^r$. Given $r > 1$ and two different term orderings using [12, Def. 4.8] we would have to keep track of two different functions ν.*

Lemma 1 *Given a nonzero word $\vec{c} \in \mathbb{F}_q^n$ let $\lambda \in \Gamma$ be the (unique) element such that $\vec{c} \cdot \varphi(f_\lambda) \neq 0$ but $\vec{c} \cdot \varphi(f_\gamma) = 0$ for all $\gamma <_{\mathbb{N}_0^r} \lambda$. Then $\vec{c} \cdot \varphi(f) \neq 0$ for all f with $\rho(f) = \lambda$ and $\vec{c} \cdot \varphi(f) = 0$ for all f with $\rho(f) <_{\mathbb{N}_0^r} \lambda$.*

Proof: The lemma follows by linearity of φ. □

Proposition 1 *Given a nonzero word $\vec{c} \in \mathbb{F}_q^n$ let λ be as in Lemma 1. The Hamming weight of $\vec{c}$ satisfies $w_H(\vec{c}) \geq \mu(\lambda)$.*

Proof: Let $N(\lambda) = \{i_1, \ldots, i_\mu\}$. By the definition of $N(\lambda)$ for every i_s, $s = 1, \ldots, \mu$ there exists a $j_s \in \Gamma$ with $i_s + j_s = \lambda$. Consider any nonzero linear combination of $f_{i_1}, \ldots, f_{i_\mu}$ over $\mathbb{F}_q$,

$$r = \sum_{s=1}^{\mu} k_s f_{i_s}.$$

Let $t \in \{1, \ldots, \mu\}$ be the maximal value such that $k_t \neq 0$. That is, $\rho(r) = i_t$. From (W.3) in Remark 1 we conclude that $\rho(r f_{j_t}) = \lambda$ and therefore by Lemma 1 $\vec{c} \cdot \varphi(r f_{j_t}) \neq 0$ must hold. Using the fact that φ is a morphism, we get

$$\begin{aligned} \vec{c} \cdot (\varphi(r) * \varphi(f_{j_t})) \neq 0 &\Rightarrow (\vec{c} * \varphi(r)) \cdot \varphi(f_{j_t}) \neq 0 \\ &\Rightarrow \vec{c} * \varphi(r) \neq \vec{0} \\ &\Rightarrow \vec{c} * (\sum_{s=1}^{\mu} k_s \varphi(f_{i_s})) \neq \vec{0}. \end{aligned} \tag{1}$$

Aiming for a contradiction, assume

$$w_H(\vec{c}) < \mu. \tag{2}$$

Without loss of generality we assume that the nonzero entries of $\vec{c}$ are among the first $\mu - 1$ entries. Recall, that the equation (1) holds for any choice of $k_1, \ldots, k_\mu$ not all zero. We will choose $k_1, \ldots, k_\mu$ not all zero in such a way that the first $\mu - 1$ entries of $\sum_{s=1}^{\mu} k_s \varphi(f_{i_s})$ are zero. This is possible due to a standard linear algebra result. But then (1) can not be true and therefore the assumption (2) was wrong. □

To state the next lemma we will need two definitions.

Definition 5 *Let $\alpha(1) = \vec{0}$. For $i = 2, 3, \ldots, n$ recursively define $\alpha(i)$ 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 $\gamma <_{\mathbb{N}_0^r} \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \ldots, \alpha(n)\}$.*

It is clear that the set $\{\varphi(f_{\alpha(1)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. Before proceeding we illustrate the definition with two examples.

Example 5 This is a continuation of Example 4. Recall, that $\mathcal{B} = \{X^i Y^j + I \mid 0 \leq i, 0 \leq j < q\}$ constitutes a well-behaving basis for the Hermitian order domain. Clearly, $\varphi(X^i Y^j + I) = \varphi(X^{i+q^2} Y^j + I)$ and therefore the elements in $\Delta(R, \rho, \varphi)$ need to be of the form $iq + j(q+1)$ with $0 \leq i < q^2$ and $0 \leq j < q$. But there are exactly $n = \dim(\varphi(R)) = q^3$ such numbers and therefore $\Delta(R, \rho, \varphi) = \{iq + j(q+1) \mid 0 \leq i < q^2, 0 \leq j < q\}$.

Example 6 This is a continuation of Example 3 where we considered a family of weight functions on the order domain $R = \mathbb{F}_q[X_1, \ldots, X_m]$. Denote $\{P_1, \ldots, P_{q^m}\} = \mathbb{F}_q^m$ and write $n = q^m$. Define $\varphi : R \to \mathbb{F}_q^n$ by $\varphi(F(X_1, \ldots, X_m)) = (F(P_1), \ldots, F(P_n))$. Recall, that for any of the described weight functions $\mathcal{B} = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1, \ldots, 0 \leq i_m\}$ is a well-behaving basis. Clearly, $\varphi(X_1^{i_1} \cdots X_m^{i_m}) = \varphi(X_1^{i_1+q} \cdots X_m^{i_m}) = \cdots = \varphi(X_1^{i_1} \cdots X_m^{i_m+q})$ and therefore the elements in $\Delta(R, \rho, \varphi)$ need to be of the form $(i_1, \ldots, i_m)$ with $0 \leq i_1 < q, \ldots, 0 \leq i_m < q$. But there are exactly $n = \dim(\varphi(R)) = q^m$ such values and therefore $\Delta(R, \rho, \varphi) = \{(i_1, \ldots, i_m) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q\}$.

Definition 6 *For $\alpha \in \Delta(R, \rho, \varphi)$ let*

$$M(\alpha) = \{\lambda \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Gamma \text{ such that } \alpha + \beta = \lambda\} \text{ and } \sigma(\alpha) = \#M(\alpha).$$

Proposition 2 *Let $\{\alpha(1), \ldots, \alpha(n)\}$ be as in Definition 5. Given a nonzero word $\vec{c}$ expand it as follows*

$$\vec{c} = \sum_{s=1}^{n} k_s \varphi(f_{\alpha(s)}), \quad k_1, \ldots, k_n \in \mathbb{F}_q.$$

Let t be the maximal value such that k_t is nonzero. The Hamming weight of $\vec{c}$ satisfies $w_H(\vec{c}) \geq \sigma(\alpha(t))$.

Proof: Write $\sigma(\alpha(t)) = \sigma$, $M(\alpha(t)) = \{\lambda_1, \ldots, \lambda_\sigma\}$ and let $\beta_1, \ldots, \beta_\sigma$ be such that $\alpha(t) + \beta_1 = \lambda_1, \ldots, \alpha(t) + \beta_\sigma = \lambda_\sigma$. Writing $f = \sum_{s=1}^{t} k_s f_{\alpha(s)}$ we get $\vec{c} = \varphi(f)$. Now by assumption k_t is nonzero but $k_s = 0$ for $t < s$ and therefore $\rho(f) = \alpha(t)$ follows. We get $\rho(f f_{\beta_1}) = \lambda_1, \ldots, \rho(f f_{\beta_\sigma}) = \lambda_\sigma$. But then from the definition of $\Delta(R, \rho, \varphi)$ we conclude that $\varphi(f f_{\beta_1}), \ldots, \varphi(f f_{\beta_\sigma})$ are linearly independent. In other words $\vec{c} * \varphi(f_{\beta_1}), \ldots, \vec{c} * \varphi(f_{\beta_\sigma})$ are linearly independent. However, the vector space $\{\vec{b} \mid \text{ there exists an } \vec{a} \text{ such that } \vec{b} = \vec{c} * \vec{a}\}$ is clearly of dimension exactly $w_H(\vec{c})$ and therefore $\sigma \leq w_H(\vec{c})$ must hold.
□

With Proposition 1 and Proposition 2 in hand we are now able to deal with some very large classes of codes. We start by stating a very general theorem.

Theorem 1 *Given numbers $i_1, \ldots, i_t$ with $1 \leq i_1 < \cdots < i_t \leq n$ consider the corresponding elements $f_{\alpha(i_1)}, \ldots, f_{\alpha(i_t)} \in \mathcal{B}$. The code*

$$Span_{\mathbb{F}_q}\{\varphi(f_{\alpha(i_1)}), \ldots, \varphi(f_{\alpha(i_t)})\}$$

is of dimension t and has minimum distance at least

$$\min\{\sigma(\alpha(i_s)) \mid s = 1, \ldots, t\}.$$

The dual code is of dimension $n-t$ and has minimum distance at least

$$\begin{aligned} & \min\{\mu(\alpha(i)) \mid i \in \{1,\ldots,n\}\backslash\{i_1,\ldots,i_t\}\} & (3)\\ \geq\ & \min\{\mu(\lambda) \mid \lambda \in \Gamma\backslash\{\alpha(i_1),\ldots,\alpha(i_t)\}\}. & (4)\end{aligned}$$

Proof: The result concerning the first code follows immediately from Proposition 2. Concerning the dual code we observe that since $\{\varphi(f_{\alpha(1)}),\ldots,\varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$, a nonzero word $\vec{c}$ will have to satisfy $\vec{c}\cdot\varphi(f_\alpha)\neq 0$ for some $\alpha\in\Delta(R,\rho,\varphi)$. Combining Lemma 1 with the definition of $\Delta(R,\rho,\varphi)$ we see that the smallest value $\lambda\in\Gamma$ such that $\vec{c}\cdot\varphi(f_\lambda)\neq 0$ is an element in $\Delta(R,\rho,\varphi)$. But by construction of the dual code $\vec{c}\cdot\varphi(f_{\alpha(i_1)})=\cdots=\vec{c}\cdot\varphi(f_{\alpha(i_t)})=0$ holds. Hence, the smallest possible $\lambda\in\Gamma$ such that $\vec{c}\cdot\varphi(f_\lambda)\neq 0$ must be contained in $\Delta(R,\rho,\varphi)\backslash\{\alpha(i_1),\ldots,\alpha(i_t)\}$. The estimate (3) of the minimum distance of the dual code now follows immediately from Proposition 1. The number in (3) clearly is larger than or equal to the number in (4). □

The estimates (3) and (4) of the minimum distance of the dual code are known as the order bound. They are instance of the Feng-Rao bound. Consider the following particular classes of codes.

Definition 7

$$\begin{aligned} E(\lambda) &= \varphi(R_\lambda) = \mathit{Span}_{\mathbb{F}_q}\{\varphi(f_\gamma) \mid \gamma \leq_{\mathbb{N}_0^r} \lambda\}\\ \tilde{E}_\varphi(s) &= \mathit{Span}_{\mathbb{F}_q}\{\varphi(f_\lambda) \mid \lambda\in\Delta(R,\rho,\varphi) \ \ \mathit{and}\ \ \sigma(\lambda)\geq s\}\\ C(\lambda) &= (E(\lambda))^\perp = \{\vec{c}\in\mathbb{F}_q^n \mid \vec{c}\cdot\varphi(f_\gamma)=0 \ \ \mathit{for\ all}\ \ \gamma\leq_{\mathbb{N}_0^r}\lambda\}\\ \tilde{C}(s) &= \{\vec{c}\in\mathbb{F}_q^n \mid \vec{c}\cdot\varphi(f_\gamma)=0 \ \ \mathit{for\ all}\ \ \gamma \ \ \mathit{with}\ \ \mu(\gamma)<s\}\\ \tilde{C}_\varphi(s) &= \{\vec{c}\in\mathbb{F}_q^n \mid \vec{c}\cdot\varphi(f_\gamma)=0 \ \ \mathit{for\ all}\ \ \gamma\in\Delta(R,\rho,\varphi) \ \ \mathit{with}\ \ \mu(\gamma)<s\}\end{aligned}$$

Note that the codes in Example 4 were of the type $E(\lambda)$ and $C(\lambda)$. In larger generality we see from Example 2 that one-point geometric Goppa codes $C_{\mathcal{L}}(D,m\mathcal{P})$ are codes $E(\lambda)$ from order domains with a numerical semigroup. Similarly one-point geometric Goppa codes $C_\Omega(D,m\mathcal{P})$ are codes $C(\lambda)$ from order domains with a numerical semigroup. The codes $\tilde{E}_\varphi(s)$, $\tilde{C}(s)$ and $\tilde{C}_\varphi(s)$ are said to be improved codes. This name is justified by the following theorem.

Theorem 2 *We have*

$$\begin{aligned} E(\lambda) &= \mathit{Span}_{\mathbb{F}_q}\{\varphi(f_\gamma) \mid \gamma\in\Delta(R,\rho,\varphi) \ \ \mathit{and}\ \ \gamma\leq_{\mathbb{N}_0^r}\lambda\}\\ C(\lambda) &= \{\vec{c}\in\mathbb{F}_q^n \mid \vec{c}\cdot\varphi(f_\gamma)=0 \ \ \mathit{for\ all}\ \ \gamma\in\Delta(R,\rho,\varphi) \ \ \mathit{with}\ \ \gamma\leq_{\mathbb{N}_0^r}\lambda\}\end{aligned}$$

The minimum distances of the codes in Definition 7 satisfy

$$\begin{aligned} d\left(E(\lambda)\right) &\geq \min\{\sigma(\gamma) \mid \gamma \in \Delta(R,\rho,\varphi) \quad \textit{and} \quad \gamma \leq_{\mathbb{N}_0^r} \lambda\} && (5)\\ d\left(\tilde{E}_\varphi(s)\right) &\geq s \\ d\left(C(\lambda)\right) &\geq \min\{\mu(\eta) \mid \eta \in \Delta(R,\rho,\varphi), \lambda <_{\mathbb{N}_0^r} \eta\} && (6)\\ &\geq \min\{\mu(\eta) \mid \eta \in \Gamma, \lambda <_{\mathbb{N}_0^r} \eta\} && (7)\\ d\left(\tilde{C}(s)\right) &\geq s \\ d\left(\tilde{C}_\varphi(s)\right) &\geq s \end{aligned}$$

Proof: The description of $E(\lambda)$ and $C(\lambda)$ is an immediate consequence of the definition of $\Delta(R,\rho,\varphi)$. The estimates of the minimum distances of all codes but $\tilde{C}(s)$ follow from Theorem 1. Finally, $\tilde{C}(s) \subseteq \tilde{C}_\varphi(s)$ and therefore $d(\tilde{C}(s)) \geq d(\tilde{C}_\varphi(s))$ holds. □

To illustrate the theorem we consider two examples.

Example 7 This is a continuation of Example 5. Consider the Hermitian polynomial $X^4 - Y^3 - Y$ over $\mathbb{F}_9$. The set $\Delta(R,\rho,\varphi) = \{\alpha(1),\ldots,\alpha(27)\}$ was established in Example 5. We now list the corresponding values of $\mu(\alpha(i))$ and $\sigma(\alpha(i))$.

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

i	10	11	12	13	14	15	16	17	18
$\alpha(i)$	12	13	14	15	16	17	18	19	20
$\mu(\alpha(i))$	7	8	9	10	11	12	13	14	15
$\sigma(\alpha(i))$	15	14	13	12	11	10	9	8	7

i	19	20	21	22	23	24	25	26	27
$\alpha(i)$	21	22	23	24	25	26	28	29	32
$\mu(\alpha(i))$	16	17	18	19	20	21	23	24	27
$\sigma(\alpha(i))$	6	6	4	3	4	3	2	2	1

For $i = 1,\ldots,19$ $\sigma(\alpha(i)) = n - \alpha(i)$ and therefore for $i = 1,\ldots,19$ the code $E(\alpha(i))$ has minimum distance at least $n - \alpha(i) = 27 - \alpha(i)$ and dimension $k = i$. For larger values of i the picture is a little more complicated. For instance the minimum distance of $E(22)$ is at least 6. The minimum distances of $E(24)$, $E(25)$ and $E(26)$ are all estimated to 3. The corresponding dimensions

are $k = 22, 23, 24$. The code $\tilde{E}_\varphi(4)$ however has minimum distance at least 4 and dimension $k = 22$. For $i = 8, \ldots, 23$ $\min\{\mu(\alpha(s)) \mid i < s\} = i-2$ and therefore for $i = 8, \ldots, 23$ the code $C(\alpha(i))$ has minimum distance at least $i-2$ and dimension $k = 27 - i$. For smaller or larger values of i the picture is a little more complicated. For instance the minimum distance of $C(4)$, $C(6)$ and $C(7)$ are estimated by 3. The corresponding dimensions are $k = 24, 23, 22$. The code $\tilde{C}_\varphi(4)$ however has minimum distance at least 4 and dimension 22. The codes $C(26)$, $C(28)$ and $C(29)$ have minimum distances at least 23, 24 respectively 27. In this example we considered the particular case $q^2 = 9$. The general case where q^2 is arbitrary is treated in [6]. It is shown that all estimates on the minimum distances are tight. The class of codes $E(\lambda)$ equals the class of codes $C(\lambda)$. Similarly, the class of codes $\tilde{E}_\varphi(s)$ equals the class of codes $\tilde{C}_\varphi(s)$.

Example 8 This is a continuation of Example 3 and Example 6. Consider the polynomial ring $\mathbb{F}_5[X, Y]$. For any of the described weight functions the values of $\Delta(R, \rho, \varphi)$ are

$$\begin{array}{ccccc} (0,4) & (1,4) & (2,4) & (3,4) & (4,4) \\ (0,3) & (1,3) & (2,3) & (3,3) & (4,3) \\ (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \\ (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\ (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \end{array}$$

with corresponding σ-values respectively μ-values

$$\begin{array}{ccccc} 5 & 4 & 3 & 2 & 1 \\ 10 & 8 & 6 & 4 & 2 \\ 15 & 12 & 9 & 6 & 3 \\ 20 & 16 & 12 & 8 & 4 \\ 25 & 20 & 15 & 10 & 5 \end{array} \quad \text{respectively} \quad \begin{array}{ccccc} 5 & 10 & 15 & 20 & 25 \\ 4 & 8 & 12 & 16 & 20 \\ 3 & 6 & 9 & 12 & 15 \\ 2 & 4 & 6 & 8 & 10 \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

To choose a particular weight function among the ones described in Example 3 we need to fix the term ordering $<_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$. Let the term ordering $<_{\mathbb{N}_0^2}$ be the graded lexicographic ordering given by $(a, b) <_{\mathbb{N}_0^2} (c, d)$ if either $a + b < c + d$ holds or $a + b = c + d$ holds with $b < d$. The generalized Reed-Muller code

$$\mathrm{RM}_5(s, 2) = \{\varphi(F(X, Y)) \mid \deg(F) \leq s\}$$

is then seen to be equal to $E((0, s))$. By the first part of Theorem 2 we see that

$$E((0, s)) \;=\; \mathrm{Span}_{\mathbb{F}_5}\{\varphi(X^i Y^j) \mid 0 \leq i < 5, 0 \leq j < 5, i + j \leq s\}.$$

We list the performance of a few of the codes. We have $d(\tilde{E}_\varphi(5)) \geq 5$ and $k(\tilde{E}_\varphi(5)) = 17$ whereas $d(E((0, 4))) \geq 5$ and $k(E((0, 4))) = 15$. We have $d(\tilde{E}_\varphi(4)) \geq 4$ and $k(\tilde{E}_\varphi(4)) = 20$ whereas $d(E((0, 5))) \geq 4$ and $k(E((0, 5))) = 19$. The study of μ gives a similar picture of the codes $C(\lambda)$ and $\tilde{C}_\varphi(s)$. In this example we considered the particular case $\mathbb{F}_5[X, Y]$. The general case $\mathbb{F}_q[X_1, \ldots, X_m]$

was treated in [7]. It is shown that the estimates on the minimum distances are always tight. The class of codes $E(\lambda)$ equals the class of codes $C(\lambda)$. Similarly, the class of codes $\tilde{E}_\varphi(s)$ equals the class of codes $\tilde{C}_\varphi(s)$. The improved codes coming from the order domain $\mathbb{F}_q[X_1, \ldots, X_m]$ are known as hyperbolic codes or Massey-Costello-Justesen codes.

The above example illustrates the fact that using weights in $\mathbb{N}_0^r$ with $r > 1$ one can often construct rather long and still relatively good codes in a very simple way. We will see one more example of this in Section 5. We note without a proof that it is possible to make asymptotic good concatenated codes that beats the performance of the Justesen codes for small rates by using as outer codes hyperbolic codes instead of Reed-Solomon codes.
We conclude the section by mentioning briefly some other interesting results from the literature. First we note that the bounds in Theorem 1 and Theorem 2 can be easily extended to deal not only with the minimum distance but with any generalized Hamming weight. Details can be found in [11], [10] and [2]. Next we note that a modification of the order bound was made in [3] to make the bound applicable to general geometric Goppa codes. Another result we would like to mention is that it is possible to modify Sudan's list decoding without multiplicity so that it works for any evaluation code from order domain theory. Details can be found in [8]. Finally, we note that there exists another improved code construction besides the ones described here, namely the improved generic evaluation codes. They were introduced in [4] and allow for correction of so-called generic errors of high weight. The minimum distances of these codes however are not in general very high. In the next section we relate the bounds in Theorem 2 to the usual bounds from algebraic geometry on codes defined from curves.

4 One-point geometric Goppa codes

In this section we treat weight functions with a numerical semigroup. We will always assume that $\mathbb{N}_0 \backslash \Gamma$ is finite which is not really a restriction as any numerical semigroup will be isomorphic to a (unique) numerical semigroup such that the requirement holds. We observed in Example 2 that if $\mathcal{P}$ is a rational place in an algebraic function field of one variable and $v_\mathcal{P}$ is the corresponding valuation then $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ is an order domain with a weight function given by $\rho(x) = -v_\mathcal{P}(x)$. Clearly, any subring of such an order domain will again be an order domain and if the subring is non trivial then the corresponding semigroup $\Gamma \subseteq \mathbb{N}_0$ will be non trivial. It is an obvious question if there are other examples of order domains with numerical weight functions than the ones coming from $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$. This question was settled in [14, Th. 1]. The answer is no. Hence, if we restrict to algebraic structures over $\mathbb{F}_q$ then what we are discussing in the present section are nothing but the algebraic structures giving us one-point geometric Goppa codes. Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ be pairwise different rational places

not equal to $\mathcal{P}$. Then the map $\varphi : \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P}) \to \mathbb{F}_q^n$ is clearly a surjective morphism between $\mathbb{F}_q$-algebras and therefore one-point geometric Goppa codes $C_{\mathcal{L}}(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, s\mathcal{P})$ respectively $C_{\Omega}(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, s\mathcal{P})$ are codes of the form $E(s)$ respectively $C(s)$ coming from order domains with a weight function with a numerical semigroup. As we shall see we will be able to establish the usual bounds from algebraic geometry on their minimum distances using only a little effort.

We start by introducing some notation. Write $\Gamma = \{\lambda_1 = 0, \lambda_2, \ldots\}$ where $\lambda_i < \lambda_{i+1}$ for $i = 1, 2, \ldots$. We define $g(i) = \#\{\lambda \in \mathbb{N}_0 \backslash \Gamma \mid \lambda < \lambda_i\}$ and $g = \#\mathbb{N}_0 \backslash \Gamma$. According to the discussion above Γ is the Weirstrass semigroup of a rational place and therefore by the Weirstrass Gap Theorem g equals the genus of the function field under consideration. The following results from [12, Lem. 5.15 and Th. 5.24] are easily proven.

Lemma 2 *For any $i \in \mathbb{N}_0$ we have $\Gamma \backslash (\lambda_i + \Gamma) = \lambda_i$ and $\mu(\lambda_i) = i - g(i) + \#D(i)$ where $D(i) = \{(x, y) \mid x, y \in \mathbb{N}_0 \backslash \Gamma \quad and \quad x + y = \lambda_i\}$.*

Applied to the special case of one-point geometric Goppa codes the Goppa bounds from algebraic geometry states.

Theorem 3 *Assume Γ is numerical with $\mathbb{N}_0 \backslash \Gamma$ finite. We have*

$$d(E(s)) \geq n - s \tag{8}$$
$$d(C(\lambda_t)) \geq t + 1 - g \tag{9}$$

The usual proof of the Goppa bounds requires the use of the Riemann-Roch theorem. However, in the case of one-point geometric Goppa codes order domain theory provides an alternative proof by combining Theorem 2 and Lemma 2.

Theorem 4 *Assume Γ is numerical with $\mathbb{N}_0 \backslash \Gamma$ finite. The bound in (5) is at least as good as the bound (8) and sometimes better. The bound in (7) is at least as good as the bound (9) and sometimes better.*

Proof: To prove the first claim we need only consider numbers $i \in \Delta(R, \rho, \varphi)$ with $i \leq s$. We have $\sigma(i) = \#(\Delta(R, \rho, \varphi) \cap (i + \Gamma))$. By Lemma 2 the number of elements in $\Delta(R, \rho, \varphi)$ that are not in $i + \Gamma$ is at most i and therefore $\sigma(i) \geq n - i$ holds. Equality holds only when $\Gamma \backslash (i + \Gamma) \subseteq \Delta(R, \rho, \varphi)$. We conclude $\min\{\sigma(i) \mid i \in \Delta(R, \rho, \varphi), i \leq s\} \geq n - s$. Concerning the last claim we have

$$\min\{\mu(\eta) \mid \eta \in \Gamma \quad \text{and} \quad \lambda_t < \eta\} = \min\{i - g(i) + \#D(i) \mid t < i\} \geq t + 1 - g$$

with equality if and only if $\lambda_{t+1} = \lambda_t + 1$, $g(t + 1) = g$ and $\#D(t + 1) = 0$ holds. $\square$

5 Gröbner basis theoretical tools for the construction of order domains

In this section we will see how to construct order domains by use of only simple Gröbner basis theoretical tools. The method to be described can be viewed as a generalization of the Hermitian order domain construction from Example 1. We start by recalling some basic facts from Gröbner basis theory. In the following let k be any field.

Definition 8 *Denote by $\mathcal{M}(X_1, \ldots, X_m)$ the set of monomials in $X_1, \ldots, X_m$. Given a term ordering $<_{\mathcal{M}}$ on $\mathcal{M}(X_1, \ldots, X_m)$ and an ideal $I \subseteq k[X_1, \ldots, X_m]$ the footprint (or the Gröbner éscalier) of I is the set*

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

Theorem 5 *Let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal. Then $\{M + I \mid M \in \Delta_{<_{\mathcal{M}}}(I)\}$ is a basis for $k[X_1, \ldots, X_m]/I$ as a vector space over k.*

Example 9 This is a continuation of Example 1 where we considered the Hermitian order domain $R = \mathbb{F}_{q^2}[X, Y]/I$, with $I = \langle X^{q+1} - Y^q - Y \rangle$. Let a weighted degree lexicographic ordering $<_w$ on $\mathcal{M}(X, Y)$ be given as follows. We have $X^\alpha Y^\beta <_w X^\gamma Y^\delta$ if either $\alpha q + \beta(q+1) < \gamma q + \delta(q+1)$ holds or $\alpha q + \beta(q+1) = \gamma q + \delta(q+1)$ but $\beta < \delta$ holds. Clearly, $\Delta_{<_w}(I) = \{X^i Y^j \mid 0 \leq i, 0 \leq j < q\}$ and therefore by Theorem 5 $\mathcal{B} = \{X^i Y^j + I \mid 0 \leq i, 0 \leq j < q\}$ is a basis for R.

For the construction of order domains we will need generalized weighted degree orderings. These are defined as follows

Definition 9 *Given weights $w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^r \backslash \{\vec{0}\}$ let $\mathbb{N}_0^r$ be ordered by some fixed term ordering $<_{\mathbb{N}_0^r}$. Let $<_{\mathcal{M}}$ be a fixed term ordering on $\mathcal{M}(X_1, \ldots, X_m)$. The weights extend to a monomial function $w : \mathcal{M}(X_1, \ldots, X_m) \to \mathbb{N}_0^r$ by $w(X_1^{\alpha_1} \cdots X_m^{\alpha_m}) = \sum_{i=1}^m \alpha_i w(X_i)$. For a monomial M we call $w(M)$ the weight of M. Now the generalized weighted degree ordering $<_w$ induced by w, $<_{\mathbb{N}_0^r}$ and $<_{\mathcal{M}}$ is the term ordering defined as follows. Given $M_1, M_2 \in \mathcal{M}(X_1, \ldots, X_m)$ then $M_1 <_w M_2$ if and only if one of the following two conditions holds*

(GWD.1) $w(M_1) <_{\mathbb{N}_0^r} w(M_2)$

(GWD.2) $w(M_1) = w(M_2)$ *and* $M_1 <_{\mathcal{M}} M_2$.

We observe, that if the weights are numerical then we do not need to define the ordering $<_{\mathbb{N}_0^{r=1}}$ as there exists only one term ordering on $\mathbb{N}_0$. In this case the generalized weighted degree ordering simplifies to the usual weighted degree ordering. We can now describe the main result of this section.

Theorem 6 *Let I be an ideal in $k[X_1, \ldots, X_m]$ and assume $\mathcal{G}$ is a Gröbner basis for I with respect to a generalized weighted degree ordering $<_w$. Suppose that the elements of the corresponding footprint $\Delta_{<_w}(I)$ have mutually distinct weights and that every element of $\mathcal{G}$ has exactly two monomials of highest weight in its support. Write $\Gamma = \{w(M) \mid M \in \Delta_{<_w}(I)\} \subseteq \mathbb{N}_0^r$. For $f \in k[X_1, \ldots, X_m]/I$ denote by F the (unique) remainder of any polynomial in f after division with $\mathcal{G}$. Then $R = k[X_1, \ldots, X_m]/I$ is an order domain with a weight function $\rho : R \to \Gamma \cup \{-\infty\}$ defined by $\rho(0) = -\infty$ and $\rho(f) = \max_{<_{\mathbb{N}_0^r}}\{w(M) \mid M \in Supp(F)\}$ for $f \neq 0$.*

Proof: Theorem 5 tells us that $\mathcal{B} = \{M + I \mid M \in \Delta_{<_w}(I)\}$ is a basis for R as a vector space over k. For $f \in \mathcal{B}$ let $F \in \Delta_{<_w}(I)$ be the unique monomial such that $f = F + I$. The map $\rho : \mathcal{B} \to \Gamma$ given by $\rho(f) = w(F)$ is well-defined and by assumption it is bijective. If we can show that $\mathcal{B} = \{f_\lambda \mid \lambda \in \Gamma\}$ is a well-behaving basis then from Definition 2 it follows that a weight function is given just as described in the theorem above. For $\gamma \in \Gamma$ we denote by f_γ the element in $\mathcal{B}$ with $\rho(f_\gamma) = \gamma$ and write $f_\gamma = F_\gamma + I$ where $F_\gamma \in \Delta_{<_w}(I)$. It follows by the definition of ρ that $w(F_\gamma) = \gamma$ holds. Recall from Definition 1, that $R_{-\infty} = \{0\}$ and that for $\lambda \in \Gamma$ we define $R_\lambda = \mathrm{Span}_k\{f_\gamma \mid \gamma \leq_{\mathbb{N}_0^r} \lambda\}$. We must show that if $\alpha, \beta \in \Gamma$ then $f_\alpha f_\beta \in R_{\alpha+\beta}$ but $f_\alpha f_\beta \notin R_\delta$ for any δ with $\delta <_{\mathbb{N}_0^r} \alpha + \beta$. By the definition of ρ this corresponds to showing that if $f_\alpha f_\beta$ is written as

$$\sum_{\eta \in \Gamma, k_\eta \in k} k_\eta F_\eta + I$$

then

$$\max_{<_{\mathbb{N}_0^r}}\{w(M) \mid M \text{ is in the support of } \sum_{\eta \in \Gamma, k_\eta \in k} k_\eta F_\eta\} = \alpha + \beta$$

holds. Multiplying $f_\alpha = F_\alpha + I$ with $f_\beta = F_\beta + I$ we get $F_\alpha F_\beta + I$. Clearly, $F_\alpha F_\beta$ is a monomial but it need not be an element in $\Delta_{<_w}(I)$. To find

$$\sum_{\eta \in \Gamma, k_\eta \in k} k_\eta F_\eta$$

we reduce $F_\alpha F_\beta$ modulo $\mathcal{G}$. At every stage of this reduction by induction the derived polynomial will have exactly one monomial of highest weight in its support and the weight of this monomial equals $w(F_\alpha F_\beta) = \alpha + \beta$. □

Example 10 This is a continuation of Example 1 and Example 9 where we considered the Hermitian order domain. Clearly, $\mathcal{G} = \{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for I with respect to $<_w$. We have $w(X^{q+1}) = w(Y^q) = q(q+1) > w(Y) = q$ and therefore all polynomials in $\mathcal{G}$ contains exactly two monomials of highest weight. It is easily verified that no two different monomials in $\Delta_{<_w}(I)$ are of the same weight and therefore all the conditions in Theorem 6 are satisfied.

Example 11 This is a continuation of Example 3 where we considered a family of weight functions on the order domain $R = k[X_1, \ldots, X_m]$. Using the convention that $\mathcal{G} = \emptyset$ is a Gröbner basis for the ideal $\langle 0 \rangle$ the description in Example 3 can be viewed as an instance of Theorem 6.

Theorem 6 actually captures all order domains relevant in coding theory including the spaces $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ used in the construction of one-point geometric Goppa codes (Example 2 and Section 4). This not too obvious result is the content of [9, Th. 10.4]. To explain precisely what [9, Th. 10.4] is saying we consider the general definition of an order function in Remark 2. We observe that although the well-order $(\Gamma, <_\Gamma)$ is not born with a binary operation the order function induces one. More precisely, one can define an operation $\oplus$ on Γ by the rule $\rho(f) \oplus \rho(g) = \rho(fg)$. Denoting by 0 the minimal element of Γ, $(\Gamma, \oplus, 0)$ becomes a semigroup. Now [9, Th. 10.4] deals with the case where an order domain and an order function is given for which the semigroup $(\Gamma, \oplus, 0)$ is finitely generated. Under this condition the following three things hold. Firstly, $(\Gamma, \oplus, 0)$ is isomorphic to a sub semigroup of $\mathbb{N}_0^r$ for some r. Secondly, under the isomorphism $<_\Gamma$ is the restriction of a term ordering on $\mathbb{N}_0^r$ to Γ. Finally and most importantly, up to isomorphism the order domain and the order function can be described as in Theorem 6. In particular if an order function ρ has a finitely generated semigroup $(\Gamma, \oplus, 0)$ then ρ is isomorphic to a weight function. Furthermore, [9, Th. 11.9] states that if the transcendence degree of R is r and $(\Gamma, \oplus, 0)$ is finitely generated then it is possible to embed $(\Gamma, \oplus, 0)$ into $(\mathbb{N}_0^r, +, 0)$ but impossible to embed it into $(\mathbb{N}_0^{r-1}, +, 0)$. We next observe that every numerical semigroup is finitely generated and therefore in theory the algebraic structure $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ used in the construction of one-point geometric Goppa codes can be described as in Theorem 6. Unfortunately, no general method has been developed that put order domains $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ on the form as in Theorem 6. Any development in this direction would be of great importance to order domain theory. One main advantage of Theorem 6 is that it allows us to construct in a very easy way order domains of higher transcendence degree. We now give such an example.

Example 12 Let

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

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

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 $<_w$ 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 $<_{\mathbb{N}_0^2}$ be any fixed term ordering on $\mathbb{N}_0^2$ that satisfies

(q^2,q), (q,q^2), $(0,q^2+q) <_{\mathbb{N}_0^2} (q^2+q,0)$ and $(q,q^2) <_{\mathbb{N}_0^2} (q^2,q)$. Finally let $<_{\mathcal{M}}$ be any fixed term ordering on $\mathcal{M}(X,Y,Z,U)$ that satisfies $YZ^q <_{\mathcal{M}} X^q$ and $Z^{q+1} <_{\mathcal{M}} U^q$. 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 6 are satisfied. From Theorem 6 we get a weight function

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

The particular choice of terms not of highest weight in H_1 and H_2 will be important in a later example where we derive codes from the above order domain.

Consider any finitely generated semigroup $\Gamma = \langle \lambda_1, \ldots, \lambda_m \rangle \subseteq \mathbb{N}_0^r$ and a term ordering $<_{\mathbb{N}_0^r}$. Let an ordering $<_w$ on $\mathcal{M}(X_1,\ldots,X_m)$ be defined by $w(X_1) = \lambda_1, \ldots, w(X_m) = \lambda_m$ and some term ordering $<_{\mathcal{M}}$. The ideal

$$\begin{aligned} I_\Gamma &= \langle M - N \mid M,N \in \mathcal{M}(X_1,\ldots,X_m),\, w(M) = w(N)\rangle \\ &\subseteq k[X_1,\ldots,X_m] \end{aligned} \tag{10}$$

is called a toric ideal. I_Γ has a Gröbner basis with respect to $<_w$ that consists of a collection of binomials of the form from (10). In fact, the Gröbner basis can be found by use of elimination theory (see [9, Pro. 10.6].) By (10) no two different monomials of the same weight can be simultaneously members of $\Delta_{<_w}(I_\Gamma)$ and therefore the conditions in Theorem 6 are satisfied. That is, we have a weight function

$$\rho : R_\Gamma = k[X_1,\ldots,X_m]/I_\Gamma \to \Gamma \cup \{-\infty\}.$$

This sort of a trivial order domain plays a special role in order domain theory. Namely, it was shown in [13] that the conditions in Theorem 6 regarding the defining polynomials of a k-algebra $R = k[X_1,\ldots,X_m]/I$ and a semigroup $\Gamma \subseteq \mathbb{N}_0^r$ are equivalent to saying that R has a flat deformation to R_Γ. This result has proved very useful. As an example it is used in [13, Sec. 6] in combination with some results on deformation of Grassmannians to derive weight functions on all Grassmannians.

6 Gröbner basis theoretical tools for the code construction

In this section we shall see that not only is Gröbner basis theory an important tool for the construction of order domains - it is also an important tool for the construction of the corresponding codes. Recall, that for the code construction we need an order domain R over $\mathbb{F}_q$ and a surjective $\mathbb{F}_q$-linear map $\varphi : R \to \mathbb{F}_q^n$

satisfying $\varphi(fg) = \varphi(f) * \varphi(g)$. Recall, that such a map is called a morphism between $\mathbb{F}_q$-algebras. Given an order domain $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ as in Theorem 6 the most obvious choice of φ would be $\varphi(F + I) = (F(P_1), \ldots, F(P_n))$ where $\{P_1, \ldots, P_n\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$. Here, $\mathcal{V}_{\mathbb{F}_q}(I)$ denotes the variety of I. Theorem 7 tells us that there are no maps beside this that have the desired properties.

Theorem 7 *Let $\varphi : \mathbb{F}_q[X_1, \ldots, X_m]/I \to \mathbb{F}_q^n$ be a surjective $\mathbb{F}_q$-linear map satisfying $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in \mathbb{F}_q[X_1, \ldots, X_m]/I$. Then there exists a set $\{P_1, \ldots, P_n\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$, $P_i \neq P_j$ for $i \neq j$ such that $\varphi(F(X_1, \ldots, X_m) + I) = (F(P_1), \ldots, F(P_n))$ holds for all $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$.*

Proof: We will use the notation $\varphi(f) = (\varphi_1(f), \ldots, \varphi_n(f))$. The assumption that φ is surjective implies that $\varphi_i : \mathbb{F}_q[X_1, \ldots, X_m]/I \to \mathbb{F}_q$, $i = 1, \ldots, n$ are pairwise different surjective maps. The remaining assumptions imply that $\varphi_i : \mathbb{F}_q[X_1, \ldots, X_m]/I \to \mathbb{F}_q$ is a ring homomorphism with $\varphi_i(c + I) = c$ for all $c \in \mathbb{F}_q$. Writing $x_1 = X_1 + I, \ldots, x_m = X_m + I$ and identifying $c + I$ with c for all $c \in \mathbb{F}_q$ we get $F(X_1, \ldots, X_m) + I = F(x_1, \ldots, x_m)$. This is nothing but the usual way of doing arithmetic on residue classes. Now let $P_i^{(1)} = \varphi_i(x_1), \ldots, P_i^{(m)} = \varphi_i(x_m) \in \mathbb{F}_q$. The fact that φ_i is a ring homomorphism with $\varphi_i(c + I) = c$ for all $c \in \mathbb{F}_q$ now implies that $\varphi_i(F(x_1, \ldots, x_m)) = F(P_i^{(1)}, \ldots, P_i^{(m)})$ holds. That is, $\varphi_i(F(X_1, \ldots, X_m) + I) = F(P_i^{(1)}, \ldots, P_i^{(m)})$. For every $F(X_1, \ldots, X_m) \in I$ we have $\varphi_i(F(x_1, \ldots, x_m)) = \varphi_i(0 + I) = 0$ and therefore $P_i = (P_i^{(1)}, \ldots, P_i^{(n)})$ is a zero of $F(X_1, \ldots, X_m)$. In other words $P_i \in \mathcal{V}_{\mathbb{F}_q}(I)$. □

In conclusion we see that a very large class of algebraic geometry codes including one-point geometric Goppa codes can be described by use of only simple Gröbner basis theoretical tools. Unfortunately, given a general order domain R then it is not at all obvious how to derive the description in Theorem 6. However, it is still possible to apply the simple Gröbner basis theoretical tools when dealing with the codes at a theoretical level. As an example we note that one can reprove the result in Section 4 regarding the minimum distance of the codes $E(\lambda)$ and $\tilde{E}_\varphi(s)$ in a pure Gröbner basis theoretical setting.
The remainder of the present section is about the case where a description as in Theorem 6 is known. As we are normally interested in large codes we concentrate mostly on the case where φ is defined by evaluating in all the points of the variety $\mathcal{V}_{\mathbb{F}_q}(I)$. Recall, that for the actual code construction we would like to know for which $\lambda \in \Gamma$ we have $\varphi(R_\lambda) \neq \varphi(R_\gamma)$ for all $\gamma <_{\mathbb{N}_0^r} \lambda$. The set of such λs was denoted $\Delta(R, \rho, \varphi)$ in Section 3. The following not too surprising theorem explains the choice of notation.

Theorem 8 *Consider an order domain R and a weight function $\rho : R \to \Gamma \cup \{-\infty\}$ described as in Theorem 6. Let φ be the morphism $\varphi : R \to \mathbb{F}_q^n$ given by $\varphi(F + I) = (F(P_1), \ldots, F(P_n))$ where $\mathcal{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$, $P_i \neq P_j$ for*

$i \neq j$. *We have* $\Delta(R,\rho,\varphi) = \{w(M) \mid M \in \Delta_{<_w}(I_q)\}$ *where* $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle$.

Remark 5 *It is possible to generalize Theorem 8 to deal with the situation where* $\{P_1,\ldots,P_n\}$ *(*$P_i \neq P_j$ *for* $i \neq j$*) is not necessarily the entire variety* $\mathcal{V}_{\mathbb{F}_q}(I)$ *but is any subset. From the fact that every finite set of points constitutes a variety we conclude that there exist polynomials* $G_1(X_1,\ldots,X_m),\ldots,G_s(X_1,\ldots X_m)$ *such that* $\{P_1,\ldots,P_n\} = \mathcal{V}_{\mathbb{F}_q}(I + \langle G_1,\ldots,G_s\rangle)$. *But then we can apply [1, Prop. 20] which states that if* $\{P_1,\ldots,P_n\} = \mathcal{V}_{\mathbb{F}_q}(I + \langle G_1,\ldots,G_s\rangle)$ *then the result in Theorem 8 holds again if we replace* $I_q = I + \langle X_1^q - X_1,\ldots,X_m^q - X_m\rangle$ *with* $I + \langle G_1,\ldots,G_s\rangle + \langle X_1^q - X_1,\ldots,X_m^q - X_m\rangle$.

Remark 6 *The concept of affine variety codes was coined in [5]. The construction is based on an ideal* $I \subseteq \mathbb{F}_q[X_1,\ldots,X_m]$ *from which we define* I_q *just as in Theorem 8. We write* $\{P_1,\ldots,P_n\} = \mathcal{V}_{\mathbb{F}_q}(I_q)$, $R = \mathbb{F}_q[X_1,\ldots,X_m]/I_q$ *and let* L *be any subspace of the vector space* R. *Defining* $\varphi : R \to \mathbb{F}_q^n$ *by* $\varphi(F(X_1,\ldots,X_m)+I) = (F(P_1),\ldots,F(P_n))$ *the code* $C(I,L) = \{\varphi(f) \mid f \in L\}$ *and its dual are called affine variety codes. We observe that Theorem 7, Theorem 8 and Remark 5 provide us with a way of interpreting order domain codes as affine variety codes.*

Theorem 8 immediately applies to the Hermitian order domain and the polynomial ring $\mathbb{F}_q[X_1,\ldots,X_m]$. However, we already derived the corresponding set $\Delta(R,\rho,\varphi)$ in Examples 5 and 6 so we will not treat them again. Instead we apply Theorem 8 to the order domain in Example 12.

Example 13 In Example 12 we considered $R = \mathbb{F}_{q^2}[X,Y,Z,U]/I$ where $I = \langle H_1(X,Y,Z,U), H_2(X,Y,Z,U)\rangle$ and $H_1(X,Y,Z,U) = X^q + YZ^q - Y^qZ - X$, $H_2(X,Y,Z,U) = U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U$ with $a,b \in \mathbb{F}_q$. We defined weights $w(X) = (q,1), w(Y) = (0,q), w(Z) = (q,0), w(U) = (q+1,0) \in \mathbb{N}_0^2$ and chose as term ordering $<_{\mathbb{N}_0^2}$ any term ordering satisfying (q^2,q), (q,q^2), $(0,q^2+q) <_{\mathbb{N}_0^2} (q^2+q,0)$ and $(q,q^2) <_{\mathbb{N}_0^2} (q^2,q)$. As ordering $<_{\mathcal{M}}$ we chose any term ordering on $\mathcal{M}(X,Y,Z,U)$ that satisfies $YZ^q <_{\mathcal{M}} X^q$ and $Z^{q+1} <_{\mathcal{M}} U^q$. Defining $<_w$ accordingly we showed that R is an order domain satisfying the conditions in Theorem 6. By applying Buchberger's first criterion we now see 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}. Hence, we get

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

The footprint is of size q^6 and we therefore get codes of length $n = q^6$. The footprint $\Delta_{<_w}(I_q)$ has the form of a box. From this observation it is not difficult to show that the dimension of $\tilde{C}_\varphi(s)$ equals the dimension of $\tilde{E}_\varphi(s)$ for all

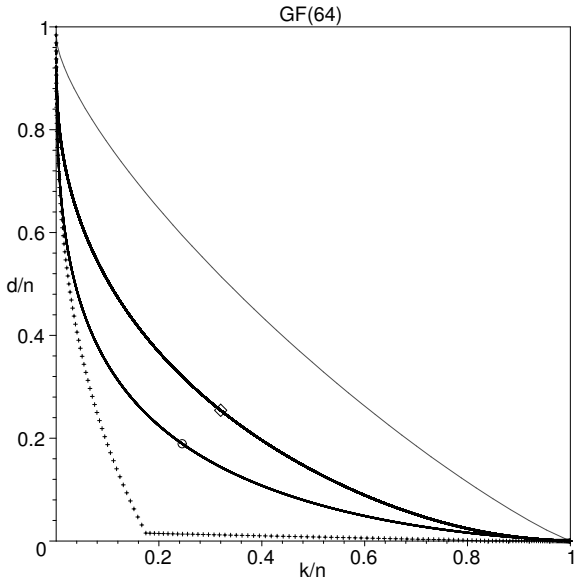

Figure 1:

$s = 1, 2, \ldots, q^6$. In Figure 1 we plot the estimated performances of the codes $\tilde{E}_\varphi(\delta)$ and $\tilde{C}_\varphi(\delta)$ from the present example in the case $\mathbb{F}_{q^2} = \mathbb{F}_{64}$. These codes are of length $n = 262144$ and are marked with a $\diamond$. The hyperbolic codes and the generalized Reed-Muller codes from $\mathbb{F}_{64}[X_1, X_2, X_3]$ are of the same length. For comparison we also plot their performances. The performances of the hyperbolic codes are given by the graph marked with a $\circ$ and the performances of the generalized Reed-Muller codes are marked with $+$'s. The last graph is the asymptotic Gilbert-Varshamov bound.

7 The connection to valuation theory

The theory of order domains has grown too large in its almost ten years lifetime for us to be able to cover all interesting aspects in the present paper. One of the aspects that we have not treated is the connection to valuation theory. We now give a brief discussion of the subject and refer the reader to the literature for more details. In Example 2 and Section 4 we demonstrated the close connection between weight functions with $\Gamma \subseteq \mathbb{N}_0 \cup \{-\infty\}$ and valuations on curves. It should come as no surprise that every weight function corresponds to a valuation on an extension of the order domain. In Remark 2 we defined a more general class of functions called order functions which maps to a well-order $(\Gamma, <_\Gamma)$. As mentioned in Section 5 we can make Γ into a semigroup by defining the binary operation $\oplus$ on Γ by $\rho(f) \oplus \rho(g) = \rho(fg)$. It was shown in [15, Th. 2.1] and [9, Pro. 6.1] that the above observation regarding a connection to valuation theory applies

to order functions in general, in that an order function $\rho : R \to \Gamma \cup \{-\infty\}$ defines a valuation $\tilde{\rho} : \mathrm{QF}(R) \to \mathrm{D}(\Gamma) \cup \{\infty\}$ by $\tilde{\rho}(0) = \infty$ and $\tilde{\rho}(f/g) = \rho(g) - \rho(f)$. Here, $\mathrm{QF}(R)$ denotes the field of fractions of R and $\mathrm{D}(\Gamma)$ is the totally ordered semigroup of differences of Γ. We have seen in Section 4 that every valuation related to a rational place of a function field in one variable defines an order function. For function fields in more variables the picture is more complicated as for these there are classes of valuations that do not define order functions. A thoroughly treatment of the problem in the case of a function field in two variables can be found in [15]. Moreover, sufficient conditions for a valuation to define an order function can be found in [13, Th. 2]. These conditions then are used in [13] to construct order functions on the basis of projective varieties that have a flag of subvarieties satisfying certain mild conditions. Using this method order functions on all Hermitian hypersurfaces are described.

8 Aknowledgements

The author wishes to express a special thank to Professor Ryutaroh Matsumoto who drew the author's attention to Theorem 7. Also the author would like to thank the anonymous referees as well as Professor Massimiliano Sala and Professor Shojiro Sakata for their helpful comments and suggestions.

References

[1] H. E. Andersen, On puncturing of codes from norm-trace curves, *Finite Fields and Their Applications*, **13**, 2007, pp. 136-157

[2] H. E. Andersen, O. Geil, Evaluation codes from order domain theory, *Finite Fields and Their Applications*, 2007, doi:10.1016/j.ffa.2006.12.004

[3] P. Beelen, The order bound for general algebraic geometric codes, *Finite Fields and Their Applications*, 2006, doi:10.1016/j.ffa.2006.09.006

[4] M. Bras-Amorós and M. E. O'Sullivan, The Correction Capability of the Berlekamp-Massey-Sakata algorithm with Majority Voting, *Appl. Algebra Engrg. Comm. Comput.,* **17**, 2006, pp. 315-335

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

[6] O. Geil, On codes from norm-trace curves, *Finite Fields and their Applications*, **9**, 2003, pp. 351-371

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

[8] O. Geil and R. Matsumoto, Generalized Sudan's list decoding for order domain codes, manuscript, 2007, 13 pages

[9] O. Geil and R. Pellikaan, On the structure of order domains, *Finite Fields and their Applications*, **8**, 2002, pp. 369-396

[10] O. Geil and C. Thommesen, On the Feng-Rao Bound for Generalized Hamming Weights, Proc. AAECC-16, *Lecture Notes in Comput. Sci. 3857*, Springer, Berlin, 2006, pp. 295-306

[11] P. Heijnen, R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inf. Theory*, **44**, 1998, pp. 181-196

[12] 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, pp. 871-961

[13] J. B. Little, The Ubiquity of Order Domains for the Construction of Error Control Codes, *Advances in Mathematics of Communications*, **1**, 2007, pp. 151-171

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

[15] M. E. O'Sullivan, New codes for the Berlekamp-Massey-Sakata algorithm, *Finite Fields and Their Applications*, **7**, 2001, pp. 293-317