Affine Variety Codes and Order Domain Codes

Olav Geil, Aalborg University

Lecture Notes for: "Gröbner Bases, Geometric Codes and Order Domains," University of Trento, June 8-13, 2009

1 Notation and background material

$$\begin{aligned} I &= \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle \subseteq \mathbf{F}_q[\vec{X}] \\ \\ I_q &= I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle \\ &= \langle F_1(\vec{X}) \ldots, F_s(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle \\ \\ R &= \mathbf{F}_q[\vec{X}]/I \\ \\ R_q &= \mathbf{F}_q[\vec{X}]/I_q \end{aligned}$$

If we write $\mathbf{V}_{\mathbf{F}_q}(I_q) = \{P_1, \ldots, P_n\}$, then we know from Max's introduction that the map ev : $R_q \mapsto \mathbf{F}_q^n$ given by $\mathrm{ev}(F + I) = (F(P_1), \ldots, F(P_n))$ is a vector space isomorphism. It extends naturally to a surjective vector space homomorphism ev : $R \mapsto \mathbf{F}_q^n$.

In this course we shall consider codes of the form $\mathrm{ev}(L)$ and $(\mathrm{ev}(L))^\perp$ where $L \subseteq R_q$ or $L \subseteq R$. When working with these codes the following results will be useful.

From Max's introduction we know that $\{M + I \mid M \in \Delta_\prec(I)\}$ is a basis for R. This in particular holds for $I = I_q$, in which case of course $R = R_q$. Here, $\Delta_\prec(I)$ is the set of monomials that can not be found as leading monomials of any polynomial in I.
Also from Max's introduction we know that for general ideal $J \subseteq \mathbf{F}_q[\vec{X}]$ the size of a variety is bounded above by the size of the corresponding footprint. That is, we have the footprint bound:

$$\#\mathbf{V}_{\mathbf{F}_q}(J) \leq \#\Delta_\prec(J). \tag{1}$$

In case J contains $X_1^q - X_1, \ldots, X_m^q - X_m$ then equality holds in (1).

2 Reed-Solomon codes, Generalized Reed-Muller codes and Hyperbolic codes

2.1 (Generalized) Reed-Solomon codes

Write $\mathbf{F}_q = \{P_1, \ldots, P_{n=q}\}$ and define

$$\mathrm{RS}_k = \{(F(P_1), \ldots, F(P_n)) \mid F \in \mathbf{F}_q[X], \deg(F) < k\}$$

If $k \leq n$ then $\dim(\mathrm{RS}_k) = k$ and $d(\mathrm{RS}_k) = n - k + 1$.
Generator matrix is

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ P_1 & P_2 & \cdots & P_n \\ \vdots & \vdots & \ddots & \vdots \\ P_1^{k-1} & P_2^{k-1} & \cdots & P_n^{k-1} \end{bmatrix}$$

Proof: Assume

$$(F_1(P_1), \ldots, F_1(P_n)) = (F_2(P_1), \ldots, F_2(P_n))$$

where $\deg(F_1), \deg(F_2) < k \leq n$. $F_1 - F_2$ now is a polynomial of degree less than n having n zeros. Hence, it is the zero polynomial. This explains the dimension.
A non-zero polynomial of degree less than k can have at most $k-1$ zeros. Hence, minimum distance is at least $n - (k-1) = n - k + 1$. This gives a lower bound on the minimum distance. The polynomial

$$\prod_{i=1}^{k-1} (X - P_i)$$

has $k - 1$ zeros and we see that the bound is sharp.

2.2 Generalized Reed-Muller codes

We consider polynomials in $\mathbf{F}_q[X_1, \ldots, X_m]$ which we evaluate in the points $\mathbf{F}_q^m = \{P_1, \ldots, P_{n=q^m}\}$ (every point is an m-tuple).

$$\begin{aligned} \mathrm{RM}_q(s, m) &= \{(F(P_1), \ldots, F(P_n)) \mid \deg(F) \leq s\} \\ &= \{(F(P_1), \ldots, F(P_n)) \mid \deg(F) \leq s \\ &\qquad \text{and } \ 0 \leq \deg_{X_1}(F), \ldots, \deg_{X_m}(F) < q\} \end{aligned}$$

Length is $n = q^m$. Dimension is

$$k = \#\{(i_1, \ldots, i_m) \mid i_1 + \cdots + i_m \leq s, 0 \leq i_1, \ldots, i_m < q\}.$$

For $0 \leq s \leq m(q-1)$ write $s = a(q-1) + b$ with $0 \leq b < q - 1$. Minimum distance is $(q-b)q^{m-a-1}$.

Proof of minimum distance: Let $\vec{c} \in \mathrm{RM}_q(s,m)\backslash\{\vec{0}\}$ then $\vec{c} = (F(P_1), \ldots, F(P_n))$ for some non-zero polynomial with leading monomial say $X_1^{i_1} \cdots X_m^{i_m}$. We have $i_1 + \cdots + i_m \leq s$ and $i_1, \ldots, i_m < q$. The number of non-zeros in $\vec{c}$ is

$$\begin{aligned} & n - \#\Delta_{\prec}(\langle X_1^q - X_1, \ldots, X_m^q - X_m, F(\vec{X})\rangle) \\ \geq\ & q^m - \#\Delta_{\prec}(\langle X_1^q, \ldots, X_m^q, X_1^{i_1} \cdots X_m^{i_m}\rangle) \\ =\ & (q-i_1)\cdots(q-i_m). \end{aligned} \tag{2}$$

Minimum value of (2) is attained "on the border". That is, when as many i_s as possible equal $q-1$ and only one other is different from zero. This proves that the minimum distance is at least as what is claimed. That it is not larger follows from the fact that

$$\Big(\prod_{i=1}^{a}\big(\prod_{s=1}^{q-1}(X_i - \alpha_s)\big)\Big)\big(\prod_{t=1}^{b}(X_m - \alpha_t)\big)$$

has exactly $(q-i_1)\cdots(q-i_m)$ non-zeros. Here, $\{\alpha_1, \ldots, \alpha_q\} = \mathbf{F}_q$.

Example 1 *In this example we consider $RM_3(2,2)$. The points are $\mathbf{F}_3^2 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$ and therefore the code $RM_3(2,2)$ is of length $n = 9$. Counting the number of monomials of total degree at most 2 we find that the dimension is $k = 6$. From previous theory we find that minimum distance is $d = 3$. Generator matrix is*

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Example 2 *In this example we consider Generalized Reed-Muller codes $RM_8(s,2)$. In the proof for the minimum distance we used the fact that $ev(F(X,Y))$ has Hamming weight at least $n - \#\Delta_{\prec}(\langle X^8, Y^8, lm(F)\rangle = (8-i)(8-j)$, when $lm(F) = X^iY^j$. These numbers are listed in the table below.*

Y^7	8	7	6	5	4	3	2	1
Y^6	16	14	12	10	8	6	4	2
Y^5	24	21	18	15	12	9	6	3
Y^4	32	28	24	20	16	12	8	4
Y^3	40	35	30	25	20	15	10	5
Y^2	48	42	36	30	24	18	12	6
Y	56	49	42	35	28	21	14	7
1	64	56	48	40	32	24	16	8
	1	X	X^2	X^3	X^4	X^5	X^6	X^7

We get codes with the following values of the parameters $[k,d]$: $[1,64], [3,56], [6,48], [10,40], [15,32], [21,24], [28,16], [36,8], [43,7], [49,6], [54,5], [58,4], [61,3], [63,2], [64,1]$

2.3 Hyperbolic codes

The hyperbolic codes are improved Generalized Reed-Muller codes. Therefore again we consider polynomials in $\mathbf{F}_q[X_1, \ldots, X_m]$ which we evaluate in the points $\mathbf{F}_q^m = \{P_1, \ldots, P_{n=q^m}\}$ (every point is an m-tuple).

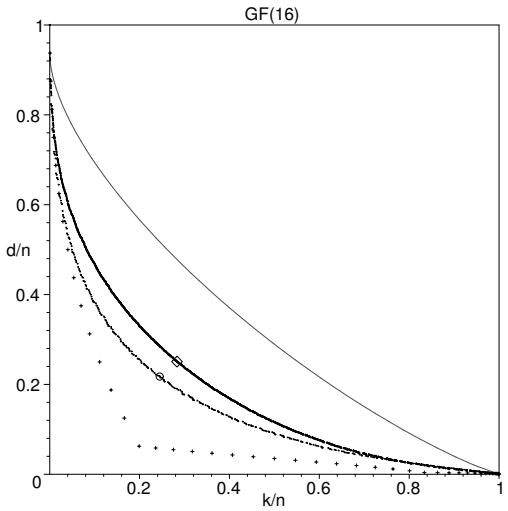
$$\begin{aligned} \mathrm{Hyp}_q(s,m) &= \mathrm{Span}_{\mathbf{F}_q}\{\mathrm{ev}(X_1^{i_1}\cdots X_m^{i_m}) \mid \prod_{s=1}^{m}(q-i_s) \geq q^m - s \\ &\qquad \text{and } \ 0 \leq i_1, \ldots, i_m < q\} \end{aligned}$$

Minimum distance is $d\Big(Hyp_s(s,m)\Big) = q^m - s$. There exists closed formula bounds for the dimensions in terms of n and d. Calculating the exact dimensions is a job for a computer.

Proof of minimum distance: Let $\vec{c} \in \mathrm{Hyp}_q(s,m)\backslash\{\vec{0}\}$ then $\vec{c} = (F(P_1)\ldots, F(P_n))$ for some non-zero polynomial F with leading monomial say $X_1^{i_1}\cdots X_m^{i_m}$. We have $\prod_{s=1}^{m}(q-i_s) \geq q^m - s$ and $i_1, \ldots, i_m < q$. From previous proof (subsection on Generalized Reed-Muller codes) we have that Hamming weight is at least $q^m - s$. We can find particular codeword having this weight and we are through.

Example 3 *This is a continuation of Example 2. Looking up the table there we find that* $RM_8(7,2)$ *is an* $[n = 64, k = 36, d = 8]$ *code whereas there are hyperbolic codes with parameters* $[64, 48, 8], [64, 35, 15]$ *and* $[64, 37, 14]$.

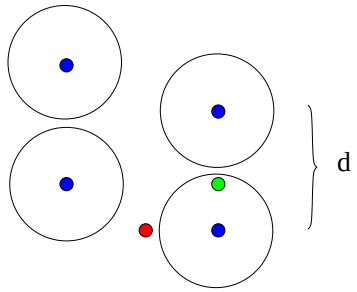
Example 4 *In this example we compare the codes* $RM_{16}(s,3)$ *with the codes* $Hyp_{16}(s,3)$. *These codes are all of length* $n = 4096$. *The performance of the first one are marked with* $+$*'s. The hyperbolic codes are the ones marked with a* $\circ$



3 The second weight of Generalized Reed-Muller codes

To get a complete picture of how good a code performs under maximum likelihood decoding one needs a complete picture of the distances in the code. For

linear codes this corresponds to a complete picture of the Hamming weights.



This motivates why we are interested in finding the second smallest Hamming weight that occurs in the Generalized Reed-Muller code. We consider here only the case $s < q$ and we state the result in the language of number of zeros of a polynomial rather than in the language of Hamming weight.

Proposition 1 *Let $F(X_1, \ldots, X_m) \in \mathbf{F}_q[X_1, \ldots, X_m]$ be of total degree s where $2 \leq s < q$ and $2 \leq m$. Then either $F(\vec{X})$ has sq^{m-1} zeros or it has at most $sq^{m-1} - (s-1)q^{m-2}$ zeros.*

Before proving Proposition 1 we give a definition and state a few results that will be useful to us.

Definition 1 *Consider an ideal $\langle G_1(\vec{X}), \ldots, G_v(\vec{X})\rangle$. Then*

$$R(G_i, G_j) := S(G_i, G_j) \quad rem \quad (G_i, \ldots, G_v)$$

Here, $S(G_i, G_j)$ is the S-polynomial introduced by Max and rem $(G_i, \ldots, G_v)$ means remainder modulo the ordered set $(G_i, \ldots, G_v)$.

Remark 1 *$R(G_i, G_j) \in \langle G_1, \ldots, G_v\rangle$ and if $R(G_i, G_j) \neq 0$ then $lm(R(G_i, G_j)) \preceq lm(S(G_i, G_j))$.*

Lemma 1 *Let $2 \leq m$ and $2 \leq s < q$. Consider tuples $(i_1, \ldots, i_m) \in \mathbf{N}_0^m$ such that $i_1, \ldots, i_m < s$ and $i_1 + \cdots + i_m = s$. The minimal value of $\prod_{l=1}^m (q - i_l)$ is $q^m - sq^{m-1} + (s-1)q^{m-2}$.*

Lemma 2 *Let $2 \leq m$ and $2 \leq s < q$. Consider tuples $(i_1, \ldots, i_m) \in \mathbf{N}_0^m$ such that $i_1 < s$, $i_2, \ldots, i_m < q$ and $i_1 + \cdots + i_m = q$. The minimal value of*

$$(s - i_1) \prod_{l=2}^{m} (q - i_l)$$

is $(s-1)q^{m-2}$.

Proof of Proposition 1
Let $\prec$ be the total degree lexicographic ordering and let $\mathrm{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$.

We have $i_1 + \cdots + i_m = s$.
Assume first that $0 \leq i_1 < s, \ldots, 0 \leq i_m < s$ holds. We get

$$\begin{aligned} & \#\Delta_{\prec}(\langle F(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle) \\ \leq & \#\Delta_{\prec}(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q \rangle) \\ = & q^m - \prod_{l=1}^{m} (q - i_l) \end{aligned}$$

Lemma 1 now applies.
Assume finally w.l.o.g. $i_1 = s$, $i_2 = \cdots = i_m = 0$ and $\mathrm{lc}(F) = 1$. Recall, from Max's introduction that Buchberger's algorithm extends a basis for an ideal to a Gröbner basis in the following way. It calculates all possible S-polynomials between basis elements and then it reduces them modulo the basis. Every time a non-zero remainder is found it is added to the basis. When eventually at some point all S-polynomials can be reduced to zero then the basis is a Gröbner basis. A usefull lemma tells us that whenever $\gcd(\mathrm{lm}(G_1), \mathrm{lm}(G_2)) = 1$ we have $S(G_1, G_2) \ \mathrm{rem} \ (G_1, G_2) = 0$. Hence, to check if $\{F, X_1^q - X_1, \ldots, X_m^q - X_m\}$ is a Gröbner basis we consider in the first iteration of Buchberger's algorithm only the polynomial

$$\begin{aligned} H(\vec{X}) & := S(X_1^q - X_1, F(\vec{X})) \\ & = X_1^q - X_1 - X_1^{q-s} F(\vec{X}) \end{aligned}$$

Observe that the total degree of H is at most q. Following Buchberger's algorithm we then reduce $H(\vec{X}$ modulo $(F, X_1^q - X_1, \ldots, X_m^q - X_m)$ to get the remainder $R(\vec{X})$. If $R(\vec{X})$ equals 0 then $\{F, X_1^q - X_1, \ldots, X_m^q - X_m\}$ is a Gröbner basis. According to the footprint bound F then has precisely sq^{m-1} zeros. If the remainder is non-zero then we consider its leading monomial, say $X_1^{v_1} \cdots X_m^{v_m}$ (we do not proceed with Buchberger's algorithm in this case). We have $0 \leq v_1 < s$, $0 \leq v_2 < q, \ldots, 0 \leq v_m < q$ and $v_1 + \cdots + v_m \leq q$ holds by Remark 1 and the choice of ordering (the total degree ordering). We have

$$\begin{aligned} & \#\Delta_{\prec}(\langle F(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle) \\ \leq & \#\Delta_{\prec}(\langle X_1^s, X_2^q, \ldots, X_m^q, X_1^{v_1} \cdots X_m^{v_m} \rangle) \\ = & sq^{m-1} - (s - v_1) \prod_{i=2}^{m} (q - v_i) \end{aligned}$$

Lemma 2 now applies. One can easily find a polynomial with the prescribed number of zeros.

4 Codes from Norm-Trace Curves

We will consider codes from the norm-trace polynomial

$$X^{\frac{q^r-1}{q-1}} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y^q - Y.$$

We write $I = \langle X^{\frac{q^r-1}{q-1}} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y^q - Y \rangle$. The norm map $N : \mathbf{F}_{q^r} \to \mathbf{F}_q$ is given by $N(\alpha) = \alpha^{(q^r-1)/(q-1)}$ and the trace map is given by $Tr : \mathbf{F}_{q^r} \to \mathbf{F}_q$ $Tr(\beta) = \beta^{q^{r-1}} + \beta^{q^{r-2}} + \cdots + \beta^q + \beta$. Hence, the name of the norm-trace polynomial is justified. It is well-known that for every $\gamma \in \mathbf{F}_q$ there are exactly q^{r-1} $\beta \in \mathbf{F}_{q^r}$ with $Tr(\beta) = \gamma$. Hence, the size of the variety $\mathcal{V}(I_{q^r})$ is $q^r q^{r-1} = q^{2r-1}$. Combining this observation with the footprint bound we see that $\#\Delta_\prec(I_{q^r}) = q^{2r-1}$. Hence, if we choose a monomial ordering with $X^{\frac{q^r-1}{q-1}} \prec Y^{q^{r-1}}$ then $\{X^{\frac{q^r-1}{q-1}} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y^q - Y, X^{q^r} - X, Y^{q^r} - Y\}$ becomes a Gröbner basis. For such a monomial ordering we get

$$\Delta_\prec(I_{q^r}) = \{X^i Y^j \mid 0 \leq i < q^r, 0 \leq j < q^{r-1}\}$$

and therefore

$$\{X^i Y^j + I_{q^r} \mid 0 \leq i < q^r, 0 \leq j < q^{r-1}\}$$

constitutes a basis for $R_{q^r} = \mathbf{F}_{q^r}[X,Y]/I_{q^r}$.

We now choose a particular monomial ordering. Namely, the weighted degree lexicographic ordering given as follows. First we write $W(X^iY^j) = i \cdot q^{r-1} + j \cdot \frac{q^r-1}{q-1}$. We now have $X^{i_1}Y^{j_1} \prec_w X^{i_2}Y^{j_2}$ iff one of the following conditions holds:

- $w(X^{i_1}Y^{j_1}) < w(X^{i_2}Y^{j_2})$
- $w(X^{i_1}Y^{j_1}) = w(X^{i_2}Y^{j_2})$ but $j_1 < j_2$.

Example 5 *Consider the Norm-Trace polynomial $X^3+Y^2+Y \in \mathbf{F}_4[X,Y]$ We have $I_4 = \langle X^3 + Y^2 + Y, X^4 + X, Y^4 + Y \rangle$ and $\mathbf{V}(I_4) = \{P_1, \ldots, P_8\}$. The developed theory tells us that $R_4 = \mathbf{F}_4[X,Y]/I_4$ has basis*

$$\{1 + I_4, X + I_4, Y + I_4, X^2 + I_4, XY + I_4, X^3 + I_4, X^2Y + I_4, X^2Y + I_4\}$$

(the corresponding weights are: $\{0,2,3,4,5,6,7,9\}$)
Consider the code

$$E(3) = Span_{\mathbf{F}_4}\{ev(1 + I_4), ev(X + I_4), ev(Y + I_4)\}$$

Here, the map ev corresponds to evaluation in the 8 points. We will show that $E(3)$ has minimum distance at least 5.
To this end, let $\vec{c} \in E(3) \backslash \{\vec{0}\}$. Then $\vec{c} = ev(F)$ for some $F = a_0 + a_1X + a_2Y$ where not all a_i's are equal to zero. Recall, that $w_H(\vec{c}) = n - \#\Delta_{\prec_w}(I_4 + \langle F \rangle)$.
Case 1: If $lm(F) = 1$ then $\Delta_{\prec_w}(I_4 + \langle F \rangle) \subseteq \Delta_{\prec_w}(\langle X^4, Y^2, 1 \rangle) = \emptyset$. Hence, $w_H(\vec{c}) \geq 8$.
Case 2: If $lm(F) = X$ then $\Delta_{\prec_w}(I_4 + \langle F \rangle) \subseteq \Delta_{\prec_w}(\langle X, Y^2 \rangle) = \{1, Y\}$. Hence, $w_H(\vec{c}) \geq 6$.
Case 3: If $lm(F) = Y$ we need a more involved analysis. Observe, that

$$\Delta_{\prec_w}(I_4 + \langle F \rangle) \subseteq \Delta_{\prec_w}(I_4) \backslash lm(\langle F, X^3 + Y^2 + Y \rangle)$$

We therefore have

$$\begin{aligned} w_H(\vec{c}) &\geq n - (\#\Delta_{\prec_w}(I_4) - \#\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle)) \\ &= \#\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle) \end{aligned}$$

The set $\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle)$ *clearly contains* Y, XY, X^2Y *and* X^3Y. *We now show that it actually also contains* X^3. *To see this simply observe that* $(a_0+a_1X+Y^2)\cdot Y$ *rem* $X^3+Y^2+Y = (a_0+1)Y + a_1XY + X^3$. *So no matter what is* a_0 *and* a_1 *we have* X^3 *in the considered set. We conclude* $w_H(\vec{c}) \geq 5$.

Remark 2 *We make the following very important observation which holds for general norm-trace polynomials. Firstly. the norm-trace polynomial has exactly two monomials of highest weight in its support. Secondly, the monomials in* $\Delta_{\prec_w}(I_{q^r})$ *are all of different weights. The first observation implies that if we consider a polynomial* $F(X,Y)$ *with* $Supp(F) \subseteq \Delta_{\prec_w}(I_{q^r})$ *then it will have a unique monomial of highest weight (which will of course be the leading monomial). Combining this fact with the second observation we see, that whenever we reduce* F *modulo the norm-trace polynomial the weight of the leading monomial will not change (but the leading monomial itself may).*

Example 6 *This is a continuation of Example 5. The above remark implies that we can detect the size of* $\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle)$ *simply by considering weights.*
Case 1: Let $lm(F) = 1$. *We have* $w(lm(F)) = w(1) = 0$. *Hence,*

$$\begin{aligned} \#\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle) \geq \\ \#\{0+0, 0+2, 0+3, 0+4, 0+5, 0+6, 0+7, 0+9\} = 8 \end{aligned}$$

Case 2: Let $lm(F) = X$. *We have* $w(lm(F)) = w(X) = 2$. *Hence,*

$$\begin{aligned} \#\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle) \geq \\ \#\{2+0, 2+2, 2+3, 2+4, 2+5, 2+7\} = 6 \end{aligned}$$

Case 3: Let $lm(F) = Y$. *We have* $w(lm(F)) = w(Y) = 3$. *Hence,*

$$\begin{aligned} \#\Delta_{\prec_w}(I_4) \cap lm(\langle F, X^3+Y^2+Y\rangle) \geq \\ \#\{3+0, 3+2, 3+3, 3+4, 3+6\} = 5 \end{aligned}$$

Example 7 *In this Example we use the technique from the previous example to deal with codes defined from* $X^4 - Y^3 - Y \in \mathbf{F}_9[X,Y]$. *We have*

$$\Delta_{\prec_w}(I_9) = \{X^iY^j \mid 0 \leq i < 9, 0 \leq j < 3\}$$

In the table below we list the corresponding weights w *and something that we call* $\sigma(w)$. *We have* $\sigma(\lambda) := \#\Big(\Delta_{\prec_w}(I_9) \cap (\lambda + w(\Delta_{\prec_w}(I_9)))\Big)$. *Here,* $\lambda + w(\Delta_{\prec_w}(I_9)) = \{\lambda+\gamma \mid \gamma \in w(\Delta_{\prec_w}(I_9))\}$. *Define corresponding codes by*

w	0	3	4	6	7	8	9	10	11
$\sigma(w)$	27	24	23	21	20	19	18	17	16
w	12	13	14	15	16	17	18	19	20
$\sigma(w)$	15	14	13	12	11	10	9	8	7
w	21	22	23	24	25	26	28	29	32
$\sigma(w)$	6	6	4	3	4	3	2	2	1

$$E(s) = Span_{\mathbf{F}_9}\{ev(X^iY^j + I_9) \mid X^iY^j \in \Delta(I_9), w(X^iY^j) \leq s\}$$

We have $d(E(12))$ *is* $[n = 27, k = 10, d \geq 15]$ *and* $d(E(24))$ *is* $[n = 27, k = 22, d \geq 3]$.
We could construct an improved code by leaving out $w = 24$ *and including instead* $w = 25$. *This would produce a code with parameters* $[n = 27, k = 22, d \geq 4]$.

5 The affine variety code $C(I, L)$

Let I be any ideal in $\mathbf{F}_q[\vec{X}]$, and let I_q be defined as usual. Let $\mathcal{V}(I_q) = \{P_1, \ldots, P_n\}$. Given a subspace $L \subseteq R_q$ we denote $C(I, L) = \mathrm{ev}(L)$. Such a code is called an affine variety code. Observe, that all codes considered so far are examples of affine variety codes (the Generalized Reed-Muller codes and the Hyperbolic codes fits into the definition if we choose $I = \langle 0 \rangle$).

Definition 2 *Let* $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ *be a basis for* $L \subseteq R_q$ *such that* $Supp(B_i) \subseteq \Delta_\prec(I_q)$, *for* $i = 1, \ldots, \dim(L)$. *If* $lm(B_1) \prec lm(B_2) \prec \cdots \prec lm(B_{\dim(L)})$ *holds then the basis is called well-behaving.*

Remark 3 *Reducing the representatives of the residue classes modulo a Gröbner basis we get that the first requirement is satisfied. Using then Gaussian elimination we can make sure that the second requirement is satisfied. Hence, a well-behaving basis always exists.*

Remark 4 *The typical example of a well-behaving basis is when the representatives of the residue classes are monomials from* $\Delta_\prec(I_q)$.

Definition 3 *Let* $L \subseteq R_q$ *and consider any well-behaving basis. Then define* $\Box_\prec(L) = \{lm(B_1), \ldots, lm(B_{\dim(L)})\}$.

Remark 5 *If the representatives are monomials from the footprint then* $\Box_\prec(L)$ *equals the representatives.*

Definition 4 *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* $lm(H) = M_1$ *we have*

$$lm(M_1M_2 \ \ rem \ \ \mathcal{G}) = lm(HM_2 \ \ rem \ \ \mathcal{G}).$$

From Gröbner basis theory we know that the remainder is unique no matter which Gröbner basis is used. Hence, the above definition is independent of the choice of $\mathcal{G}$. The motivation of the above definition is as follows. Assume $\mathrm{Supp}(F) \subseteq \Delta_\prec(I_q)$, $F \neq 0$ and consider $\vec{c} = \mathrm{ev}(F)$. If $\mathrm{lm}(F) = M_1$ and (M_1, M_2) is OWB then we know that

$$\mathrm{lm}(M_1 M_2 \ \ \mathrm{rem} \ \ \mathcal{G}) \in \Delta_\prec(I_q) \backslash \mathrm{lm}(I_q + \langle F \rangle).$$

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

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

Proof: Let $\vec{c} \in C(I, L) \backslash \{\vec{0}\}$. Then there exists an F such that $\mathrm{Supp}(F) \subseteq \Delta_\prec(I_q)$, $\mathrm{lm}(F) = P \in \Box_\prec(L)$ and $\mathrm{ev}(F + I_q) = \vec{c}$. From the footprint bound we know

$$w_H(\vec{c}) \ \ = \ \ n - \#\Delta_\prec(I_q + \langle F \rangle)$$

We now study $\Delta_\prec(I_q + \langle F \rangle)$. If $N, K \in \Delta_\prec(I_q)$ satisfy that (P, N) is OWB and $\mathrm{lm}(PN \ \ \mathrm{rem} \ \ \mathcal{G}) = K$ then

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

Hence,

$$\#\Delta_\prec(I_q + \langle F \rangle) \leq \#\Delta_\prec(I_q) - \#\big\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q) \text{ such that } (P, N) \text{ is OWB and } \mathrm{lm}(PN \ \ \mathrm{rem} \ \ \mathcal{G}) = K\big\}. \quad (3)$$

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

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

6 The affine variety code $C(I, L)^\perp$

Consider the code

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

The following theorem is a reformulation of 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*

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

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

$$\vec{c}\cdot\mathrm{ev}(K+I_q)\neq 0 \tag{4}$$

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 (4) holds. By linearity of the inner product and the minimality of K we have $K\notin\square_{\prec}(L)$. 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 $\mathrm{lm}(P_iN_i \text{ rem } \mathcal{G})=K$ for $i=1,\ldots,\delta$. The OWB property implies that

$$\mathrm{lm}\big(\big(\sum_{\substack{t=1,\ldots,i\\ a_i\neq 0}}\big)N_i \text{ rem } \mathcal{G}\big)=K$$

The minimality of K therefore ensures that

$$\vec{c}\cdot\mathrm{ev}\Big(\big(\sum_{\substack{t=1,\ldots,i\\ a_i\neq 0}} a_tP_t\big)N_i \ \text{ rem } \ \mathcal{G}+I_q\Big)\neq 0 \tag{5}$$

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

$$(a_1,\ldots,a_n)*(b_1,\ldots,b_n)=(a_1b_1,\ldots,a_nb_n).$$

As

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

we conclude from (5) that

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

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

$$\vec{e}\in\big\{\mathrm{ev}\big(\big(\sum_{t=1}^{\delta}a_tP_t\big)+I_q\big)\big|a_1,\ldots,a_\delta\in\mathbb{F}_q,\ \text{not all } a_i \text{ equal } 0\big\}. \tag{6}$$

The space consisting of (6) and $(0,\ldots,0)$ is of dimension δ and therefore the Hamming weight of $\vec{c}$ needs to be at least δ.

7 The order domain conditions

Recall from the examples in Section 4 that it helped us a lot that the defining polynomial(s) of I contained exactly two monomials of the highest weight and that the footprint $\Delta_{\prec_w}(I_q)$ contained no two different monomials of the same weight. When this kind of behavior is present we will say that the order domain conditions are satisfied. To define the order domain conditions formally we start by defining the generalized weighted degree orderings.

Definition 5 *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 $\mathbf{N}_0^r$. Define*

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

Let $\prec_{\mathcal{M}}$ be a monomial ordering on $\mathcal{M}(\vec{X})$. 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

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

Definition 6 *Let $I \subseteq k[X_1, \ldots, X_m]$. Let $\prec_w$ be a generalized weighted degree ordering. Assume I possesses a Gröbner basis $\mathcal{B}$ such that*

- *any $G \in \mathcal{B}$ has exactly two monomials of highest weight in its support*
- *no two monomials in $\Delta_{\prec_w}(I)$ are of the same weight*

Then $(I, \prec_w)$ satisfies the order domain conditions.

Lemma 3 *Assume the order domain conditions are satisfied. Let F be a polynomial with exactly one monomial of highest weight. Then $w(lm(F)) = w(lm(F \ \ rem \ \ \mathcal{B}))$. In particular $w(lm(F)) = w(lm(F \ \ rem \ \ \mathcal{B}))$ holds for all F with $Supp(F) \subseteq \Delta_{\prec_w}(I)$*

Proof: In the process of dividing F modulo $\mathcal{B}$ the leading monomial may be replaced. However, always with a monomial of the same weight.

Clearly, the norm-trace polynomials satisfy the order domain conditions. We now show that also the structures giving us Reed-Solomon codes, Generalized Reed-Muller codes and Hyperbolic codes can be put into a form such that they satisfy the order domain conditions.

Example 8 *Consider the ideals* $I = \{0\} = \langle 0 \rangle \subseteq \mathbf{F}_q[X_1, \ldots, X_m]$, $I_q = \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$. *We define weights by* $w(X1^{i_1} \cdots X_m^{i_m}) = (i_1, \ldots, i_m)$ *and we order* $\mathbf{N}_0^m$ *by some monomial ordering* $\prec_{\mathbf{N}_0^m}$. *As no two different monomials are of the same weight we can choose* $\prec_{\mathcal{M}}$ *to be any monomial ordering on* $\mathcal{M}(\vec{X})$ *(it will never be used). There are no defining equation of* I *and therefore the order domain conditions are trivially satisfied.*

Example 9 *Let* $a, b \in \mathbf{F}_q$ *and consider*

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

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

$$I = \langle H_1, H_2 \rangle \subseteq \mathbf{F}_{q^2}[X, Y, Z, U].$$

Choose weights $w(X) = (q, 1)$, $w(Y) = (0, q)$, $w(Z) = (q, 0)$, $w(U) = (q+1, 0) \in \mathbf{N}_0^2$ *and let* $\prec_{\mathbf{N}_0^2}$ *be any fixed monomial ordering on* $\mathbf{N}_0^2$ *with* $(q^2, q), (q, q^2), (0, q^2 + q) \prec_{\mathbf{N}_0^2} (q^2+q, 0)$ *and* $(q, q^2) \prec_{\mathbf{N}_0^2} (q^2, q)$. *Finally, let* $\prec_{\mathcal{M}}$ *be any fixed monomial ordering on* $\mathcal{M}(X, Y, Z, U)$ *that satisfies* $YZ^q \prec_{\mathcal{M}} X^q$ *and* $Z^{q+1} \prec_{\mathcal{M}} U^q$. *The leading monomial of* H_1 *resp.* H_2 *is* X^q *resp.* U^q *and therefore* $\mathcal{B} = \{H_1, H_2\}$ *is a Gröbner basis (as the leading monomials are relatively prime). By inspection the order domain conditions are seen to be satisfied.*

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.*

Proof: Follows by the same arguments as where used in Section 4.

Definition 7 *Assume* I *and* $\prec_w$ *satisfy the order domain conditions. Let* $\Gamma = w(\Delta_{\prec_w}(I))$ *and define for all* $\lambda \in \Delta_{\prec_w}(I_q)$

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

and for all $\lambda \in \Gamma$

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

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

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

is a well-behaving basis. 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 $\delta \in \mathbf{N}$.

$$L_1 = \mathrm{Span}_{\mathbf{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), w(M) \preceq_{\mathbf{N}_0^r} \vec{s}\} \quad (7)$$

$$L_2 = \mathrm{Span}_{\mathbf{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \sigma(w(M)) \geq \delta\} \quad (8)$$

$$L_3 = \mathrm{Span}_{\mathbf{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \mu(w(M)) < \delta\}. \quad (9)$$

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.

Remark 6 *Assume that the pair I and $\prec_w$ satisfies the order domain conditions. Let $U \subseteq \mathcal{V}_{\mathbf{F}_q}(I)$. 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 $\mathcal{V}_{\mathbf{F}q}(I)$. All we need to do is to replace I_q with I_U in all the previous definitions and results.

8 Order domains

Definition 8 *Let k be a field and let R be a k-algebra. Let $\Gamma \subseteq \mathbb{N}_0^r$ be a semigroup and assume $\prec_{\mathbf{N}_0^r}$ is a monomial 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 $\mathcal{B} = \{f_\lambda \mid \lambda \in \Gamma\}$[1] and for all $\lambda \in \Gamma$ define $R_\lambda = Span_k\{f_\gamma \mid \gamma \preceq_{\mathbf{N}_0^r} \lambda\}$. 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 $\delta \prec_{\mathbf{N}_0^r} \lambda + \gamma$.*
The map ρ extends to a function on R by

- $\rho(0) = -\infty$
- *If $f \in R_\lambda$ but $f \notin R_\gamma$ for any $\gamma \prec_{\mathbf{N}_0^r} \lambda$ then $\rho(f) = \lambda$*

Such a function is called a weight function.

The following is an equivalent definition.

Definition 9 *Let $\prec_{\mathbf{N}_0^r}$ be a monomial 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

[1] with the underlying assumption that $\rho(f_\lambda) = \lambda$

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

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

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

(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* $\rho(f - ag) \prec_{\mathbf{N}_0^r} \rho(g)$

We note that weight functions are special cases of order functions. To get the general definition of an order function we replace $(\Gamma \subseteq \mathbb{N}_0^r, \prec_{\mathbf{N}_0^r})$ by any well-order $(\Gamma, <_\Gamma)$. Then we replace (W.3) with

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

In the following we consider only weight functions.

Example 10 *Let $\mathcal{P}$ be a rational place in an algebraic function field of one variable and let $\nu_\mathcal{P}$ be the valuation corresponding to $\mathcal{P}$. Then $R = \cup_{m=0}^{\infty} \mathcal{L}(m\mathcal{P})$ is an order domain with a (numerical) weight function given by $\rho(x) = -\nu_\mathcal{P}(x)$ for all $x \in R$. The whole function field is Quot(R).*

It is not surprisingly that there is a strong connection between order domains and ideals satisfying the order domain conditions. This connection is worked out in the following two theorems.

Theorem 4 *(The Factorring Theorem)*
Let $\prec_w$ be a generalized weighted degree ordering on $\mathcal{M}(X_1, \ldots, X_m)$ and let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal. If $(I, \prec_w)$ satisfies the order domain conditions then $R = k[X_1, \ldots, X_m]/I$ is an order domain with a weight function defined as follows:
Given a nonzero $f \in R$ write $f = F + I$ where Supp$(F) \subseteq \Delta_{\prec_w}(I)$. We have $\rho(f) = \max\{w(M) \mid M \in$ Supp$(F)\}$ and $\rho(0) = -\infty$.

Proof: We construct a basis for R as follows

$$\mathcal{B} = \{M + I \mid M \in \Delta_{\prec_w}(I)\}.$$

We must show that it is well-behaving. The second order domain condition implies that $\rho : \mathcal{B} \to w(\Delta_{\prec_w}(I))$ is a bijection. Consider $f_1, f_2 \in R$. We may assume $f_1 = F_1 + I$, $f_2 = F_2 + I$ where $\mathrm{Supp}(F_1), \mathrm{Supp}(F_2) \subseteq \Delta_{\prec_w}(I)$. Let $\mathrm{lm}(F_1) = M_1$ and $\mathrm{lm}(F_2) = M_2$. The polynomial F_1F_2 has precisely one monomial of highest weight, namely M_1M_2. When reduced modulo the Gröbner basis the weight is not changed (see Lemma 3). Therefore when f_1f_2 is written

$f_1 f_2 = F + I$ with $\mathrm{Supp}(F) \in \Delta_{\prec_w}(I)$ we have

$$\begin{aligned} w(\mathrm{lm}(F)) &= w(M_1 M_2) \\ &= w(M_1) + w(M_2) \\ &= \rho(f_1) + \rho(f_2) \end{aligned}$$

Hence, the definition of ρ in the theorem satisfies $\rho(f_1 f_2) = \rho(f_1) + \rho(f_2)$ and the proof is complete.

Theorem 5 *(The Presentation Theorem)*
Given $\prec_{\mathbf{N}_0^r}$ and $\Gamma = \langle \lambda_1, \ldots, \lambda_m \rangle \subseteq \mathbf{N}_0^r$. Let $\rho : R \to \Gamma \cup \{-\infty\}$ be a weight function. Then there exists a generalized weighted degree ordering $\prec_w$ and an ideal $I \subseteq k[X_1, \ldots, X_m]$ such that $R \simeq k[X_1, \ldots, X_m]/I$ and such that $(I, \prec_w)$ satisfies the order domain conditions.

Fix ANY monomial ordering $\prec_{\mathcal{M}}$ on $\mathbf{N}_0^m \simeq \mathcal{M}(X_1, \ldots, X_m)$. Now $(w, \prec_{\mathbf{N}_0^r}, \prec_{\mathcal{M}})$ defines a generalized weighted degree ordering $\prec_w$.

Choose $x_1, \ldots, x_m \in R$ with $\rho(x_1) = \lambda_1, \ldots, \rho(x_m) = \lambda_m$. Consider the homomorphism from $k[X_1, \ldots, X_m]$ to R given by $X_i \mapsto x_i$. Denote by I the kernel. Clearly, $k[X_1, \ldots, X_m]/I \simeq R$.

Definition 10 *Let*

$$\begin{aligned} B(\Gamma) \;:=\; \{(n_1, \ldots, n_m) \in \mathbf{N}_0^m \mid \;& \textit{if } \lambda_1 n_1 + \cdots + \lambda_m n_m = \lambda_1 k_1 + \cdots + \lambda_m k_m \\ & \textit{then } (n_1, \ldots, n_m) \prec_{\mathcal{M}} (k_1, \ldots, k_m)\} \end{aligned}$$

Let $V(\Gamma)$ be the set of minimal elements in $\mathbf{N}_0^m \backslash B(\Gamma)$ with respect to the ordering $<$ given by $(r_1, \ldots, r_m) < (s_1, \ldots, s_m)$ if $r_i \leq s_i$ holds for $i = 1, \ldots, m$ and $r_i = s_i$ does not hold for all $i = 1, \ldots, m$.

Remark 7 *Dickson's Lemma tells us that $V(\Gamma)$ is finite.*

Proposition 3 *$\{\vec{x}^{\vec{N}} \mid \vec{N} \in B(\Gamma)\}$ forms a k-basis for R.*

Proof: As two different elements in the set have different weights, the elements are linearly independent by the definition of a weight function. let $h \in R \backslash \{0\}$. There exists $\vec{N} = (n_1, \ldots, n_m) \in B(\Gamma)$ such that $\rho(\vec{x}^{\vec{N}}) = \rho(h)$. We can choose $c_{\vec{N}} \in K$ such that $\rho(h - c_{\vec{N}}) \prec_{\mathbf{N}_0^r} \rho(h)$. Continuing this way we see that

$$h = \sum_{\vec{N} \in B(\Gamma)} c_{\vec{N}} \vec{x}^{\vec{N}}$$

where only finitely many $c_{\vec{N}} \neq 0$. Here we used the fact that a decreasing sequence of monomials will eventually terminate.

Corollary 1 $R = k[x_1, \ldots, x_m]$

Lemma 4 $\Delta_{\prec_w}(I) = \{\vec{X}^{\vec{N}} \mid \vec{N} \in B(\Gamma)\}$.

Proof: As $\Delta_{\prec_w}(I)$ constitutes a basis for $k[X_1,\ldots,X_m]/I$ and $\{\vec{x}^{\vec{N}} \mid \vec{N} \in B(\Gamma)\}$ constitutes a basis for R it is enough to show

$$\Delta_{\prec_w}(I) \subseteq \{\vec{X}^{\vec{N}} \mid \vec{N} \in B(\Gamma)\}.$$

Aiming for a contradiction assume

$$\vec{X}^{\vec{P}} \in \Delta_{\prec_w}(I) \backslash \{\vec{X}^{\vec{N}} \mid N \in B(\Gamma)\}.$$

By Proposition 3 we can write

$$\vec{x}^{\vec{P}} = \sum_{\substack{\vec{N} \in B(\Gamma) \\ \rho(\vec{x}^{\vec{N}}) \prec_{\mathbf{N}_0^r} \rho(\vec{x}^{\vec{P}})}} c_{\vec{N}} \vec{x}^{\vec{N}}.$$

The polynomial

$$\vec{X}^{\vec{P}} - \sum_{\substack{\vec{N} \in B(\Gamma) \\ \rho(\vec{x}^{\vec{N}}) \prec_{\mathbf{N}_0^r} \rho(\vec{x}^{\vec{P}})}} c_{\vec{N}} \vec{X}^{\vec{N}}$$

belongs to I and by the definition of $B(\Gamma)$ we have that the leading monomial is $\vec{X}^{\vec{P}}$. This is in contradiction with the assumption and we are through.

Observe that the above lemma implies that the second order domain conditions in Definition 6 is satisfied.

Proposition 3 ensures that the following definition makes sense.

Definition 11 *For each $\vec{N} \in V(\Gamma)$ let*

$$F_{\vec{N}}(\vec{X}) := \vec{X}^{\vec{N}} - \sum_{\vec{M} \in B(\Gamma)} c_{\vec{M}} \vec{X}^{\vec{M}}$$

where

$$\vec{x}^{\vec{N}} = \sum_{\vec{M} \in B(\Gamma)} c_{\vec{M}} \vec{x}^{\vec{M}}$$

Proposition 4

$$\mathcal{B} = \{F_{\vec{N}}(\vec{X}) \mid \vec{N} \in V(\Gamma)\}$$

is a Gröbner basis for I with respect to $\prec_w$.

Proof: The above set is finite. From Lemma 4 and the definition of $V(\Gamma)$ we get that $\langle \mathrm{lm}(\mathcal{B}) \rangle = \langle \mathrm{lm}(I) \rangle$. By definition $\mathcal{B} \subseteq I$. Hence, it is satisfies all the conditions for being a Gröbner basis.

By construction $F_{\vec{N}}(\vec{X})$ contains exactly two monomials of highest weight in its support. Hence, also the first order domain condition in Definition 6 is satisfied. All together we proved that the order domain conditions are satisfied. That is, Theorem 5 has been proved.

Theorem 6 *Let $\rho : R \to \Gamma \cup \{-\infty\}$ be a weight function with finitely generated value semigroup $\Gamma \subseteq \mathbf{N}_0^r$. We may assume r is chosen smallest possible. Then r equals the transcendence degree of* $\mathbf{Quot}(R)$.

9 Codes from order domains

Having defined order domains we now consider the maps that will help us construct codes.

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

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

for all $f, g \in R$ (here $*$ is the component-wise product).

Although in principle any finitely generated order domain[2] can be described as a factor ring satisfying the order domain conditions such a description might not at all be easy to find. This is why we need the above general description of an evaluation map. In the case of a factor ring the morphism in Definition 12 simply corresponds to evaluation in affine points.

Proposition 5 *Let $\varphi : R = \mathbf{F}_q[X_1, \ldots, X_m]/I \to \mathbf{F}_q^n$ be a morphism of $\mathbf{F}_q$ algebras. There exists a set*

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

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.

Proof: We will use the notation $\varphi(f) = (\varphi_1(f), \ldots, \varphi_n(f))$. The assumption that φ is surjective implies $\varphi_i \neq \varphi_j$ for $i \neq j$. The remaining assumptions imply that $\varphi_i : \mathbf{F}_q[\vec{X}]/I \to \mathbf{F}_q$ is a ring homomorphism with $\varphi_i(c+I) = c$ for all $c \in \mathbf{F}_q$. Writing $x_1 = X_1 + I, \ldots, x_m = X_m + I$ and identifying $c+I$ with c for all $c \in \mathbf{F}_q$ we get $F(X_1, \ldots, X_m) + I = F(x_1, \ldots, x_m)$. Now let $P_i^{(1)} = \varphi_i(x_1), \ldots, P_i^{(m)} = \varphi_i(x_m) \in \mathbf{F}_q$. The fact that φ_i is a ring homomorphism with $\varphi_i(c + I) = c$ for all $c \in \mathbf{F}_q$ 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 $P_i = (P_i^{(1)}, \ldots, P_i^{(m)})$ is a zero of $F(\vec{X})$. In other words $P_i \in \mathcal{V}_{\mathbf{F}_q}(I)$.

Definition 13 *Let R be an order domain over $\mathbf{F}_q$ with a weight function $\rho : R \to \Gamma \cup \{-\infty\}$ and let $\{f_\lambda \mid \rho(f_\lambda) = \lambda, \lambda \in \Gamma\}$ be a well-behaving basis. Let $\varphi : R \to \mathbf{F}_q^n$ be a morphism. 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*

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

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

[2] an order domain with a weight function with finitely generated value semigroup

Proposition 6 *If* $\{P_1, \ldots, P_n\} = \mathbf{V}_{\mathbf{F}_q}(I_q)$ *and* $\varphi(F + I) = (F(P_1), \ldots, F(P_n))$ *then*

$$\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q)). \tag{10}$$

If $\{P_1, \ldots, P_n\} \subsetneq \mathbf{V}_{\mathbf{F}_q}(I_q)$ *a similar result holds.*

Proof: We only consider the case $\{P_1, \ldots, P_n\} = \mathcal{V}_{\mathbf{F}_q}(I_q)$. Both the sets $\Delta(R, \rho, \varphi)$ and $\Delta_{\prec_w}(I_q)$ are of size n. Hence, we will be through 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 $2 \leq i \leq n$. Write $f_{\alpha(i)} = F + I$ with $\mathrm{Supp}(F) \subseteq \Delta_{\prec_w}(I)$ where $w(\mathrm{lm}(F)) = \alpha(i)$. We have

$$\varphi(F + I) = \varphi(F \text{ rem } \mathcal{G} + I) \tag{11}$$

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 both $\mathrm{Supp}(F \text{ rem } \mathcal{G})$ and $\mathrm{Supp}(F)$ are contained in $\Delta_{\prec_w}(I)$ and therefore

$$\rho(F + I) = w(\mathrm{lm}(F)) \succeq_w \rho(F \text{ rem } \mathcal{G} + I) = w(\mathrm{lm}(F \text{ rem } \mathcal{G}))$$

But then, by (11) $\alpha(i)$ does not satisfy the definition of the $\alpha(i)$'s. We have reached at a contradiction.

Definition 14 *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*

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

Definition 15 *Let* R *be an order domain over* $\mathbf{F}_q$ *and let* φ *be a morphism. 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*

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

Theorem 7 *The minimum distance of* $E(\lambda)$ *is at least*

$$\min\{\sigma(\eta) \mid \eta \preceq_{\mathbf{N}_0^r} \lambda, \eta \in R(R, \rho, \delta)\}$$

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

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

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

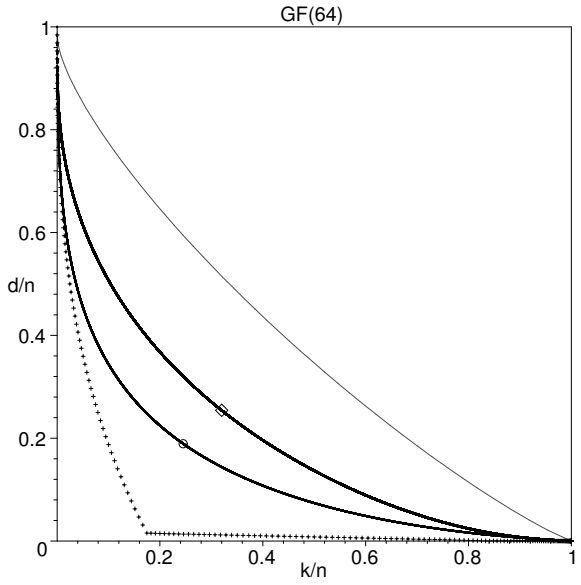


Figure 1:

Proof: In the case of a finitely generated order domain the results follow by considering the codes as affine variety codes.

Example 11 *This is a continuation of Example 9 where we showed that* $\{H_1, H_2\}$ *is a Gröbner basis with respect to the generalized weighted degree ordering* $\prec_w$ *under consideration. Now lets turn to the code construction. Applying Buchberger's algorithm we find that*

$$\{H_1, H_2, X^{q^2} - X, Y^{q^2} - Y, Z^{q^2} - Z, U^{q^2} - U\}$$

is a Gröbner basis for I_{q^2}*. Hence, we get*

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

The footprint is of size q^6 *and we therefore get codes of length* $n = q^6$*. The footprint* $\Delta_{\prec_w}(I_q)$ *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* $s = 1, 2, \ldots, q^6$*. 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.*

Proposition 7 *(The shape of a box) Let* $\mathbb{V}_{\mathbf{F}_q}(I_q) = \{P_1, P_2, \ldots, P_n\}$ *and consider the evaluation map* $\varphi : R \to \mathbb{F}_q^n$ *given by* $\varphi(F+I) = (F(P_1), F(P_2), \ldots, F(P_n))$*.*

Let $\Delta(R,\rho,\varphi) = \{\alpha(1),\alpha(2),\ldots,\alpha(n)\}$ be defined accordingly. If $\Delta_{\prec_w}(I_q)$ is of the form

$$\Delta_{\prec_w}(I_q) = \{X_1^{\beta_1}X_2^{\beta_2}\ldots X_m^{\beta_m} \mid \beta_1 \leq \gamma_1, \beta_2 \leq \gamma_2, \ldots, \beta_m \leq \gamma_m\} \qquad (12)$$

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

$$\mu(\rho(X_1^{\beta_1}\cdots X_m^{\beta_m}+I)) = \sigma(\rho(X_1^{\gamma_1-\beta_1}\cdots X_m^{\gamma_m-\beta_m}+I)) \qquad (13)$$

holds for any $X_1^{\beta_1}\cdots X_m^{\beta_m} \in \Delta(I_q)$.

Example 12 *The footprints used in the construction of Generalized Reed-Muller code, hyperbolic codes and norm-trace codes have shapes of a box.*

Example 13 *Let $I := \langle X^5+Y^4+Y, Y^5+Z^4+Z, Z^5+U^4+U^2\rangle \subseteq \mathbb{F}_{16}[X,Y,Z,U]$ (note the term U^2). Define the generalized weighted degree ordering $\prec_w$ on $\mathcal{M}(X,Y,Z,U)$ as follows. Consider weights $w(X) = 64, w(Y) = 80, w(Z) = 100, w(U) = 125 \in \mathbb{N}_0$. Let $\prec_{\mathbb{N}_0}$ be the usual (and unique) monomial ordering on $\mathbb{N}_0$ and let $\prec_{\mathcal{M}}$ be the lexicographic ordering on $\mathcal{M}(X,Y,Z,U)$ given by $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z \prec_{\mathcal{M}} U$. Clearly, $\{X^5+Y^4+Y, Y^5+Z^4+Z, Z^5+U^4+U^2\}$ is a Gröbner basis and by inspection the order domain conditions are satisfied. We therefore get a weight function*

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

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

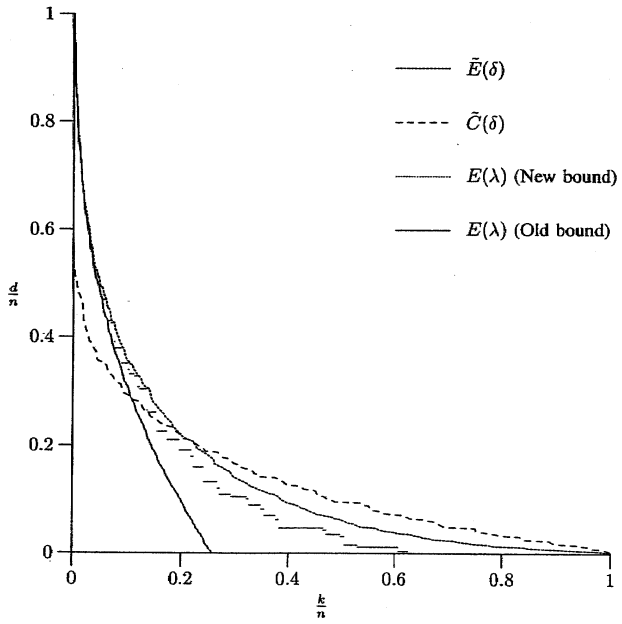
$$\{Y^4, Z^4, U^4, X^{10}Y^2Z^2, X^5Y^2ZU^2, X^{10}ZU^2, X^5Y^2Z^3, X^{10}Z^3, X^{10}Y^3, X^{15},$$
$$XY^3Z^3U^2, X^6Y^3U^2, X^{11}U^2, X^6Z^2U^2, X^6Y^3Z^2, X^{11}Y, X^{11}Z, X^6YZU^2,$$
$$X^6YZ^3, X^{10}Y^2U^2, X^5YZ^2U^2\}.$$

By definition of a Gröbner basis the footprint of I_{16} consists of the monomials that are not divisible of any of the above 21 monomials. The footprint is found to be of size $n = 512$ and we therefore have a morphism $\varphi : R \to \mathbb{F}_{16}^{512}$ for the code construction. It is clear that the footprint does not satisfy the conditions in (12). That is, it does not have the shape of a box. Therefore it should come as no surprise that the codes $\tilde{C}(\delta)$ and the codes $\tilde{E}(\delta)$ perform quite differently. In the figure below we plot the estimated performance of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$. It is clear that for values of k/n smaller than approximately 0.2 the codes $\tilde{E}(\delta)$ are the best whereas for larger values the codes $\tilde{C}(\delta)$ are the best. Finally in the figure we plot the usual Goppa bound (old bound) for the $E(\lambda)$ codes versus the improved bound from the present paper (new bound).

$I = \langle X^5 - Y^4 - Y, Y^5 - Z^4 - Z, Z^5 - U^4 - U^2 \rangle \subseteq \mathbb{F}_{16}[X, Y, Z, U]$

$\omega(X) = 64, \ \omega(Y) = 80, \ \omega(Z) = 100, \ \omega(U) = 125$

Alphabet $= \mathbb{F}_{16}$, $n = 512$



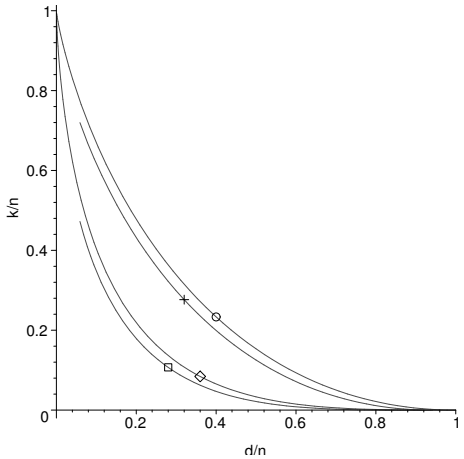
10 The tensor product construction

Given weight functions $\rho_1 : R_1 \to \Gamma_1 \cup \{-\infty\}$, $\Gamma_1 \subseteq \mathbf{N}^{r_1}$ and $\rho_2 : R_2 \to \Gamma_2 \cup \{-\infty\}$ $\Gamma_2 \subseteq \mathbf{N}^{r_2}$ we can construct a weight function ρ on the tensor product $R_1 \otimes R_2$ by $\rho(f_1 f_2) = (\rho_1(f_1), \rho_2(f_2))$ for all $f_1 \in R_1$ and $f_2 \in R_2$. We only need to choose a proper ordering $\prec_{\mathbf{N}_0^{r_1+r_2}}$. Clearly, we can consider repeated tensor products of order domains.

Example 14 *The polynomial ring in m variables can be considered at m tensor products of the polynomial ring in one variable.*

Example 15 *In this example we consider the tensor product of m Hermitian*

order domains. This involves weights in $\mathbb{N}_0^m$*. In the figure below we consider codes over the alphabet* $\mathbb{F}_{256}$*. From above we have the codes:* $Hyp_{256}(s,2)$ *of length* $n = 65536$*,* $Herm_{256}(s,2)$ *of length* $n = 16777216$*,* $Hyp_{256}(s,3)$ *of length* $n = 16777216$*,* $Herm_{256}(s,3)$ *of length* $n = 68719476736$*.*



11 One-point geometric Goppa codes

From the discussion so far it is clear that one-point geometric Goppa codes and their improvements can be considered as order domain codes where the weight functions under consideration are numerical. Actually, it has been shown that restricting to numerical weight functions produces no other codes than this. The bounds described in this note fortunately turns out to be improvements to the Goppa bounds.

Definition 16 *Consider* $\Gamma \subseteq \mathbf{N}_0$*,* $\mathbf{N}_0 \backslash \Gamma$ *finite. Write*

$$\Gamma = \{\lambda_1 = 0, \lambda_2, \ldots\}, \qquad \lambda_i < \lambda_{i+1},\ i = 1, 2, \ldots$$

Define

$$\begin{aligned} g(i) &= \#\{\lambda \in \mathbf{N}_0 \backslash \Gamma \mid \lambda < \lambda_i\} \\ g &= \#\mathbf{N}_0 \backslash \Gamma \\ D(i) &= \{(x,y) \mid x, y \in \mathbf{N}_0 \backslash \Gamma \quad \textit{and} \quad x + y = \lambda_i\} \end{aligned}$$

Lemma 5

$$\begin{aligned} \lambda_i &= \#\big(\Gamma \backslash (\lambda_i + \Gamma)\big) \\ \mu(\lambda_i) &= i - g(i) + D(i) \end{aligned}$$

Using the lemma we find the following theorem.

Theorem 8 *Given numerical weight functions we get*

$$d\big(E(\lambda_t)\big) \geq \min\{\sigma(\lambda_i) \mid i = 1, \ldots, t\} \geq n - \lambda_t$$

$$d\big(C(\lambda_t)\big) \geq \min\{\mu(\lambda_i) \mid i = t+1, \ldots\} \geq t + 1 - g$$

The right most expressions are known as the Goppa bounds.