Evaluation Codes from an Affine Variety Code Perspective[1]

Olav Geil
Department of Mathematical Sciences, Aalborg University,
Fr. Bajersvej 7G, 9220 Aalborg Ø, Denmark,
olav@math.aau.dk

Abstract: *Evaluation codes (also called order domain codes) are traditionally introduced as generalized one-point geometric Goppa codes. In the present paper we will give a new point of view on evaluation codes by introducing them instead as particular nice examples of affine variety codes. Our study includes a reformulation of the usual methods to estimate the minimum distances of evaluation codes into the setting of affine variety codes. Finally we describe the connection to the theory of one-point geometric Goppa codes.*

1 Introduction

Over the years the theory of geometric Goppa codes has produced many interesting results. The only drawback is that the codes are often described theoretically and that concrete generator matrices or parity check matrices are often not rendered. As an attempt to simplify the description of one-point geometric Goppa codes and to support an easy generalization of such codes to higher dimensional objects than curves, Høholdt, van Lint, and Pellikaan founded the theory of order domains in [20]. You may say that order domains are manufactured to simplify the concrete code constructions. That is, generator matrices and parity check matrices are easily described. The codes defined from order domains are often called evaluation codes or order domain codes. The minimum distance and in larger generality the generalized Hamming weights of evaluation codes can be found by applying one of two bounds that rely only on some relatively simple theory. For a parity check matrix description one applies the order bound [20], [19] and [18]. This bound is an incidence of the Feng-Rao bound [11], [12], [29]. If instead a generator matrix description is given then one uses the bound in [2] which relies on the same notion as does the more well-known order bound.

[1] **Appeared as Chapter 4 in "Advances in Algebraic Geometry Codes," Edited by E. Martinez Moro, C. Munuera and D. Ruano, World Scientific Comp., 2008**

Although evaluation codes have their origin in the study of geometric Goppa codes in the present paper we will turn things upside down and introduce them as particular nice examples of affine variety codes. This adds a new perspective to the theory of evaluation codes as well as to the theory of affine variety codes. We reformulate the Feng-Rao bound and the bound from [2] into the setting of affine variety codes. Having done this we see that the affine variety codes for which we get maximal information from the above two bounds are the affine variety codes related to order domains. We conclude the paper by describing the connection to the theory of one-point geometric Goppa codes.

2 Affine variety codes

Affine variety codes were introduced by Fitzgerald and Lax in [13]. The definition of the codes calls for an ideal $I \subseteq \mathbf{F}_q[X_1, \ldots, X_m]$ from which we start by defining

$$\begin{aligned} I_q &= I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle && (1) \\ R_q &= \mathbf{F}_q[X_1, \ldots, X_m]/I_q. && (2) \end{aligned}$$

Let

$$V = \{P_1, \ldots, P_n\} = \mathcal{V}_{\mathbf{F}_q}(I_q) = \mathcal{V}_{\bar{\mathbf{F}}_q}(I_q)$$

be the variety of I_q. Here, $\bar{k}$ means the algebraic closure of the field k and $P_i \neq P_j$ for $i \neq j$. Define an $\mathbf{F}_q$ linear map $\mathrm{ev} : R_q \rightarrow \mathbb{F}_q^n$ by

$$\mathrm{ev}(F + I_q) = (F(P_1), \ldots, F(P_n)).$$

We will call this map an evaluation map. Writing $P_j = (P_j^{(1)}, \ldots, P_j^{(m)})$ for $j = 1, \ldots, n$ we see that the i-th entry of

$$\mathrm{ev}\Bigg(\Bigg(\prod_{s=1,\ldots,m} \prod_{\substack{j=1,\ldots,n \\ P_j^{(s)} \neq P_i^{(s)}}} (X_s - P_j^{(s)})\Bigg) + I_q\Bigg)$$

is nonzero whereas all other entries equal zero. Therefore, the map ev is surjective. We next show that ev is also injective. To this end we first recall from [4, Pro. 8.14] that if J is an ideal in a polynomialring $k[X_1, \ldots, X_m]$

where k is perfect and if J contains a squarefree univariate polynomial in every variable then J is a radical ideal. This clearly makes I_q radical. Next we recall from The Strong Nullstellensatz [7, Th. 6, Sec. 4.2] that if an ideal $J \subseteq \bar{k}[X_1, \ldots, X_m]$ is radical then the vanishing ideal of the variety $\mathcal{V}_{\bar{k}}(J)$ is J itself. This implies that the vanishing ideal in $\mathbf{F}_q[X_1, \ldots, X_m]$ of V equals I_q and therefore the map ev is injective. We have shown that ev is a vector space isomorphism. We can now define the affine variety codes.

Definition 1 *Let I_q and R_q be as in (1) and (2) and assume that L is an $\mathbf{F}_q$-vector subspace of R_q. Define the affine variety code $C(I, L) = ev(L)$, and the affine variety code $C(I, L)^{\perp}$ to be the orthogonal complement of $C(I, L)$ with respect to the usual inner product on $\mathbf{F}_q^n$. That is,*

$$C(I, L)^{\perp} = \{\vec{c} \mid \vec{c} \cdot ev(F + I_q) = 0 \textit{ for all } F + I_q \in L\}$$

where $\vec{f} \cdot \vec{h}$ denotes the inner product of $\vec{f}$ and $\vec{h}$.

3 Some Gröbner basis theoretical tools

In this section we present some Gröbner basis theoretical tools that will be very useful in the construction of affine variety codes. The tools will also help us to estimate the parameters of the codes. We start by recalling the concept of a footprint.

Definition 2 *Let $J \subseteq k[X_1, \ldots, X_m]$ be an ideal and let $\prec$ be a fixed monomial ordering. Denote by $\mathcal{M}(X_1, \ldots, X_m)$ the monomials in the variables $X_1, \ldots, X_m$. The footprint of J with respect to $\prec$ is the set*

$$\Delta_{\prec}(J) = \{M \in \mathcal{M}(X_1, \ldots, X_m) \mid M \textit{ is not the leading monomial of any polynomial in } J\}.$$

Given a basis for the ideal J it may indeed not be obvious at a first glance what is the footprint. However, every polynomial ideal possesses a particular type of basis from which the footprint can be easily read off. These are the Gröbner bases.

Definition 3 *Let $J \subseteq k[X_1, \ldots, X_m]$ be an ideal and $\prec$ a monomial ordering. A finite subset $\mathcal{G}$ of J is called a Gröbner basis (with respect to $\prec$) if for every polynomial $P(X_1, \ldots, X_m) \in J$ there exists a $G \in \mathcal{G}$ such that the leading monomial of G divides the leading monomial of P.*

One of the main results in Gröbner basis theory is that a Gröbner basis $\mathcal{G}$ for J is indeed a basis for J. Given a basis for J we can extend it to a Gröbner basis by applying Buchberger's algorithm. Hence, there is a method to detect the footprint $\Delta_{\prec}(J)$.

The next couple of results explain our interest in the footprint. From [7, Pro. 4, Sec. 5.3] we have the following proposition.

Proposition 1 *Let the notation be as in Definition 2. The set*

$$\{M + J \mid M \in \Delta_{\prec}(J)\} \tag{3}$$

constitutes a basis for $k[X_1, \ldots, X_m]/J$ as a vector space over k.

Throughout this paper we will make extensively use of the division algorithm for multivariate polynomials [7, Sec. 2.3] with which we will assume the reader to be familiar. Given a monomial ordering, a polynomial H and an ordered list of polynomials $(G_1, \ldots, G_r)$ the algorithm calculates the remainder of H modulo $(G_1, \ldots, G_r)$. This remainder is written H rem $(G_1, \ldots, G_r)$. When $\mathcal{G} = \{G_1, \ldots, G_s\}$ constitutes a Gröbner basis (for the ideal $\langle G_1, \ldots, G_r\rangle$) the remainder does not depend on how we order the elements in the list $(G_1, \ldots, G_r)$ and therefore in this case we will simply talk about the remainder modulo $\mathcal{G}$. We observe that to write an element $H + J \in k[X_1, \ldots, X_m]/J$ as a linear combination of the elements in (3) we need only find the remainder of H modulo the Gröbner basis $\mathcal{G}$. Moreover, as a consequence of Proposition 1 and the definition of a Gröbner basis, H rem $\mathcal{G}$ are the same no matter which Gröbner basis is chosen for J as long as $\prec$ is fixed.

Applying the above theory to the case $R_q = \mathbf{F}_q[X_1, \ldots, X_m]/I_q$ we see that for every fixed choice of $\prec$ Proposition 1 gives us a basis $\{M + I_q \mid M \in \Delta_{\prec}(I_q)\}$ for R_q. If $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ is a basis for a subspace $L \subseteq R_q$ we may therefore without loss of generality assume that $\mathrm{Supp}(B_1), \ldots, \mathrm{Supp}(B_{\dim(L)}) \subseteq \Delta_{\prec}(I_q)$. Here, $\mathrm{Supp}(F)$ means the support of F. Once the variety $\mathcal{V}_{\mathbb{F}_q}(I_q)$ is found we can then easily specify the generator matrix for $C(I, L)$ as well as easily specify the parity check matrix for $C(I, L)^{\perp}$. The length of the codes clearly is

$$n = \#\mathcal{V}_{\mathbb{F}_q}(I_q) = \#\mathcal{V}_{\mathbb{F}_q}(I) = \#\Delta_{\prec}(I_q).$$

As ev is an isomorphism the dimension of $C(I, L)$ is $\dim(L)$ whereas the dimension of $C(I, L)^{\perp}$ equals $n - \dim(L)$. What remains is to estimate the

minimum distances of the codes. This will be done in Section 4 and Section 5 below.
In Section 4 we will need the following corollary to Proposition 1. It is an incidence of the more general footprint bound [8, Cor. 2.5, Sec. 4.2].

Corollary 1 *Let $F_1, \ldots, F_s \in \mathbf{F}_q[X_1, \ldots, X_m]$. The number of common zeros of $F_1, \ldots, F_s$ over $\mathbf{F}_q$ is $\#\Delta_\prec(\langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m\rangle)$ (here $\prec$ is any monomial ordering).*

Proof: Let n be the number of common zeros. As explained in the previous section R_q is isomorphic to $\mathbf{F}_q^n$ as a vector space over $\mathbf{F}_q$ under the isomorphism ev. By Proposition 1 the dimension of R_q is $\#\Delta_\prec(I_q)$. The proof is complete.

4 A bound on the minimum distance of $C(I, L)$

We now estimate the minimum distance of $C(I, L)$. The bound that we present can be viewed as an interpretation of the bound in [2, Th. 8]. Let $\prec$ and $I \subseteq \mathbf{F}_q[X_1, \ldots X_m]$ be fixed and consider a subspace $L \subseteq R_q$. By using Gaussian elimination any basis of L can be transformed into a basis of the following form.
Definition 4 *A basis $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ for $L \subseteq R_q$ where $Supp(B_i) \subseteq \Delta_\prec(I_q)$ for $i = 1, \ldots, \dim(L)$ and where $lm(B_1) \prec \cdots \prec lm(B_{\dim(L)})$ is said to be well-behaving with respect to $\prec$. Here, $lm(F)$ means the leading monomial of F.*

For fixed $\prec$ the sequence $\big(\mathrm{lm}(B_1), \ldots, \mathrm{lm}(B_{\dim(L)})\big)$ is the same for all choices of well-behaving bases of L. Therefore the following definition makes sense.

Definition 5 *Let L be a subspace of R_q and define*

$$\Box_\prec(L) = \{lm(B_1), \ldots, lm(B_{\dim(L)})\}$$

where $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ is any well-behaving basis of L with respect to $\prec$.

Definition 6 *Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to $\prec$. An ordered pair of monomials (M_1, M_2), $M_1, M_2 \in \Delta_\prec(I_q)$ is said to be one-way well-behaving (OWB) if for all H with $Supp(H) \subseteq \Delta_\prec(I_q)$ and $lm(H) = M_1$*

$$lm(M_1 M_2 \text{ rem } \mathcal{G}) = lm(H M_2 \text{ rem } \mathcal{G})$$

holds.

As already mentioned F rem $\mathcal{G} = F$ rem $\mathcal{G}'$ if $\mathcal{G}$ and $\mathcal{G}'$ are Gröbner bases for I_q with respect to identical ordering. Therefore the definition of OWB is independent of which Gröbner basis $\mathcal{G}$ we consider as long as $\prec$ is fixed.

Theorem 1 *Let $\prec$ be fixed. The minimum distance of $C(I, L)$ is at least*

$$\min \Big\{ \#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \textit{ such that } \\ (P, N) \textit{ is OWB and } lm(PN \textit{ rem } \mathcal{G}) = K\} \Big| P \in \Box_\prec(L) \Big\}.$$

Proof: Let $\vec{c} \in C(I, L)$. Then there exists an F such that $\mathrm{Supp}(F) \subseteq \Delta_\prec(I_q)$, $\mathrm{lm}(F) = P \in \Box_\prec(L)$ and $\mathrm{ev}(F + I_q) = \vec{c}$. By Corollary 1 the Hamming weight of $\vec{c}$ is equal to $n - \#\Delta_\prec(I_q + \langle F \rangle)$ and therefore we take a closer look at $\Delta_\prec(I_q + \langle F \rangle)$. If $N, K \in \Delta_\prec(I_q)$ satisfy that (P, N) is OWB and $\mathrm{lm}(PN \text{ rem } \mathcal{G}) = K$ then

$$K \in \Delta_\prec(I_q) \backslash \Delta_\prec(I_q + \langle F \rangle).$$

Hence,

$$\#\Delta_\prec(I_q + \langle F \rangle) \leq \#\Delta_\prec(I_q) - \#\Big\{ K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \\ \text{such that } (P, N) \text{ is OWB and } \mathrm{lm}(PN \text{ rem } \mathcal{G}) = K \Big\}. \quad (4)$$

But $n = \#\Delta_\prec(I_q)$ and therefore the Hamming weight of $\vec{c}$ is at least

$$\#\Big\{ K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \\ \text{such that } (P, N) \text{ is OWB and } \mathrm{lm}(PN \text{ rem } \mathcal{G} = K \Big\}.$$

The proof is complete.

It is of course possible to apply Theorem 1 for different choices of $\prec$ to see which one gives the sharpest estimate. To get the full advantage of Theorem 1 we need to have some information of the algebraic structure of R_q. The following Corollary, however, easily applies to any affine variety code. Also this bound could be applied for different choices of $\prec$ to get the sharpest estimate.

Corollary 2 *Let $\prec$ be fixed. The minimum distance of $C(I, L)$ is at least*

$$\min \Big\{ \#\{K \in \Delta_\prec(I_q) \mid P \textit{ divides } K\} \Big| P \in \Box_\prec(L) \Big\}. \quad (5)$$

Proof: Let K, P be as in (5). Clearly $\frac{K}{P} \in \Delta_{\prec}(I_q)$. To see that $(P, \frac{K}{P})$ is OWB let H be a polynomial with $\mathrm{lm}(H) = P$ and $\mathrm{Supp}(H) \subseteq \Delta_{\prec}(I_q)$. Clearly, the leading monomial of $H\frac{K}{P}$ is equal to K. The division algorithm, when applied to $H\frac{K}{P}$ and $\mathcal{G}$, starts by moving K to the remainder. This is due to $K \in \Delta_{\prec}(I_q)$. When we run the division algorithm all other terms A are either moved to the remainder, are replaced with with polynomials S such that $\mathrm{lm}(S) \prec \mathrm{lm}(A)$ holds, or are replaced with 0. Therefore,

$$\mathrm{lm}\big(H\frac{K}{P} \text{ rem } \mathcal{G}\big) = K = \mathrm{lm}\big(P\frac{K}{P} \text{ rem } \mathcal{G}\big).$$

The proof is complete.

Remark 1 *It is possible to modify Theorem 1 and Corollary 2 to also deal with generalized Hamming weights. For the case of Theorem 1 this corresponds to interpreting the bound in [2, Th. 10].*

Example 1 *Let* $I = \langle 0 \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$. *Then*

$$\mathcal{G} = \{X_1^q - X_1, \ldots, X_m^q - X_m\}$$

is a Gröbner basis for I_q *(regardless of the ordering* $\prec$ *chosen). Hence,*

$$\Delta_{\prec}(I_q) = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q\}$$

holds and

$$\{X_1^{i_1} \cdots X_m^{i_m} + I_q \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q\}$$

is a basis for $R_q = \mathbb{F}_q[X_1, \ldots, X_m]/I_q$ *as a vectorspace over* $\mathbb{F}_q$. *It follows that the corresponding affine variety codes are of length* $n = \#\Delta_{\prec}(I_q) = q^m$. *Let* s *be an integer* $0 \leq s \leq m(q-1)$. *If we choose* L *to be the space generated by the basis elements* $X_1^{i_1} \cdots X_m^{i_m} + I_q$ *with* $i_1 + \cdots + i_m \leq s$ *then we get*

$$L = \{F(X_1, \ldots, X_m) + I_q \mid \deg(F) \leq s\}. \tag{6}$$

Here, $\deg(F)$ *means the total degree of* F. *Clearly,*

$$\Box_{\prec}(I_q) = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\}.$$

The code $C(I, L)$ *is known as the generalized Reed-Muller code* $RM_q(s, m)$, *and Corollary 2 tells us that the minimum distance of* $RM_q(s, m)$ *is at least*

$$\min\{(q - i_1) \cdots (q - i_m) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\} \tag{7}$$

as

$$\#\{X_1^{j_1}\cdots X_m^{j_m}\in\Delta_\prec(I_q)\mid X_1^{i_1}\cdots X_m^{i_m}\ \textit{divides}\ X_1^{j_1}\cdots X_m^{j_m}\} = (q-i_1)\cdots(q-i_m).$$

Writing $s=a(q-1)+b$ with $a,b\in\mathbb{N}_0$ and $0\leq b<q-1$ the number in (7) can be shown to be equal to $(q-b)q^{m-a-1}$. Now letting $\mathbb{F}_q=\{\alpha_1,\ldots,\alpha_q\}$ and defining

$$F=(X_1^{q-1}-1)\cdots(X_a^{q-1}-1)(X_{a+1}-\alpha_1)\cdots(X_{a+1}-\alpha_b)$$

we see that $ev(F+I_q)\in C(I,L)$ is of Hammingweight equal to $(q-b)q^{m-a-1}$. Hence, Corollary 2 produces the correct value of the minimum distance of the generalized Reed-Muller codes. It is interesting to observe that the minimum distance of the generalized Reed-Muller codes was originally established using quite different and more complicated methods [23].
If the goal is to produce codes with good parameters then there is better choice of L than (6) namely

$$L=Span_{\mathbb{F}_q}\{X_1^{i_1}\cdots X_m^{i_m}\mid 0\leq i_1<q,\ldots,0\leq i_m,(q-i_1)\cdots(q-i_m)\geq\delta\}. \tag{8}$$

Corollary 2 tells us that the corresponding code $C(I,L)$ is of minimum distance at least δ and it is the largest code of prescribed minimum distance δ. If actually $i_1,\ldots,i_m$ exists with $(q-i_1)\cdots(q-i_m)=\delta$ then, as above, we can detect a codeword of Hammingweight δ and we conclude that Corollary 2 produces the actual minimum distance in this case. The codes $C(I,L)$ corresponding to (8) are called Massey-Costello-Justesen codes [26], [22] and are of course examples of improved generalized Reed-Muller codes.

5 The Feng-Rao bound for $C(I,L)^\perp$

In this section we reformulate the Feng-Rao bound into the setting of affine variety codes.
Theorem 2 *Let $\prec$ be fixed. The minimum distance of $C(I,L)^\perp$ is at least*

$$\min\big\{\#\{P\in\Delta_\prec(I_q)\mid\exists N\in\Delta_\prec(I_q)\ \textit{such that}\ (P,N)\ \textit{is OWB and}\ lm(PN\ rem\ \mathcal{G})=K\}\big|K\in\Delta_\prec(I_q)\backslash\Box_\prec(L)\big\}. \tag{9}$$

Proof: Let $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ be a well-behaving basis for L. Consider $\vec{c} \in C(I,L)^\perp \backslash \{\vec{0}\}$. That is, $\vec{c}$ satisfies $\vec{c} \cdot \mathrm{ev}(B_i + I_q) = 0$ for $i = 1, \ldots, \dim(L)$ but

$$\vec{c} \cdot \mathrm{ev}(K + I_q) \neq 0 \tag{10}$$

holds for some $K \in \Delta_\prec(I_q)$. Let $K \in \Delta_\prec(I_q)$ be smallest possible with respect to $\prec$ such that (10) holds. By linearity of the inner product and the minimality of K we have $K \notin \Box_\prec(L)$. Consider OWB pairs $(P_1, N_1), \ldots, (P_\delta, N_\delta)$, where $P_1, N_1, \ldots, P_\delta, N_\delta \in \Delta_\prec(I_q)$, $P_1 \prec \cdots \prec P_\delta$ and $\mathrm{lm}(P_i N_i \text{ rem } \mathcal{G}) = K$ for $i = 1, \ldots, \delta$. The minimality of K and the OWB property of (P_i, N_i) ensure that

$$\vec{c} \cdot \mathrm{ev}\Big(\big(\sum_{\substack{t = 1, \ldots, i \\ a_i \neq 0}} a_t P_t \big) N_i \text{ rem } \mathcal{G} + I_q \Big) \neq 0 \tag{11}$$

holds for any $i \in \{1, \ldots, \delta\}$. Let $*$ be the componentwise product on $\mathbb{F}_q^n$ given by

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

As

$$\big(\sum_{\substack{t = 1, \ldots, i \\ a_i \neq 0}} a_t P_t \big) N_i \text{ rem } \mathcal{G} \ + \ I_q \quad = \quad \big(\sum_{\substack{t = 1, \ldots, i \\ a_i \neq 0}} a_t P_t \big) N_i \ + \ I_q$$

we conclude from (11) that

$$\vec{c} * \mathrm{ev}\Big(\big(\sum_{\substack{t = 1, \ldots, i \\ a_i \neq 0}} a_t P_t \big) + I_q \Big) \neq \vec{0}$$

for any $i \in \{1, \ldots, \delta\}$. Hence, $\vec{c} * \vec{e} \neq \vec{0}$ for all

$$\vec{e} \in \big\{ \mathrm{ev}\big(\big(\sum_{t=1}^{\delta} a_t P_t \big) + I_q \big) \big| a_1, \ldots, a_\delta \in \mathbb{F}_q, \text{ not all } a_i \text{ equal } 0 \big\}. \tag{12}$$

The space consisting of (12) and $(0, \ldots, 0)$ is of dimension δ and therefore the Hamming weight of $\vec{c}$ needs to be at least δ. The proof is complete.

It is of course possible to apply Theorem 2 to different choices of $\prec$ to see which one gives the sharpest estimate. Theorem 2 requires that we have some information about the algebraic structure of R_q. The following Corollary, however, easily applies to any affine variety code. Also this bound could be applied for different choices of $\prec$ to get the sharpest estimate.

Corollary 3 *Let the notation be as in Theorem 2. The minimum distance of $C(I, L)^\perp$ is at least*

$$min\big\{\#\{P \in \Delta_\prec(I_q) \mid P \text{ divides } K\}\big|K \in \Delta_\prec(I_q)\backslash\Box_\prec(L)\big\}.$$

Proof: See the proof of Corollary 2.

Remark 2 *It is possible to modify Theorem 2 and Corollary 3 to also deal with generalized Hamming weights. For the case of Theorem 2 this corresponds to interpreting the last part of [18, Th. 1].*

Example 2 *This is a continuation of Example 1. It is well-known that the dual code of a generalized Reed-Muller code is again a generalized Reed-Muller code. More precisely,*

$$RM_q(s, m) = RM_q((q-1)m-1-s, m)^\perp$$

holds [9, Th. 2.2.1]. Applying Corollary 3 to $RM((q-1)m-1-s, m)^\perp$ we see that the minimum distance of $RM_q(s, m)$ is at least

$$\min\big\{(i_1+1)\cdots(i_m+1) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \\ i_1 + \cdots + i_m \geq (q-1)m - s\big\}. \quad (13)$$

Writing again $s = a(q-1)+b$ with $0 \leq b < q-1$ (13) becomes equal to $(q-b)q^{m-a-1}$ which we in Example 1 have seen to be equal to the true minimum distance of $RM_q(s, m)$. Hence, also Corollary 3 produces the true value of the minimum distance of generalized Reed-Muller codes. If the goal is to produce codes $C(I, L)^\perp$ with good parameters then choosing L to be

$$L = Span_{\mathbb{F}_q}\big\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \\ (i_1+1)\cdots(i_m+1) < q^m - s\big\} \quad (14)$$

would be a better choice. The codes $C(I,L)^\perp$ corresponding to (14) are called hyperbolic codes and are denoted $Hyp_q(s,m)$ [14, Def. 6]. By [14, Th. 3] $Hyp_q(s,m)$ equals $C(I,L')$ where L' is the space in (8) with $r = q^m - s$. That is, hyperbolic codes are the same as Massey-Costello-Justesen codes. We showed in Example 1 that the minimum distance of $C(I,L')$ is at least $q^m - s$. Applying Corollary 3 to $Hyp_q(s,m)$ also gives the result that the minimum distance is at least $q^m - s$. Hence, Corollary 2 and Corollary 3 produce the same results for generalized Reed-Muller codes and for Hyperbolic codes.

6 Using weighted degree orderings

In this section we consider two examples where the monomial ordering is a weighted degree lexicographic ordering.

Definition 7 *Let $w(X_1), \ldots, w(X_m) \in \mathbf{N}$ and define the weight of $X_1^{i_1} \cdots X_m^{i_m}$ to be the number $w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m)$. The weighted degree lexicographic ordering on $\mathcal{M}(X_1, \ldots, X_m)$ is the ordering with $X_1^{i_1} \cdots X_m^{i_m} \prec X_1^{j_1} \cdots X_m^{j_m}$ if either $w(X_1^{i_1} \cdots X_m^{i_m}) < w(X_1^{j_1} \cdots X_m^{j_m})$ holds or $w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m})$ holds but $X_1^{i_1} \cdots X_m^{i_m} \prec_{lex} X_1^{j_1} \cdots X_m^{j_m}$. Here, $\prec_{lex}$ is the lexicographic ordering with $X_m \prec_{lex} \cdots \prec_{lex} X_1$.*

One of the qualities of weighted degree lexicographic orderings is the following lemma. The proof of the lemma is left for the reader.

Lemma 1 *Let a weighted degree lexicographic ordering be given as in Definition 7. If H has got exactly one monomial of highest weight w' in its support and G has exactly two monomials of highest weight in its support then H rem (G) has exactly one monomial of highest weight in its support and this weight is w'.*

The codes $C(I,L)^\perp$ in the next example were originally treated in [24] whereas the codes $C(I,L)$ are treated for the first time in the present paper.

Example 3 *Consider the ideals*

$$I = \langle X^3Y + Y^3 + X \rangle \subseteq \mathbf{F}_8[X,Y]$$

$$I_q = I + \langle X^8 + X, Y^8 + Y \rangle \subseteq \mathbf{F}_8[X,Y].$$

Let $\prec$ be the weighted degree lexicographic ordering defined by setting $w(X) = 2$, $w(Y) = 3$ and by interpreting X as X_1 and Y as X_2. Clearly, $\mathcal{B} = \{X^3Y + Y^3 + X\}$ is a Gröbner basis for I and

$$\Delta_{\prec}(I) = \{X^iY^j \mid \ \textit{if } i \geq 3 \textit{ then } j = 0\}$$

holds. Using Buchberger's algorithm we find the following Gröbner basis for I_q

$$\mathcal{G} = \{X^3Y + Y^3 + X, X^8 + X, XY^5 + X^5 + X^2Y^2 + Y, Y^7 + X^7\}$$

and therefore

$$\Delta_{\prec}(I_q) = \big\{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, X^4, Y^3, X^2Y^2, X^5, XY^3, Y^4, X^6, X^2Y^3, XY^4, X^7, Y^5, X^2Y^4, Y^6\big\} \quad (15)$$

with corresponding weights

$$\{0, 2, 3, 4, 5, 6, 6, 7, 8, 8, 9, 10, 10, 11, 12, 12, 13, 14, 14, 15, 16, 18\}.$$

The elements in (15) are listed in increasing order with respect to $\prec$. Using Lemma 1 and some other results we can detect altogether 166 useful OWB pairs plus a few more that we will not use. We illustrate the method used to check for the OWB property by considering a few OWB pairs. First to see that (X^3, X) is OWB we must show that HX rem $\mathcal{G} = X^3X$ rem $\mathcal{G}$ for all H with $lm(H) = X^3$. We have

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + a_5XY + a_6Y^2 + X^3)X \ \textit{rem } \mathcal{G}\big) = X^4 \quad (16)$$

no matter what are $a_1, \ldots, a_6$. This is because $X^3X = X^4 \in \Delta_{\prec}(I_q)$ and therefore X^4 is moved to the remainder upon division with $\mathcal{G}$. The proof that (X^3, X) is OWB is complete. To see that (XY, X^2) is OWB we cannot apply the same argument as above as $XYX^2 = X^3Y \notin \Delta_{\prec}(I_q)$. We have

$$w(1 \cdot X^2), w(X \cdot X^2), w(Y \cdot X^2), w(X^2 \cdot X^2) < w(XY \cdot X^2) = 9.$$

That is, there is only one monomial of highest weight in $(a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2$ and this weight is 9. As $X^3Y + Y^3 + Y$ has exactly two monomials of highest weight in its support Lemma 1 tells us that the monomial

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2 \ \textit{rem } \mathcal{B}\big)$$

is also of weight 9*. There is only one such monomial in* $\Delta_\prec(I)$ *namely* Y^3*. As* Y^3 *also belongs to* $\Delta_\prec(I_q)$ *we conclude*

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2 \ rem \ \mathcal{G}\big) = Y^3$$

no matter what are $a_1, \ldots, a_4$*. Hence,* (XY, X^2) *is OWB. Finally, to see that* (XY, X^2Y) *is OWB we start by recognizing from Lemma 1 that the weight of*

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y \ rem \ \mathcal{B}\big)$$

equals $w(XY \cdot X^2Y) = 12$*. However, now there are the two possibilities* X^6 *and* Y^4 *of leading monomials as both are of weight* 12 *and both belong to* $\Delta_\prec(I)$*. A closer analysis reveals that*

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y \ rem \ \mathcal{B}\big) = Y^4.$$

As Y^4 *also belongs to* $\Delta_\prec(I_q)$ *we conclude that*

$$lm\big((a_1 + a_2X + a_3Y + a_4X^2 + XY)X^2Y \ rem \ \mathcal{G}\big) = Y^4$$

and (XY, X^2Y) *is OWB.*
Observe that for fixed P *and* K *there can exist more choices of* N *such that* (P, N) *is OWB and* $lm(PN \ rem \ \mathcal{G}) = K$*. As an example both* (XY, Y^2) *and* (XY, X^3) *are OWB and satisfy*

$$lm(XY \cdot Y^2 \ rem \ \mathcal{G}) = lm(XY \cdot X^3 \ rem \ \mathcal{G}) = XY^3.$$

In table 1 we list some information about the OWB pairs. By $\bar{\sigma}(P)$ *we denote the number of detected* $K \in \Delta_\prec(I_q)$ *such that an* $N \in \Delta_\prec(I_q)$ *exists with* (P, N) *OWB and* $lm(PN \ rem \ \mathcal{G}) = K$*. By* $\bar{\mu}(K)$ *we denote the number of detected* $P \in \Delta_\prec(I_q)$ *such that an* $N \in \Delta_\prec(I_q)$ *exists with* (P, N) *OWB and* $lm(PN \ rem \ \mathcal{G}) = K$*.*

For the code construction $C(I, L)$ *we choose* L *to be spanned by the* $(M + I_q)$*'s with* $M \in \Delta_\prec(I_q)$ *and* $\bar{\sigma}(M) \geq \delta$*. By Theorem 1 this gives us codes of highest possible dimension with prescribed minimum distance at least* δ*. For the code construction* $C(I, L)^\perp$ *we choose* L *to be spanned by the* $(M + I_q)$*'s with* $M \in \Delta_\prec(I_q)$ *and* $\bar{\mu}(M) < \delta$*. By Theorem 2 this gives codes of highest possible dimension with prescribed minimum distance at least* δ*. The length of the codes equals* $n = \#\Delta_\prec(I_q)$*. From (15) we therefore have* $n = 22$*. In Table 2 we list the parameters* $[k, \delta]$ *that can be realized from Theorem 1*

Table 1: Information about the OWB pairs

M	1	X	Y	X^2	XY	Y^2	X^3	X^2Y	XY^2	X^4	Y^3
$\bar{\sigma}(M)$	22	19	14	16	12	11	5	10	9	4	8
$\bar{\mu}(M)$	1	2	2	3	4	3	4	6	6	5	8
M	X^2Y^2	X^5	XY^3	Y^4	X^6	X^2Y^3	XY^4	X^7	Y^5	X^2Y^4	Y^6
$\bar{\sigma}(M)$	7	3	6	5	2	4	3	1	2	2	1
$\bar{\mu}(M)$	9	6	10	11	7	12	13	8	14	15	17

Table 2: Parameters of the codes

$C(I, L)$	[1,22]	[2,19]	[3,16]	[4,14]	[5,12]	[6,11]
	[7,10]	[8,9]	[9,8]	[10,7]	[11,6]	[13,5]
	[15,4]	[17,3]	[20,2]	[22,1]		
$C(I, L)^\perp$	[1,17]	[2,15]	[3,14]	[4,13]	[5,12]	[6,11]
	[7,10]	[8,9]	[10,8]	[11,7]	[14,6]	[15,5]
	[17,4]	[19,3]	[21,2]			

and Theorem 2. Here k is the dimension and δ is the prescribed minimum distance. We conclude that although the bound in Theorem 1 relies on the same notion as does the bound in Theorem 2 the two bounds can sometimes produce completely different results.

In Example 3 it was quite involved to detect which pairs are OWB. This is due to the fact that in $\Delta_\prec(I)$ as well as in $\Delta_\prec(I_q)$ there were more monomials of the same weight. In the next example no two different monomials in $\Delta_\prec(I)$ will be of the same weight. As a consequence it becomes very easy to find OWB pairs.

Example 4 *Consider the ideals*

$$I = \langle X^4 - Y^3 - Y \rangle \subseteq \mathbf{F}_9[X, Y]$$

$$I_q = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbf{F}_9[X, Y].$$

Let $\prec$ be the weighted degree lexicographic ordering given by $w(X) = 3$, $w(Y) = 4$ and by interpreting X as X_2 and Y as X_1. Clearly,

$$\mathcal{B} = \{X^4 - Y^3 - Y\}$$

is a Gröbner basis for I and applying Buchberger's algorithm we find that

$$\mathcal{G} = \{X^4 - Y^3 - Y, X^9 - X\}$$

is a Gröbner basis for I_q. Hence,

$$\begin{aligned} \Delta_\prec(I) &= \{X^i Y^j \mid 0 \leq i, 0 \leq j < 3\} \\ \Delta_\prec(I_q) &= \{X^i Y^j \mid 0 \leq i < 9, 0 \leq j < 3\}. \end{aligned} \tag{17}$$

The map $w : \Delta_\prec(I) \to \langle 3, 4\rangle$ given by $w(X^i Y^j) = i3 + j4$ is a bijection. Here, $\langle 3, 4\rangle$ means the semigroup generated by 3 and 4. Hence, we can identify any monomial $M \in \Delta_\prec(I)$ uniquely by its weight. Consider a polynomial F with $Supp(F) \subseteq \Delta_\prec(I_q)$ and write $P = lm(F)$. Let $N \in \Delta_\prec(I_q)$ be arbitrary. By Lemma 1 the leading monomial of FN rem $\mathcal{B}$ is the unique monomial $K \in \Delta_\prec(I)$ of weight equal to $w(PN) = w(P) + w(N)$. If $K \in \Delta_\prec(I_q)$ holds then (P, N) is OWB. Hence, given $P, N \in \Delta_\prec(I_q)$ then (P, N) is OWB if $w(P) + w(N) \in w(\Delta_\prec(I_q))$. Next we show that if $K \in \Delta_\prec(I_q)$ and $P, N \in \Delta_\prec(I)$ satisfy $w(P) + w(N) = w(K)$ then also $P, N \in \Delta_\prec(I_q)$ holds. This in particular implies that (P, N) is OWB. Aiming for a contradiction assume that $P \notin \Delta_\prec(I_q)$. By the definition of the footprint there exists a polynomial $H \in I_q$ having P as leading monomial. As $P \in \Delta_\prec(I)$ we may without loss of generality assume that H is reduced modulo $\mathcal{B}$. That is, we may assume that $Supp(H) \subseteq \Delta_\prec(I)$ holds. From $H \in I_q$ we conclude that

$$HN \text{ rem } \mathcal{B} \in I_q. \tag{18}$$

On the other hand the assumption $Supp(H) \subseteq \Delta_\prec(I)$ in combination with Lemma 1 implies $lm(HN \text{ rem } \mathcal{B}) = K$. Here we used the fact that no two monomials in $\Delta_\prec(I)$ are of the same weight. But K is assumed to be in $\Delta_\prec(I_q)$ and therefore (18) cannot be true. We have reached at a contradiction. Assuming $N \notin \Delta_\prec(I_q)$ would lead to a similar contradiction. The above observations imply that to detect OWB pairs it is enough to study the weights. For this purpose define

$$\Gamma = w(\Delta_\prec(I)) = \langle 3, 4\rangle$$

and for $\lambda \in w(\Delta_\prec(I_q))$ let

$$\sigma(\lambda) = \#\{\eta \in w(\Delta_\prec(I_q)) \mid \eta - \lambda \in \Gamma\}$$

and for $\lambda \in \Gamma$ *let*

$$\mu(\lambda) = \#\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}.$$

We have shown above that if $P \in \Delta_\prec(I_q)$ *then there exist pairwise different elements* $K_1, \ldots, K_{\sigma(w(P))} \in \Delta_\prec(I_q)$ *and corresponding elements* $N_1, \ldots, N_{\sigma(w(P))} \in \Delta_\prec(I_q)$ *such that for* $i = 1, \ldots, \sigma(w(P))$ (P, N_i) *is OWB with* $lm(PN_i \text{ rem } \mathcal{G}) = K_i$*. Similarly, if* $K \in \Delta_\prec(I_q)$ *then there exist pairwise different elements* $P_1, \ldots, P_{\mu(w(K))} \in \Delta_\prec(I_q)$ *and corresponding elements* $N_1, \ldots, N_{\mu(w(K))} \in \Delta_\prec(I_q)$ *such that* (P_i, N_i) *is OWB with* $lm(P_iN_i \text{ rem } \mathcal{G}) = K$*. In Table 4 we list* $\sigma(w)$ *and* $\mu(w)$ *for all* $w \in w(\Delta_\prec(I_q))$*. For the purpose of the code*

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

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

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

constructions define the following subspaces of $R_q = \mathbf{F}_9[X, Y]/I_q$

$$\begin{aligned} L_1 &= Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), w(M) \leq s\} \\ L_2 &= Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), \sigma(w(M)) \geq \delta\} \\ L_3 &= Span_{\mathbb{F}_9}\{M + I_q \mid M \in \Delta_\prec(I_q), \mu(w(M)) < \delta\}. \end{aligned}$$

The corresponding affine variety codes are all of length $n = \#\Delta_\prec(I_q) = 27$*. From Theorem 1 the minimum distance of* $C(I, L_2)$ *is at least* δ *and from Theorem 2 also the minimum distance of* $C(I, L_3)^\perp$ *is at least* δ*. The codes* $C(I, L_2)$ *and* $C(I, L_3)^\perp$ *respectively are so to speak the largest codes with designed minimum distance* δ *with respect to Theorem 1 and Theorem 2 respectively. Applying Theorem 1 and Theorem 2 respectively to the codes* $C(I, L_1)$ *and* $C(I, L_1)^\perp$ *respectively we get lower bounds on the minimum distances. As an example choosing* $s = 23$ *the code* $C(I, L_1)$ *is of dimension* 21 *and minimum distance at least* 4*. Choosing* $\delta = 4$ *the code* $C(I, L_2)$ *is of dimension* 22 *and minimum distance also at least* 4*. As another example choosing*

$s = 7$ the code $C(I, L_1)^\perp$ is of dimension 22 and of minimum distance at least 3. Choosing $\delta = 4$ the code $C(I, L_3)^\perp$ is also of dimension 22 but is of minimum distance at least 4.

7 The order domain conditions

In the previous section we demonstrated that the weighted degree lexicographic ordering can sometimes be very useful when we look for OWB pairs. In particular the task of finding OWB pairs were rather simple in Example 4 due to the fact that no two monomials in $\Delta_\prec(I)$ were of the same weight and due to the fact that the defining polynomial of I possessed exactly two monomials of highest weight in its support. In this section we generalize the construction in Example 4. All proofs will be straightforward generalizations of the arguments from Example 4 and so they are mostly left out. We start by generalizing the concept of a weighted degree lexicographic ordering.

Definition 8 *Let $w(X_1), \ldots, w(X_m) \in \mathbf{N}_0^r$ and assume $\prec_{\mathbf{N}_0^r}$ is a monomial ordering on $\mathbf{N}_0^r$. Extend w to a monomial function on $\mathcal{M}(X_1, \ldots, X_m)$ by*

$$w(X_1^{i_1} \cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m).$$

Let $\prec_\mathcal{M}$ be a monomial ordering on $\mathcal{M}(X_1, \ldots, X_m)$. The generalized weighted degree ordering defined from $w(X_1), \ldots, w(X_m)$, $\prec_{\mathbf{N}_0^r}$ and $\prec_\mathcal{M}$ is the ordering $\prec_w$ given by

$$X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$$

if

$$w(X_1^{i_1} \cdots X_m^{i_m}) \prec_{\mathbf{N}_0^r} w(X_1^{j_1} \cdots X_m^{j_m})$$

holds or if

$$w(X_1^{i_1} \cdots X_m^{i_m}) = w(X_1^{j_1} \cdots X_m^{j_m})$$

holds but

$$X_1^{i_1} \cdots X_m^{i_m} \prec_\mathcal{M} X_1^{j_1} \cdots X_m^{j_m}.$$

The weighted degree of a polynomial F is $wdeg(F) = w(lm(F))$.

We now state the order domain conditions which play a central role in the present paper.

Definition 9 *Consider an ideal $I \subseteq k[X_1, \ldots, X_m]$ where k is a field. Let a generalized weighted degree ordering $\prec_w$ be given as in Definition 8. Assume I possesses a Gröbner basis $\mathcal{B}$ such that any $G \in \mathcal{B}$ has exactly two monomials of highest weight and such that no two monomials in $\Delta_{\prec}(I)$ is of the same weight. Then we say that I and $\prec_w$ satisfy the order domain conditions.*

The following lemma is an immediate generalization of Lemma 1. Again we leave the proof for the reader.

Lemma 2 *Let I, $\prec_w$ and $\mathcal{B}$ be as in Definition 9. Let F be a polynomial with exactly one monomial of highest weight. Then $w(lm(F)) = w(lm(F \text{ rem } \mathcal{B}))$. In particular $w(lm(F)) = w(lm(F \text{ rem } \mathcal{B}))$ holds for all F with $Supp(F) \subseteq \Delta_{\prec_w}(I)\}$.*

Remark 3 *If I and $\prec_w$ satisfy the order domain conditions then any polynomial G in any Gröbner basis $\mathcal{B}$ of I must contain exactly two monomials of highest weight. Hence, the choice of $\mathcal{B}$ is of no importance in Definition 9. This result is a consequence of Lemma 2 and the fact that the remainder is independent of the Gröbner basis chosen.*

The following proposition is an immediate generalization of similar results in Example 4.

Proposition 2 *Assume $I \subseteq \mathbf{F}_q[X_1, \ldots, X_m]$ and $\prec_w$ satisfy the order domain conditions. Consider $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$. A pair (P, N) where $P, N \in \Delta_{\prec_w}(I_q)$ is OWB if $w(P) + w(N) \in w(\Delta_{\prec_w}(I_q))$. If $K \in \Delta_{\prec_w}(I_q)$ and $P, N \in \Delta_{\prec_w}(I)$ satisfy $w(P) + w(N) = w(K)$, then $P, N \in \Delta_{\prec_w}(I_q)$, and (P, N) is OWB.*

Definition 10 *Assume I and $\prec_w$ satisfy the order domain conditions. Let $\Gamma = w(\Delta_{\prec_w}(I))$ and define for all $\lambda \in w(\Delta_{\prec_w}(I_q))$*

$$\sigma(\lambda) = \#\{\eta \in w(\Delta_{\prec_w}(I_q)) \mid \eta - \lambda \in \Gamma\}$$

and for all $\lambda \in \Gamma$

$$\mu(\lambda) = \#\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}.$$

Applying Theorem 1 and Theorem 2 in combination with Proposition 2 we get the following theorem.

Theorem 3 *Assume* I *and* $\prec_w$ *satisfy the order domain conditions. Let* L *be a subspace of* $R_q = \mathbb{F}_q[X_1, \ldots, X_m]/I_q$ *and assume*

$$\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$$

is a well-behaving basis (Definition 4). The minimum distance of $C(I, L)$ *is at least*

$$\min\{\sigma(w(lm(B_1))), \ldots, \sigma(w(lm(B_{\dim(L)})))\}.$$

The minimum distance of $C(I, L)^{\perp}$ *is at least*

$$\min\{\mu(w(M)) \mid M \in \Delta_{\prec_w}(I_q)\backslash\{lm(B_1), \ldots, lm(B_{\dim(L)})\} \\ \geq \min\{\mu(\lambda) \mid \lambda \in \Gamma\backslash\{w(B_1), \ldots, w(B_{\dim(L)})\}\}.$$

Consider the following choices of L. Let $\vec{s} \in \mathbf{N}_0^r$ and $\delta \in \mathbf{N}$.

$$L_1 = \mathrm{Span}_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), w(M) \preceq_{\mathbf{N}_0^r} \vec{s}\} \quad (19)$$
$$L_2 = \mathrm{Span}_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \sigma(w(M)) \geq \delta\} \quad (20)$$
$$L_3 = \mathrm{Span}_{\mathbb{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \mu(w(M)) < \delta\}. \quad (21)$$

Theorem 3 tells us that the minimum distance of $C(I, L_2)$ and $C(I, L_3)^{\perp}$ is at least δ. By construction $C(I, L_2)$ and $C(I, L_3)^{\perp}$ are the largest codes with prescribed minimum distance δ. We shall in Section 10 see that whenever the weights are numerical, that is whenever $\vec{s} = s$ is an integer, then the minimum distance of $C(I, L_1)$ is at least $n - s$. Here, $n = \#\Delta_{\prec_w}(I_q)$. Similarly we will derive in Section 10 a simple expression for a lower bound on the minimum distance of $C(I, L_1)^{\perp}$ whenever the weights are numerical.

Example 5 *This is a continuation of Example 1 and Example 2. Choose the weights* $w(X_1) = (1, 0, \ldots, 0)$*,* $w(X_2) = (0, 1, 0, \ldots, 0)$*,* $\ldots, w(X_m) = (0, \ldots, 0, 1) \in \mathbf{N}_0^m$*. Let* $\prec_{\mathbf{N}_0^m}$ *be the graded ordering on* $\mathbf{N}_0^m$ *with* $(1, 0, \ldots, 0) \prec_{\mathbf{N}_0^m} \cdots \prec_{\mathbf{N}_0^m} (0, \ldots, 0, 1)$*. Let* $\prec_{\mathcal{M}}$ *be any monomial ordering on* $\mathcal{M}(X_1, \ldots, X_m)$*. Using the convention that the empty set is a Gröbner basis for the ideal* $I = \langle 0 \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ *we see that the order domain conditions are trivially satisfied. The code* $C(I, L_1)$ *with* $\vec{s} = (0, \ldots, 0, s)$ *is the generalized Reed-Muller code* $RM_q(s, m)$*. Similarly, the codes* $C(I, L_2)$ *and* $C(I, L_3)^{\perp}$ *are the improved generalized Reed-Muller codes considered in Example 1 and Example 2. Applying Theorem 3 we count exactly the same OWB pairs that we count by applying Corollary 2 and Corollary 3.*

Given I and $\prec_w$ such that the order domain conditions are satisfied we might want to construct codes by evaluating in a subset $U \subsetneq \mathcal{V}_{\mathbb{F}_q}(I)$ rather than in the entire variety $\mathcal{V}_{\mathbb{F}_q}(I)$. The following remark deals with this situation

Remark 4 *Assume that the pair I and $\prec_w$ satisfies the order domain conditions. Let $U \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$. Every finite set of points is a variety and therefore there exists polynomials $H_1, \ldots, H_r$ such that the vanishing ideal of U equals*

$$I_U = I_q + \langle H_1, \ldots, H_r \rangle.$$

The estimates of the minimum distances of $C(I, L)$ and $C(I, L)^{\perp}$ still hold if these codes are made by evaluating in U rather than in the entire variety $\mathcal{V}_{\mathbb{F}_q}(I)$. All we need to do is to replace I_q with I_U in Definition 4, Definition 5, Proposition 2, Definition 10 and Theorem 3.

8 Weight functions and order domains

The concept of an order function was introduced by Høholdt et al. in [20] to simplify the treatment of one-point geometric Goppa codes and to provide a language for easy generalization of one-point geometric Goppa codes to objects of higher dimensions than curves. The concept was further developed in [33] and [17]. Here, we describe some terminology from [17].

Definition 11 *Let R be a k-algebra and let Γ be a subsemigroup of $\mathbb{N}_0^r$ for some r. Let $\prec$ be a monomial ordering on $\mathbb{N}_0^r$. A surjective map $\rho : R \rightarrow \Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ that satisfies the following six conditions is said to be a weight function*

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

A k-algebra with a weight function is called an order domain and Γ is called the value semigroup of ρ.

From [17][Th. 9.1 and Th. 10.4] we know that if the value semigroup Γ is finitely generated then it can be described in the language of Gröbner basis theory. We have the following result which connects Definition 11 to the theory of the previous section.

Theorem 4 *Let $\prec_w$ be a generalized weighted degree ordering on $\mathcal{M}(X_1, \ldots, X_m)$ and let $I \subset k[X_1, X_2, \ldots, X_m]$ be an ideal. If I and $\prec_w$ satisfy the order domain conditions (Definition 9) then $R = k[X_1, X_2, \ldots, X_m]/I$ is an order domain with a weight function defined as follows: Given a nonzero $f \in k[X_1, X_2, \ldots, X_m]/I$ write $f = F + I$ where Supp$(F) \subseteq \Delta_{\prec_w}(I)$. We have $\rho(f) = wdeg(F)$ and $\rho(0) = -\infty$.*
Any weight function with a finitely generated value semigroup Γ can be described as above.

Proof: We only show the first part of the theorem. Regarding the last part we refer to the proof in [17]. Assume I and $\prec_w$ satisfy the order domain conditions. The properties $(W.0)$, $(W.1)$, and $(W.2)$ are obviously satisfied. Given $f = F_1 + I$ and $g = F_2 + I$ with $\mathrm{Supp}(F_1) \subseteq \Delta_{\prec_w}(I)$ and $\mathrm{Supp}(F_2) \subseteq \Delta_{\prec_w}(I)$ let b be the leading coefficient of F_1 and let c be the leading coefficient of F_2. If we choose $a = b/c$ then the result in $(W.4)$ holds. Property $(W.5)$ follows immediately from Lemma 2. Finally, property $(W.3)$ is a consequence of $(W.5)$ (in fact $(W.3)$ is not needed in the definition of a weight function). The proof is complete.

As mentioned earlier the ideals and the monomial orderings considered in Example 4 and Example 5 satisfy the order domain conditions. Therefore by Theorem 4 the corresponding factor rings are order domains and the weights correspond to weight functions following Theorem 4.

9 Codes form order domains

We now describe the codes related to order domains. We will need a couple of definitions.

Definition 12 *Let R be an $\mathbb{F}_q$-algebra. A surjective map $\varphi : R \rightarrow \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$ linear and if*

$$\varphi(fg) = \varphi(f) * \varphi(g)$$

for all $f, g \in R$ (here $*$ is the componentwise product described in Section 5).

Definition 13 *Let* $\rho : R \rightarrow \Gamma \cup \{-\infty\}$ *be a weight function. A set*

$$\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$$

is called a well-behaving basis for R*.*

It is clear that all order domains possess well-behaving bases. Recall that we in Definition 4 introduced the concept of a well-behaving basis for $L \subseteq R_q$. The concept of a well-behaving basis for an order domain R as defined above is not the same. However, the two concepts are closely related.

Proposition 3 *Assume* R *is an order domain over* k*. If* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ *is a well-behaving basis for* R *then it is a basis for* R *as a vectorspace over* k*.*

Proof: For the case of weight functions with finitely generated value semigroup the result follows by combining the characterization in Theorem 4 with the result in Proposition 1. For the general case we refer to [17, Th. Pro. 3.2 and Def. 3.1]. The proof is complete.

Remark 5 *Given two well-behaving bases* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ *and* $\{g_\lambda \mid \rho(g_\lambda) = \lambda, \lambda \in \Gamma\}$ *then for all* $\eta \in \Gamma$*,* g_η *is a linear combination of the elements in* $\{f_\lambda \mid \lambda \preceq \eta\}$ *and the coefficients of* f_η *in this expression is nonzero.*

It follows from Remark 5 that it is of no importance in the next definition which well-behaving basis is considered.

Definition 14 *Let* R *be an order domain over* $\mathbb{F}_q$ *with a weight function* $\rho : R \rightarrow \Gamma \cup \{-\infty\}$ *and let* $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ *be a well-behaving basis. Let* $\varphi : R \rightarrow \mathbb{F}_q^n$ *be a morphism as in Definition 12. Define* $\alpha(1) = 0$*. For* $i = 2, \ldots, n$ *define recursively* $\alpha(i)$ *to be the smallest element in* Γ *that is greater than* $\alpha(1), \ldots, \alpha(i-1)$ *and satisfies*

$$\varphi(f_{\alpha(i)}) \notin Span_{\mathbb{F}_q}\{\varphi(f_\lambda) \mid \lambda \prec_{\mathbf{N}_0^r} \alpha(i)\}.$$

Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \ldots, \alpha(n)\}$*.*

Definition 15 *For $\lambda \in \Delta(R,\rho,\varphi)$ define*

$$\sigma(\lambda) = \#\{\gamma \in \Delta(R,\rho,\varphi) \mid \gamma - \lambda \in \Gamma\}.$$

For $\lambda \in \Gamma$ define

$$\mu(\lambda) = \#\{\alpha \in \Gamma \mid \lambda - \alpha \in \Gamma\}.$$

We can now define the codes.

Definition 16 *Let R be an order domain over $\mathbb{F}_q$ and let φ be a morphism as in Definition 12. Consider a fixed well-behaving basis $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$. For $\lambda \in \Gamma$ and $\delta \in \mathbf{N}$ consider the codes*

$$\begin{aligned}
E(\lambda) &= Span_{\mathbb{F}_q}\{\varphi(f_\eta) \mid \eta \preceq_{\mathbf{N}_0^r} \lambda\}\\
\tilde{E}(\delta) &= Span_{\mathbb{F}_q}\{\varphi(f_\eta) \mid \eta \in \Delta(R,\rho,\varphi) \text{ and } \sigma(\eta) \geq \delta\}\\
C(\lambda) &= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_\eta) = 0 \text{ for all } \eta \text{ with } \eta \preceq_{\mathbf{N}_0^r} \lambda\}\\
\tilde{C}(\delta) &= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_\eta) = 0 \text{ for all } \eta \in \Delta(R,\rho,\varphi) \text{ with } \mu(\eta) < \delta\}.
\end{aligned}$$

Remark 6 *From Remark 5 we conclude that the choice of well-behaving basis is of no importance for the definition of the codes $E(\lambda)$ and $C(\lambda)$.*

From [20, Th. 4.13 and Pro. 4.23] and [2, Th. 33] we have the following theorem. The result concerning $C(\lambda)$ and $\tilde{C}(\delta)$ is known as the order bound.

Theorem 5 *The minimum distance of $E(\lambda)$ is at least*

$$\min\{\sigma(\eta) \mid \eta \preceq_{\mathbf{N}_0^r} \lambda\} \tag{22}$$

and the minimum distance of $C(\lambda)$ is at least

$$\min\{\mu(\eta) \mid \lambda \prec_{\mathbf{N}_0^r} \eta \text{ and } \eta \in \Delta(R,\rho,\varphi)\} \geq \min\{\mu(\eta) \mid \lambda \prec_{\mathbf{N}_0^r} \eta\}. \tag{23}$$

The minimum distances of $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ are at least δ.

Recall from Theorem 4 that if Γ is a finitely generated value semigroup then the corresponding order domain R can be described as a factor ring. We now show that for such order domains Theorem 5 is a direct consequence of the theory developed in Section 7. We start with the following easy characterization of φ.

Proposition 4 *Let $\varphi : R = \mathbb{F}_q[X_1, \ldots, X_m]/I \rightarrow \mathbb{F}_q^n$ be a morphism as in Definition 12. There exists a set*

$$U = \{P_1, \ldots, P_n\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$$

such that $\varphi(F + I) = (F(P_1), \ldots, F(P_n))$ for all $F + I \in R$. The P_i's are pairwise different.

Applying Proposition 4 to order domains with finitely generated value semigroup we see that the codes in Definition 16 are of the type covered by Remark 4 of Section 7. Rather than dealing with the general case $U \subseteq \mathcal{V}_{\mathbb{F}_q}(I)$ we will in the following concentrate on the situation $U = \mathcal{V}_{\mathbb{F}_q}(I)$. The reader can easily generalize our findings by replacing, as in Remark 4, any occurrence of I_q with I_U.
Our most important observation is that

$$\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q)). \tag{24}$$

To show (24) we start by noting that both sets are of size n. Hence, (24) must hold if we can show

$$\Delta(R, \rho, \varphi) \subseteq w(\Delta_{\prec_w}(I_q)).$$

Clearly, $\alpha(1) = 0$ is in $w(\Delta_{\prec_w}(I_q))$ as any non-empty footprint contains 1. Aiming for a contradiction assume $\alpha(i) \notin w(\Delta_{\prec_w}(I_q))$ for some $2 \leq i \leq n$. Let $f_{\alpha(i)} = F + I$, $w(\mathrm{lm}(F)) = \alpha(i)$. We have

$$\varphi(F + I) = \varphi(F \text{ rem } \mathcal{G} + I) \tag{25}$$

where $\mathcal{G}$ is a Gröbner basis for I_q. The very definition of a Gröbner basis ensures that $\mathrm{lm}(F \text{ rem } \mathcal{G}) \in \Delta_{\prec_w}(I_q)$. Hence, $\mathrm{lm}(F \text{ rem } \mathcal{G}) \prec_w \mathrm{lm}(F)$. But then, by (25) and Definition 14, $\alpha(i) \notin \Delta(R, \rho, \varphi)$. We have reached at a contradiction and therefore (24) holds.
With (24) in hand we establish the following connections: $E(\lambda)$ and $C(\lambda)$ respectively equals $C(I, L_1)$ and $C(I, L_1)^\perp$ respectively where L_1 is as in (19). $\tilde{E}(\delta)$ equals $C(I, L_2)$ where L_2 is as in (20) and $\tilde{C}(\delta)$ equals $C(I, L_3)^\perp$ where L_3 is as in (21). We conclude that the bounds in Theorem 5 on the minimum distances of $E(\lambda)$, $\tilde{E}(\delta)$, $C(\lambda)$ and $\tilde{C}(\delta)$ are consequences of Theorem 3.

10 One-point geometric Goppa codes

One of the main reasons for introducing order domains in [20] was to have an easy description of one-point geometric Goppa codes and to have an easy way of generalizing the construction of one-point geometric Goppa codes to algebraic structures of higher transcendence degree. Presenting in the present paper things in reverse order of what is normally done we now finally come to the one-point geometric Goppa codes.
Let $\mathcal{P}$ be a rational place in an algebraic function field $\mathbb{F}$ of one variable with constant field $\mathbb{F}_q$. Let $\nu_{\mathcal{P}}$ be the valuation corresponding to $\mathcal{P}$. Consider the algebraic structure

$$R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P}). \tag{26}$$

Defining $\rho = -\nu_{\mathcal{P}}$ we have $\rho(R) = \Gamma \cup \{-\infty\}$ where $\Gamma \subseteq \mathbf{N}_0$ is known as the Weierstrass semigroup corresponding to $\mathcal{P}$. By inspection the map $\rho : R \rightarrow \Gamma \cup \{-\infty\}$ satisfies the six conditions in Definition 11 and therefore is a weight function.
Unfortunately it is not in general an easy task to determine the structure R above and therefore it is often difficult to find the factor ring description of R as guaranteed by Theorem 4. Observe, that one such description was given in Example 4 in the case of a Hermitian curve over $\mathbb{F}_9$.
The geometric Goppa codes coming from the structure in (26) are known as one-point geometric Goppa codes. We now explain the connection between these codes and the affine variety codes in Section 7. Let $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ be rational places, pairwise different, and all different from $\mathcal{P}$. The map $\varphi : R \rightarrow \mathbb{F}_q^n$, $\varphi(f) = (f(\mathcal{Q}_1), \ldots, f(\mathcal{Q}_n))$ is a morphism as in Definition 12. Therefore from Proposition 4 the rational places $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ correspond to n different affine points $P_1, \ldots, P_n$ in $\mathcal{V}(I_q)$ and $\varphi(F+I) = (F(P_1), \ldots, F(P_n))$ holds. We have

$$C_{\mathcal{L}}(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, \lambda\mathcal{P}) = C(I, L)$$

and

$$C_{\Omega}(\mathcal{Q}_1 + \cdots + \mathcal{Q}_n, \lambda\mathcal{P}) = C(I, L)^{\perp}$$

where

$$L = \{f \in R \mid \rho(f) \leq \lambda\}.$$

Let $\Gamma = \{\lambda_1, \lambda_2, \ldots\}$ where $\lambda_1 < \lambda_2 < \cdots$ holds. The Goppa bounds from algebraic geometry applied to the case of one-point geometric Goppa codes state.

Theorem 6 *Let $\mathcal{P}$ be a rational place as above and let R be the corresponding order domain as in (26). The minimum distance of $E(\lambda)$ is at least*

$$n - \lambda. \tag{27}$$

The minimum distance of $C(\lambda_t)$ is at least

$$t + 1 - g. \tag{28}$$

Now we show that the bounds in Theorem 6 can be viewed as being a consequence of Theorem 5. We will need the following technical lemma from [20, Lem. 5.15 and Th. 5.24].

Lemma 3 *Let $\Gamma = \{\lambda_1, \lambda_2, \ldots\}$ with $\lambda_1 < \lambda_2 < \cdots$ be a semigroup in $\mathbf{N}_0$ with finitely many gaps. Define*

$$g(i) = \#\{\lambda \in \mathbf{N}_0 \backslash \Gamma \mid \lambda < \lambda_i\}.$$

For any λ_i we have $\#(\Gamma \backslash (\lambda_i + \Gamma)) = \lambda_i$ and $\mu(\lambda_i) = i - g(i) + D(i)$ where

$$D(i) = \{(x, y) | x, y \in \mathbf{N}_0 \backslash \Gamma \text{ and } x + y = \lambda_i\}.$$

Here, $\lambda + \Gamma$ means $\{\lambda + \lambda_1, \lambda + \lambda_2, \ldots\}$.

Theorem 7 *For the case of one-point geometric Goppa codes the bound in (22) is always at least as good as (and sometimes better than) the bound in (27). Similarly, the bound in (23) is always at least as good as (and sometimes better than) the bound in (28).*

Proof: To prove the first claim we need only consider numbers $\lambda_i \in \Delta(R, \rho, \varphi)$, $\lambda_i \leq s$. We have $\sigma(\lambda_i) = \#(\Delta(R, \rho, \varphi) \cap (\lambda_i + \Gamma))$. From the first part of Lemma 3 we see that the number of elements in $\Delta(R, \rho, \varphi)$ that are not in $\lambda_i + \Gamma$ is at most λ_i. Therefore $\sigma(\lambda_i) \geq n - \lambda_i$ holds with equality only when $\Gamma \backslash (\lambda_i + \Gamma) \subseteq \Delta(R, \rho, \varphi)$. We conclude $\min\{\sigma(\lambda_i) \mid \lambda_i \in \Delta(R, \rho, \varphi), \lambda_i \leq s\} \geq n - s$. Concerning the last claim we have

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

with equality if and only if $\lambda_{t+1} = \lambda_t + 1$, $g(t+1) = g$ and $\#D(t+1) = 0$ hold. The proof is complete.

Having shown that the bounds in Theorem 5 on the minimum distances of the codes $E(\lambda)$ and $C(\lambda)$ are at least as good as the Goppa bounds in the case of R being of the form (26) it is clear that we can consider the codes $\tilde{E}(\delta)$ and the codes $\tilde{C}(\delta)$ related to (26) as improved one-point geometric Goppa codes.
It was shown in [27, Th. 1] that all numerical weight functions (i. e. weight functions with weights in $\mathbb{N}_0$) are either of the form (26) or is a sub algebra of such a structure. Turning to semigroups that are not numerical the related structures are no longer curves but are higher dimensional [17, Sec. 11]. The related codes can be viewed as generalizations of one-point geometric Goppa codes.

11 Bibliographical Notes

The theory of evaluation codes has grown relatively large in its ten years' lifetime and therefore it is not possible to give a full list of references on the topic in the present paper. Instead we will give just a few references on different aspects of the theory.
Examples of evaluation codes coming from higher dimensional objects than curves are given in [25] and [2]. Regarding generalized Hamming weights of evaluation codes more results can be found in [19], [3], [2], and [18]. The Feng-Rao bound as described in [11], [12], and [24] is more general than the order bound [20] in that it does not only deal with evaluation codes. The most general version of the Feng-Rao bound deals with linear codes [29], [18]. The Gröbner basis theoretical point of view on order domains are studied in [30], [31], [28], [33], [21], and [17]. Evaluation codes are described in a Gröbner basis theoretical setting in [30], [31], [1], and [2]. For the case of affine variety codes decoding algorithms can be found in [13], [10], [32]. Many papers deal with decoding of evaluation codes. Among these are [20], [6], and [16]. A study of the function μ on different families of semigroups Γ can be found in [5] and [34].

References

[1] H. E. Andersen, Codes from Order Domains, *PhD Report Series,* **12**, (2005.)

[2] H. E. Andersen and O. Geil, Evaluation codes from order domain theory, *Finite Fields and Their Applications,* **14**, (2008), pp. 92-123.

[3] A. I. Barbero and C. Munuera, The Weight Hierarchy of Hermitian Codes, *SIAM Journ. Discr. Math.,* **13**, (2000), pp. 79-104.

[4] T. Becker and V. Weispfenning, “Gröbner Bases - A Computational Approach to Commutative Algebra,” Springer Verlag, Berlin, (1993).

[5] M. Bras-Amorós, Acute Semigroups, the Order Bound on the Minimum Distance, and the Feng-Rao Improvements, *IEEE Trans. Inform. Theory,* **50**, (2004), pp. 1282-1289.

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

[7] D. Cox, J. Little, and D. O'Shea, “Ideals, Varieties, and Algorithms, 2nd ed.,” Springer, Berlin, (1997).

[8] D. Cox, J. Little, and D. O'Shea, “Using Algebraic Geometry,” Springer, Berlin, (1998).

[9] P. Delsarte, J. M. Goethals, and F. J. Mac Williams, On generalized Reed-Muller codes and their relatives, *Information and Control*, **16**, (1970), 403-442.

[10] J. B. Farr and S. Gao, Gröbner bases Padé approximation and decoding of linear codes, *Proc. of Coding theory and quantum computing (Virginia 2003), Contemp. Math.,* **381**, Amer. Math. Soc. (2005), pp. 3-18.

[11] G.-L. Feng and T.R.N. Rao, Decoding of algebraic geometric codes up to the designed minimum distance, *IEEE Trans. Inf. Theory*, **39**, (1993), pp. 37-46.

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

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

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

[15] 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), p. 331.

[16] O. Geil and R. Matsumoto, Generalized Sudan's List Decoding for Order Domain Codes, *Proc. of AAECC-17, Lecture Notes in Comput. Sci. 4851*, Springer, Berlin, (2007), pp. 50-59.

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

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

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

[20] 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.

[21] R. Pellikaan, On the existence of order functions, *Journal of Statistical Planning and Inference,* **94**, (2001), pp. 287-301.

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

[23] T. Kasami, S. Lin, and W. Peterson, New generalizations of the Reed-Muller codes. I. Primitive codes, *IEEE Transactions on Information Theory*, **14**, (1968), pp. 189-199.

[24] M. S. Kolluru, G. L. Feng, and T. R. N. Rao, Construction of Improved Geometric Gopps Codes from Klein Curves and Klein-like Curves, *Applicable Algebra in Engineering, Communication and Computing*, **10**, (2000), pp. 433-464.

[25] 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.

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

[27] 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.

[28] R. Matsumoto and S. Miura, On Construction and Generalization of Algebraic Geometry Codes, textitProc. of Algebraic Geometry, Number Thoery, Coding Theory and Cryptography, Univ. of Tokyo, January 19-20, 2000, (Ed. T. Katsura et al.), (2000) pp. 3-15.

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

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

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

[32] E. Orsini and M. Sala, Improved Decoding of Affine-Variety Codes, *BCRI preprint*, www.bcri.ucc.ie, University College Cork, Boole Centre BCRI, UCC Cork, Ireland, (2007).

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

[34] D. Ruano, Computing the Feng-Rao Distances for Codes from Order Domains, *Journ. of Algebra,*, **309**, (2007), pp. 672-682.