Order domain codes and affine variety codes

Olav Geil

Aalborg University

International School and Conference on Coding Theory,
CIMAT, 2008

The course

is about generalizing

- the Reed-Solomon Code construction

by use of

- Gröbner basis theory
- Simple linear and abstract algebra

We study

- The parameters $[n, k, d]$
- Generator and parity-check matrices
- Decoding

Gröbner basis theory is explained along the way.

Preliminaries

$\mathbf{F}_q^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbf{F}_q\}$ a vector space over $\mathbf{F}_q$.

We consider linear codes. That is, subspaces $C \subseteq \mathbf{F}_q^n$.

Encoding of message $\vec{m} \in \mathbf{F}_q^k$:
$\vec{c} = \vec{m}G$ where

$$G = \begin{bmatrix} \vec{g}_1 \\ \vec{g}_2 \\ \vdots \\ \vec{g}_k \end{bmatrix}$$

and $\{\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_k\}$ is a basis for C.

Minimum distance equals minimum weight

$$d = \min\{w_H(\vec{c}) \mid \vec{c} \in C \backslash \{\vec{0}\}\}$$

Finite Fields

Type 1: p a prime $\mathbf{F}_p = \{0, 1, \ldots, p-1\}$

$$a + b \mod p, \qquad a \cdot b \mod p$$

Example: $\mathbf{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$4 + 4 = 1, \qquad 4 \cdot 4 = 2$$

Finite Fields

Type 2: $q = p^m$, $m \geq 2$, p a prime.

$f(\alpha)$ an irreducible polynomial over $\mathbf{F}_p$ of degree m.

$$\mathbf{F}_q = \{a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha a_0 \mid a_i \in \mathbf{F}_p\}$$

$a(\alpha) \cdot b(\alpha) \mod f(\alpha)$ (calculations taking place over $\mathbf{F}_p$)

(Alternatively: $\mathbf{F}_q = \mathbf{F}_p[X]/\langle f(X)\rangle$)

Example

$p = 2$, $f(\alpha) = \alpha^2 + \alpha + 1$ is irreducible over $\mathbf{F}_2$.

$\mathbf{F}_4 = \{0, 1, \alpha, \alpha + 1\}$

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Finite fields

$\mathbf{F}_q = \{P_1, \ldots, P_q\}$

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

Hence, in $\mathbf{F}_7$

$$X^q - X = (X - 0)(X - 1)(X - 2)(X - 3)(X - 4)(X - 5)(X - 6)$$

and in $\mathbf{F}_4$

$$X^q - X = (X - 0)(X - 1)(X - \alpha)(X - \alpha + 1)$$

Reed-Solomon Codes

$\mathbb{F}_q = \{P_1, P_2, \ldots, P_q\}$.

Consider $F(X) = F_0 + F_1 X + \cdots + F_{k-1} X^{k-1} \in \mathbb{F}_q[X]$.

$$(F(P_1), F(P_2), \ldots, F(P_q))$$

is a vector of length $n = q$ over $\mathbb{F}_q$.

$$\mathrm{RS}_q(k) = \{(F(P_1), F(P_2), \ldots, F(P_q)) \mid F(X) \in \mathbb{F}_q[X], \deg(F) < k\}$$

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ P_1 & P_2 & \cdots & P_q \\ P_1^2 & P_2^2 & \cdots & P_q^2 \\ \vdots & \vdots & \ddots & \ldots \\ P_1^{k-1} & P_2^{k-1} & \cdots & P_q^{k-1} \end{bmatrix}$$

Message $\vec{m} = (F_0, F_1, \ldots, F_{k-1})$ is encoded to

$$(F(P_1), F(P_2), \ldots, F(P_q)) = \vec{m} G.$$

Reed-Solomon Codes - cont.

Theorem
Nonzero polynomial $F(X) \in \mathbf{F}_q[X]$ has at most $\deg(F)$ zeros.
Let $s \leq q$ then

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

has $s = \deg(F)$ zeros.

Consequence 1:
A nonzero codeword in $\mathrm{RS}_q(k)$ has at most $k - 1$ zeros and a code word exists with exactly $k - 1$ zeros.

$$d = n - (k - 1) = n - k + 1$$

Consequence 2:
Non-trivial linear combination of rows in G corresponds to non-zero polynomial of degree at most $k - 1 < q$. Hence, G is of full rank.

Polynomials in two variables

Definition:
Total degree lexicographic ordering on monomials in X and Y is given by $X^{i_1}Y^{j_1} \prec_{tot} X^{i_2}Y^{j_2}$ if (1) or (2) holds

(1) $i_1 + j_1 < i_2 + j_2$

(2) $i_1 + j_1 = i_2 + j_2$ and $i_1 < i_2$

$\mathrm{lm}(X^3Y + Y^3X + XY^2 + 2X^2 + 2X + 1) = X^3Y$.

Theorem:
If $\mathrm{lm}(F) = X^iY^j$ with $i, j < q$ then at most $q^2 - (q-i)(q-j)$ zeros over $\mathbf{F}_q^2$. Let $\mathbf{F}_q = \{Q_1, \ldots, Q_q\}$. The polynomial

$$\Big(\prod_{s=1}^{i}(X - Q_s)\Big)\Big(\prod_{t=1}^{j}(Y - Q_t)\Big)$$

has $q^2 - (q-i)(q-j)$ zeros.

Polynomials in two variables

$$\mathbf{F}_q^2 = \mathbf{F}_q \times \mathbf{F}_q = \{P_1, P_2, \ldots, P_{q^2}\}.$$

Corollary:
If $\mathrm{lm}(F(X,Y)) = X^i Y^j$ with $i, j < q$ then
$\big(F(P_1), F(P_2), \ldots, F(P_{q^2})\big)$ is of weight at least $(q-i)(q-j)$.

Consider $F(X,Y) \in \mathbf{F}_4[X,Y]$. Let $\mathrm{lm}(F) = X^2Y$.

$$\begin{array}{c|cccc}
Y^3 & \cdot & \cdot & * & * \\
Y^2 & \cdot & \cdot & * & * \\
Y & \cdot & \cdot & \square & * \\
1 & \cdot & \cdot & \cdot & \cdot \\
\hline
 & 1 & X & X^2 & X^3
\end{array}$$

At most 10 zeros. $\big(F(P_1), F(P_2), \ldots, F(P_{16})\big)$ at least weight 6.

Generalized Reed-Muller Codes

$$
\begin{array}{c|cccc}
Y^3 & 12 & 13 & 14 & 15 \\
Y^2 & 8 & 10 & 12 & 14 \\
Y & 4 & 7 & 10 & 13 \\
1 & 0 & 4 & 8 & 12 \\
\hline
 & 1 & X & X^2 & X^3
\end{array}
$$

Consider polynomials $F(X, Y) \in \mathbf{F}_4[X, Y]$. If $\mathrm{lm}(F) = XY^3$ then at most 13 zeros and so on.

$$
\mathrm{RM}_4(s, 2) = \{(F(P_1), \ldots, F(P_{16})) \mid \text{the total degree of } F \text{ is at most } s\}
$$

The evaluation map

$\mathbf{F}_q^2 = \{P_1, P_2, \ldots, P_{q^2}\}$ and $P_j = (P_j^{(X)}, P_j^{(Y)})$.

$$\Bigg(\prod_{\substack{j=1,\ldots,q^2 \\ P_j^{(X)} \neq P_i^{(X)}}} (X - P_j^{(X)}) \Bigg) \Bigg(\prod_{\substack{j=1,\ldots,q^2 \\ P_j^{(Y)} \neq P_i^{(Y)}}} (Y - P_j^{(Y)}) \Bigg)$$

has exactly one nonzero, namely P_i.

The map $\mathrm{ev} : \mathbf{F}_q[X, Y] \to \mathbf{F}_{q^2}$ given by
$\mathrm{ev}(F) = (F(P_1), F(P_2), \ldots, F(P_{q^2}))$ is a surjective vector space homomorphism.

The evaluation map

$$\mathrm{ev}(F(X,Y)) = \mathrm{ev}(\tilde{F}(X,Y))$$

where $\tilde{F}$ is made from F by replacing one or more of the occurrences of X^q with X and by replacing one or more of the occurrences of Y^q with Y.

$$\#\{X^iY^j \mid 0 \le i < q, 0 \le j < q\} = \#\mathbf{F}_{q^2}$$

$$\{\mathrm{ev}(X^iY^j) \mid 0 \le i < q, 0 \le j < q\}$$

is therefore a basis for $\mathbf{F}_{q^2}$ as a vector space over $\mathbf{F}_q$.

Y^3	12	13	14	15
Y^2	8	10	12	14
Y	4	7	10	13
1	0	4	8	12
	1	X	X^2	X^3

Codes	n	k	d
$\mathrm{RM}_4(0,2)$	16	1	16
$\mathrm{RM}_4(1,2)$	16	3	12
$\mathrm{RM}_4(2,2)$	16	6	8
$\mathrm{RM}_4(3,2)$	16	10	4
$\mathrm{RM}_4(4,2)$	16	13	3
$\mathrm{RM}_4(5,2)$	16	15	2
$\mathrm{RM}_4(6,2)$	16	16	1
Hyp	16	11	4

Generator matrices straight forward.

Codes over $\mathbb{F}_8$

Y^7	56	57	58	59	60	61	62	63
Y^6	48	50	52	54	56	58	60	62
Y^5	40	43	46	49	52	55	58	61
Y^4	32	36	40	44	48	52	56	60
Y^3	24	29	34	39	44	49	54	59
Y^2	16	22	28	34	40	46	52	58
Y	8	15	22	29	36	43	50	57
1	0	8	16	24	32	40	48	56
	1	X	X^2	X^3	X^4	X^5	X^6	X^7

$\mathrm{RM}_8(7, 2)$ is $[64, 36, 8]$

Hyperbolic codes with $[64, 48, 8 = 64 - 56]$ and $[64, 37, 14 = 64 - 50]$

Monomial orderings

$\mathcal{M}(X_1, \dots, X_m)$ set of monomials in $X_1, \dots, X_m$.
$\vec{X}^{\vec{\alpha}} = X_1^{\alpha_1} \cdots X_m^{\alpha_m}$, where $\vec{\alpha} = (\alpha_1, \dots, \alpha_m)$.

Definition:
A monomial ordering $\prec$ is a total ordering on $\mathcal{M}(X_1, \dots, X_m)$ satisfying

- If $\vec{X}^{\vec{\alpha}} \prec \vec{X}^{\vec{\beta}}$ then $\vec{X}^{\vec{\alpha}}\vec{X}^{\vec{\gamma}} \prec \vec{X}^{\vec{\beta}}\vec{X}^{\vec{\gamma}}$
- Every $S \subseteq \mathcal{M}(X_1, \dots, X_m)$, $S \neq \emptyset$ has a unique smallest element.

Example:
$\vec{X}^{\vec{\alpha}} \prec_{lex} \vec{X}^{\vec{\beta}}$ if $\vec{\beta} - \vec{\alpha}$ has a first non zero element > 0.

Example:
$\vec{X}^{\vec{\alpha}} \prec_{tot} \vec{X}^{\vec{\beta}}$ if (1) or (2) holds:

(1) $\sum \alpha_i < \sum \beta_i$

(2) $\sum \alpha_i = \sum \beta_i$ and $\vec{X}^{\vec{\alpha}} \prec_{lex} \vec{X}^{\vec{\beta}}$

In an ideal world...

Definition:
$J \subseteq k[\vec{X}]$ is an ideal if for all $F \in J, G \in J$ and $H \in k[\vec{X}]$

- $F + G \in J$
- $FH \in J$

$$J = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle = \{ \sum_{i=1}^{s} H_i(\vec{X}) F_i(\vec{X}) \mid H_i(\vec{X}) \in k[\vec{X}] \}$$

Example:
$\mathbf{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Rules: $2 = 0$, $\alpha^2 + \alpha + 1 = 0$
$J = \langle X^4 - X, Y^4 - Y, XY^2 + XY + \alpha \rangle \subseteq \mathbf{F}_4[X, Y]$

Varieties

Definition:
The variety $\mathcal{V}_k(J)$ is the common zeros of the polynomials in (the generators of) J.

Example:
$\mathcal{V}_{\bar{\mathbf{F}}_q}(I_q) = \mathcal{V}_{\mathbf{F}_q}(I)$ where $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ as $X_i^q - X_i$ "defines" $\mathbf{F}_q$.

Footprint

Definition:
Fix $\prec$. The set of monomials that can not be found as leading monomial of any polynomial in J is the footprint $\Delta_\prec(J)$.

Example:
$\Delta_\prec(\langle X^4 - X, Y^4 - Y\rangle) = \{X^i Y^j \mid 0 \leq i < 4, 0 \leq j < 4\}$

Footprint

Example:
$\Delta_{\prec}(\langle X^4 - X, Y^4 - Y, X^2Y + aXY + bX^2 + cX + dY + e\rangle)$ is contained in $\{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, Y^3, X^3Y\}$. May very well be smaller!!!

$$
\begin{array}{c|cccccc}
Y^5 & * & * & * & * & * & * \\
Y^4 & \square & * & * & * & * & * \\
Y^3 & \cdot & \cdot & * & * & * & * \\
Y^2 & \cdot & \cdot & * & * & * & * \\
Y & \cdot & \cdot & \square & * & * & * \\
1 & \cdot & \cdot & \cdot & \cdot & \square & * \\
\hline
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}
$$

Residue-class ring

$R = k[\vec{X}]/J$
$(F(\vec{X}) + J) + (G(\vec{X}) + J) = F(\vec{X}) + G(\vec{X}) + J$
$(F(\vec{X}) + J)(G(\vec{X}) + J) = F(\vec{X})G(\vec{X}) + J$

Theorem:
$\{M + J \mid M \in \Delta_{\prec}(I)\}$ is a basis for R as a vector space over k.

Example:
$J = \langle X^4 - X, Y^4 - Y \rangle$. $R = \mathbf{F}_4[X, Y]/J$.
$\Delta_{\prec}(J) = \{X^i Y^j \mid 0 \leq i < 4, 0 \leq j < 4\}$. Dimension of R is 16.

The evaluation map

Given $I \subseteq \mathbf{F}_q[\vec{X}]$ define $I_q := I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

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

$\mathrm{ev} : \mathbf{F}_q[\vec{X}]/I_q \rightarrow \mathbf{F}_q^n$ given by $\mathrm{ev}(F + I_q) = (F(P_1), \ldots, F(P_n))$.

Lagrange (like) interpolation possible. Hence, a surjective vectorspace homomorphism.

The evaluation map

Definition:
An ideal J is radical if $F^r \in J$, $r > 1$ implies $F \in J$.

Proposition:
I_q is radical.

Theorem: (Hilbert's Strong Nullstellensatz)
If J is radical then the vanishing ideal of $\mathcal{V}_{\bar{k}}(J)$ is J.

Corollary:
$\mathrm{ev} : \mathbf{F}_q[X_1, \ldots, X_m]/I_q \to \mathbf{F}_q^n$ is an isomorphism.

The footprint bound

Corollary:

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

Corollary:

If $\mathrm{lm}(F) = X^{i_1} \cdots X_m^{i_m}$ with $i_1, \ldots, i_m < q$ then at most $q^m - \prod(q - i_s)$ zeros over $\mathbf{F}_q^m$.

Example:

$\Delta_{\prec}(\langle X^4 - X, Y^4 - Y, X^2Y + aXY + bX^2 + cX + dY + e\rangle)$

$$
\begin{array}{c|cccccc}
Y^5 & * & * & * & * & * & * \\
Y^4 & \square & * & * & * & * & * \\
Y^3 & \cdot & \cdot & * & * & * & * \\
Y^2 & \cdot & \cdot & * & * & * & * \\
Y & \cdot & \cdot & \square & * & * & * \\
1 & \cdot & \cdot & \cdot & \cdot & \square & * \\
\hline
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}
$$

$\#$ zeros at most 10

Generalized Reed-Muller codes

$$I = \langle 0 \rangle,$$
$$I_q = \langle 0 \rangle + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle = \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$$

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

$$\mathcal{V}_{\mathbf{F}_q}(I_q) = \mathbf{F}_q^m = \{P_1, \ldots, P_{q^m}\}$$

$$\mathrm{ev}(F(\vec{X}) + I_q) = (F(P_1), \ldots, F(P_{q^m}))$$

$$\begin{aligned} \mathrm{RM}_q(s,m) \;&=\; \{\mathrm{ev}(F + I_q) \mid \deg_{X_1} < q, \ldots, \deg_{X_m}(F) < q, \\ &\qquad\qquad \deg_{tot}(F) \leq s\} \end{aligned}$$

Vectors on r.h.s. are linearly independent. Hence, dimension easily found. By the footprint bound the minimum distance is:

$$\begin{aligned} d \;&=\; \min\{\prod_{t=1}^{m}(q - i_t) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \\ &\qquad\qquad i_1 + \ldots + i_m \leq s\} \end{aligned}$$

Generalized Reed-Muller codes - continued

Minimum distance by footprint bound:
$d = \min\{\prod_{s=1}^{m}(q - i_s) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \sum_{s=1}^{m} \leq s\}$

Worst case on the border.
For $s \leq m(q-1)$ write $s = a(q-1) + b$ with $0 \leq b < q$ then min equals $(q-b)q^{m-a-1}$.

Y^3	4	3	2	1
Y^2	8	6	4	2
Y	12	9	6	3
1	16	12	8	4
	1	X	X^2	X^3

Hyperbolic codes

Y^3	4	3	2	1
Y^2	8	6	4	2
Y	12	9	6	3
1	16	12	8	4
	1	X	X^2	X^3

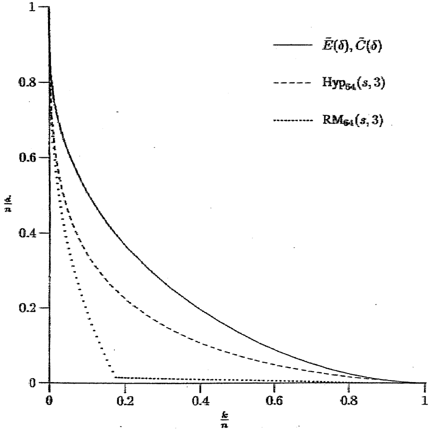
$$\begin{aligned}\mathrm{Hyp}_q(s,m) &= \mathrm{Span}_{\mathbf{F}_q}\{\mathrm{ev}(X_1^{i_1}\cdots X_m^{i_m}+I_q) \mid 0 \leq i_1 < q, \ldots, \\ &\qquad\qquad 0 \leq i_m < q, \prod_{t=1}^{m}(q-i_t) \geq \delta\},\end{aligned}$$

where $\delta = q^m - s$.

Minimum distance equals δ by footprint bound. Dimension can be calculated. Closed form estimate for dimension exists.

$$I = \langle X^q + YZ^q - Y^qZ - X,\ U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U \rangle$$
$$\subseteq \mathbb{F}_{q^2}[X,Y,Z,U], \qquad a,b \in \mathbb{F}_q$$

$$w(X) = (q,1),\ w(Y) = (0,q),\ w(Z) = (q,0),\ w(U) = (q+1,0)$$



alphabet $= \mathbb{F}_{64}$, $n = 262144$

Hermite codes

$$I = \langle X^3 - Y^2 - Y \rangle \subseteq \mathbf{F}_4[X, Y]$$
$$I_4 = \langle X^3 - Y^2 - Y, X^4 - X, Y^4 - Y \rangle$$

$$\mathcal{V}_{\mathbf{F}_4}(I_4) = \{P_1, \ldots, P_8\}$$

$$\mathrm{ev} : R_4 = \mathbf{F}_4[X, Y]/I_4 \to \mathbf{F}_4^8$$
$$\mathrm{ev}(F + I_4) = (F(P_1), \ldots, F(P_8))$$

$$E(s) = \mathrm{Span}_{\mathbf{F}_4}\{\mathrm{ev}(X^i Y^j + I_q) \mid 2i + 3j \leq s\}.$$

Hermite codes

Definition:
Let a weighted degree ordering on $\mathcal{M}(X,Y)$ be given by $X^{i_1}Y^{j_1} \prec_w X^{i_2}Y^{j_2}$ if (1) or (2) holds:

(1) $2i_1 + 3j_1 < 2i_2 + 3j_2$

(2) $2i_1 + 3j_1 = 2i_2 + 3j_2$ but $j_1 < j_2$

As ev is an isomorphism and eight zeros, the footprint is:

$$\begin{array}{c|cccccc}
Y^3 & * & * & * & * & * & * \\
Y^2 & \square & \cdot & * & * & * & * \\
Y & \cdot & \cdot & \cdot & \cdot & * & * \\
1 & \cdot & \cdot & \cdot & \cdot & \square & * \\
\hline
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}$$

Hermite codes

$E(s) = \mathrm{Span}_{\mathbf{F}_4}\{\mathrm{ev}(X^iY^j + I_q) \mid X^iY^j \in \Delta_{\prec_w}(I_4), 2i + 3j \leq s\}$
Dimension easily found.

$\#\mathcal{V}_{\mathbf{F}_4}(\langle Y + aX + b, X^3 - Y^2 - Y, X^4 - X, Y^4 - Y\rangle) =?$

Analysis so far: at most 4 zeros.

Deeper analysis will show: at most $w(Y) = 0 \cdot 2 + 1 \cdot 3 = 3$ zeros.

Affine Variety Codes

$I \subseteq \mathbf{F}_q[X_1, \ldots, X_m]$, $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$

$R_q = \mathbf{F}_q[\vec{X}]/I_q$.

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

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

$L \subseteq R_q$.

Definition:
$C(I, L) = \mathrm{ev}(L)$. $C^{\perp}(I, L)$ is the dual space.

Affine Variety codes

$\mathrm{RM}_q(s,m) = C(I,L)$ where

$$L = \mathrm{Span}_{\mathbf{F}_q}\{X_1^{i_1}\cdots X_m^{i_m} + \langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \sum_{s=1}^{m} i_s \leq s\}$$

$\mathrm{Hyp}_q(s,m) = C(I,L)$ where

$$L = \mathrm{Span}_{\mathbf{F}_q}\{X_1^{i_1}\cdots X_m^{i_m} \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, \prod_{s=1}^{m}(q - i_s) \geq q^m - s\}$$

Hermite code over $\mathbf{F}_4$ is $C(I,L)$ where

$$L = \mathrm{Span}_{\mathbf{F}_4}\{X^i Y^j + I_4 \mid 0 \leq i < 4, 0 \leq j < 2, 2i + 3j \leq s\}$$

Division algorithm

$\prec_w$ with $w(X) = 2, w(Y) = 3$

$X^5 + Y^3 + 1:$	$X^3 + Y^2 + Y$	$X^4 + X$	$Y^4 + Y$	remainder
$X^5 + X^2$		X		
$Y^3 + X^2 + 1$				
$Y^3 + X^3Y + Y^2$	Y			
$X^3Y + Y^2 + X^2 + 1$				
X^3Y				X^3Y
$Y^2 + X^2 + 1$				
$Y^2 + X^3 + Y$	1			
$X^3 + X^2 + Y + 1$				$X^3 + X^2 + Y + 1$

$$X^5 + Y^3 + 1 \ \text{rem} \ \{X^3 + Y^2 + Y, X^4 + X, Y^4 + Y\} = X^3Y + X^3 + X^2 + Y + 1$$

Gröbner basis

Definition:
$\mathcal{G} = \{G_1(\vec{X}), \ldots, G_s(\vec{X})\} \subseteq J$ is a Gröbner basis for J w.r.t. $\prec$ if whenever $M \in \mathrm{lm}(J)$ holds M is divisible by $\mathrm{lm}(G_i)$ for some i.

Facts about GB:

- A Gröbner basis is a basis.
- Buchbergers's algorithm finds GB.
- Footprint is easily read of from GB.
- For fixed $\prec$ division with remainder modulo a GB is unique.

We get:

Theorem:
$\{M + J \mid M \in \Delta_{\prec}(J)\}$ is a basis for $k[\vec{X}]/J$

Hermite code

$X^{i_1}Y^{j_1} \prec_w X^{i_2}Y^{j_2}$ if (1) or (2) holds:

(1) $2i_1 + 3j_1 < 2i_2 + 3j_2$

(2) $2i_1 + 3j_1 = 2i_2 + 3j_2$ but $j_1 < j_2$

$\{X^3 - Y^2 - Y, X^4 - X, Y^4 - Y\}$ GB with respect to $\prec_w$

$$\begin{array}{c|cccc} Y & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \hline & 1 & X & X^2 & X^3 \end{array}$$

$E(3) = C(I, L)$ with $L = \mathrm{Span}_{\mathbf{F}_4}\{1 + I_q, X + I_q, Y + I_q\}$

Motivation for definition of OWB

If $\vec{c} \in E(3)$ then $\vec{c} = \text{ev}(H(X,Y) + I_4)$ for some $H(X,Y) = aY + bX + c$. We know

$$w_H(\vec{c}) = n - \#\Delta_{\prec_w}(\langle X^3 - Y^2 - Y, X^4 - X, Y^4 - Y, H(X,Y)\rangle)$$

which is the number of elements in $\Delta_{\prec_w}(I_4)$ that is NOT in $\Delta_{\prec_w}(I_4 + \langle H(X,Y)\rangle)$.

Case 1 - $\text{lm}(H) = Y$

- $\text{lm}(1 \cdot H(X,Y) \text{ rem } \mathcal{G}) = Y$
- $\text{lm}(X \cdot H(X,Y) \text{ rem } \mathcal{G}) = XY$
- $\text{lm}(X^2 \cdot H(X,Y) \text{ rem } \mathcal{G}) = X^2Y$
- $\text{lm}(X^3 \cdot H(X,Y) \text{ rem } \mathcal{G}) = X^3Y$
- $\text{lm}(Y \cdot H(X,Y) \text{ rem } \mathcal{G}) = X^3$

Motivation for OWB continued

Here, last result follows from:

$$
\begin{aligned}
\operatorname{Im}(YH(X,Y) \text{ rem } \mathcal{G}) &= \operatorname{Im}(Y^2 + bXY + cY \text{ rem } \mathcal{G}) \\
&= \operatorname{Im}(X^3 + Y + bXY + cY \text{ rem } \mathcal{G}) \\
&= \operatorname{Im}(X^3 + bXY + (c+1)Y \text{ rem } \mathcal{G}) = X^3
\end{aligned}
$$

Hence, Y, XY, X^2Y, X^3Y, X^3 are NOT in $\Delta_{\prec_w}(I_4 + \langle H(X,Y)\rangle)$.
Hence, Hamming weight at least 5.

Case 2 - $\operatorname{Im}(H) = X$
6 element NOT in $\Delta_{\prec_w}(I_4 + \langle H(X,Y)\rangle)$ are determined.

Case 3 - $\operatorname{Im}(H) = 1$
8 element NOT in $\Delta_{\prec_w}(I_4 + \langle H(X,Y)\rangle)$ are determined.

Hence, minimum distance at least 5.

Hermite code

$$
\begin{array}{c|cccc}
Y & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot \\
\hline
 & 1 & X & X^2 & X^3
\end{array}
$$

$E(3) = C(I, L)$ with $L = \mathrm{Span}_{\mathbf{F}_4}\{1 + I_4, X + I_4, Y + I_4\}$

Notation:

$\{1 + I_4, X + I_4, Y + I_4\}$ is said to be a well-behaving basis for L because

- $\{1, X, Y\} \in \Delta_{\prec_w}(I_4)$
- $1 \prec_w X \prec_w Y$

A basis for L that is not well-behaving is $\{1 + I_4, X + Y + I_4, X + \alpha Y + I_4\}$.

We write $\square_{\prec_w}(L) = \{1, X, Y\}$

Well-behaving basis

$L \subseteq \mathbf{F}_q[\vec{X}]/I_q$.

Definition:
A basis $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ for $L \subseteq R_q$ where $\mathrm{Supp}(B_i) \subseteq \Delta_{\prec}(I_q)$ for $i = 1, \ldots, \dim(L)$ and where $\mathrm{lm}(B_1) \prec \cdots \prec \mathrm{lm}(B_{\dim(L)})$ is said to be well-behaving with respect to $\prec$.

Definition:

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

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

OWB

Definition:
Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to $\prec$. Then (M_1, M_2), $M_1, M_2 \in \Delta_{\prec}(I_q)$ is said to be OWB if for all H with $\mathrm{Supp}(H) \subseteq \Delta_{\prec}(I_q)$ and $\mathrm{lm}(H) = M_1$

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

Example:
$I_q = \langle X^4 - X, Y^4 - Y \rangle$, $\prec_{tot}$, $\mathcal{G} = \{X^4 - X, Y^4 - Y\}$ is GB.

$(X^2 Y, Y^2)$ is OWB as

$$\begin{aligned}&(X^2Y + aXY^2 + bY^3 + cX^2 + dXY + eY^2 + fX + gY + h)Y^2 \text{ rem } \mathcal{G}\\ &= X^2Y^3 + aXY + bY^2 + cX^2Y^2 + dXY^3 + eY + fXY^2 + gY^3 + hY^2\end{aligned}$$

Leading monomial equals X^2Y^3 whether or not $a = b = c = d = e = f = g = h = 0$.

Minimum distance

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

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

Order domain codes are affine variety codes where many OWB pairs are easily found.

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

$$\min\left\{\#\{K \in \Delta_{\prec}(I_q) \mid P \text{ divides } K\} \middle| P \in \Box_{\prec}(L)\right\}. \qquad (1)$$

Proof: Let K, P be as in (1). 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,

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

Hermite code

$X^{i_1}Y^{j_1} \prec_w X^{i_2}Y^{j_2}$ if (1) or (2) holds:

(1) $2i_1 + 3j_1 < 2i_2 + 3j_2$

(2) $2i_1 + 3j_1 = 2i_2 + 3j_2$ but $j_1 < j_2$

$\{X^3 - Y^2 - Y, X^4 - X, Y^4 - Y\}$ GB with respect to $\prec_w$

$$\begin{array}{c|cccc} Y & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \hline & 1 & X & X^2 & X^3 \end{array}$$

$E(3) = C(I, L)$ with $L = \mathrm{Span}_{\mathbf{F}_4}\{1 + I_q, X + I_q, Y + I_q\}$

$E(3)$ - continued

$$
\begin{array}{c|cccc}
Y & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot \\
\hline
 & 1 & X & X^2 & X^3
\end{array}
$$

Corollary gives $(Y,1),(Y,X),(Y,X^2),(Y,X^3)$ are OWB with remainder modulo $\mathcal{G}$ equal to Y, XY, X^2Y, X^3Y respectively.

$$
\begin{aligned}
(Y + aX + b)Y \text{ rem } \{X^3 - Y^2 - Y, X^4 - X, Y^4 - Y\} \\
= X^3 + aXY + (b+1)Y
\end{aligned}
$$

Hence, $\mathrm{lm}((Y + aX + b)Y \text{ rem } \mathcal{G}) = X^3$ whether or not $a = b = 0$ and therefore also (Y, Y) is OWB.

$E(3)$ - continued

$$
\begin{array}{c|cccc}
Y & \cdot & \cdot & \cdot & \cdot \\
1 & \cdot & \cdot & \cdot & \cdot \\
\hline
 & 1 & X & X^2 & X^3
\end{array}
$$

Corollary gives $(X,1),(X,X),(X,X^2),(X,Y),(X,XY),(X,X^2Y)$ are OWB with remainders modulo $\mathcal{G}$ equal to X,X^2,X^3,XY,X^2Y,X^3Y respectively.

Corollary gives $(1,N)$ OWB for all $N \in \Delta_{\prec_w}(I_4)$, and all $K \in \Delta_{\prec_w}(I_4)$ are realized as remainders.

Theorem gives $d\big(E(3)\big) \geq \min\{5,6,8\} = 5$

minimum distance

Proof: Let $\vec{c} \in C(I, L)$. Then there exists an F such that $\mathrm{Supp}(F) \subseteq \Delta_{\prec}(I_q)$, $\mathrm{lm}(F) = P \in \square_{\prec}(L)$ and $\mathrm{ev}(F + I_q) = \vec{c}$. By the footprint bound the Hamming weight of $\vec{c}$ is equal to $n - \#\Delta_{\prec}(I_q + \langle F \rangle)$. 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,

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

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

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

Hermite Codes - general case

$$I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbf{F}_{q^2}[X,Y]$$
$$I_{q^2} = \langle X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle$$

Let $w(X^iY^j) = qi + (q+1)j$. Define $X^{i_1}Y^{j_1} \prec_w X^{i_2}Y^{j_2}$ if (1) or (2) holds:

(1) $w(X^{i_1}Y^{j_1}) < w(X^{i_2}Y^{j_2})$

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

$\mathcal{H} = \{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for I
$\mathcal{G} = \{X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y\}$ is a Gröbner basis for I

Hence,
$\Delta_{\prec_w}(I) = \{X^iY^j \mid 0 \leq i, 0 \leq j < q\}$
$\Delta_{\prec_w}(I_{q^2}) = \{X^iY^j \mid 0 \leq i < q^2, 0 \leq j < q\}$

Hermite Codes - the general case

Example: the case $q^2 = 4$

$$\begin{array}{c|cccccccc} Y & 3 & 5 & 7 & 9 & 11 & 13 & \cdots \\ 1 & 0 & 2 & 4 & 6 & 8 & 10 & \cdots \\ \hline & 1 & X & X^2 & X^3 & X^4 & X^5 & \cdots \end{array} \qquad \begin{array}{c|cccc} Y & 3 & 5 & 7 & 9 \\ 1 & 0 & 2 & 4 & 6 \\ \hline & 1 & X & X^2 & X^3 \end{array}$$

$$w(\Delta_{\prec_w}(I)) \qquad\qquad w(\Delta_{\prec_w}(I_{q^2}))$$

Fact 1 (general case):
If $M, M' \in \Delta_{\prec_w}(I)$ and $w(M) = w(M')$ holds, then $M = M'$.

Fact 2 (general case):
Assume $F(X, Y)$ has a single monomial of highest weight, say w'. Then the polynomial $F(X, Y)$ rem $\{X^{q+1} - Y^q - Y\}$ has a single monomial of highest weight and this weight equals w'.

Hermite Codes - the general case

Example: the case $q^2 = 4$

Y	3	5	7	9	11	13	$\cdots$
1	0	2	4	6	8	10	$\cdots$
	1	X	X^2	X^3	X^4	X^5	$\cdots$

$w(\Delta_{\prec_w}(I))$

Y	3	5	7	9
1	0	2	4	6
	1	X	X^2	X^3

$w(\Delta_{\prec_w}(I_{q^2}))$

To see (Y, Y) OWB observe:

- Let $\mathrm{Im}(F) = Y$ and $\mathrm{Supp}(F) \in \Delta_{\prec_w}(I_4)$ then F has a single monomial of highest weight and this weight is 3.
- From fact 2 we see $w(F(X,Y)Y \text{ rem } \mathcal{H}) = w(Y^2) = 6$.
- From fact 1 $\mathrm{Im}(F(X,Y)Y \text{ rem } \mathcal{H}) = X^3$
- By inspection $X^3 \in \Delta_{\prec_w}(I_{q^2})$ and therefore $\mathrm{Im}(F(X,Y)Y \text{ rem } \mathcal{G}) = X^3$

Hermite Codes - the general case

Example: the case $q^2 = 4$

$$\begin{array}{cccc} 3 & 5 & 7 & 9 \\ 0 & 2 & 4 & 6 \\ \multicolumn{4}{c}{w(\Delta_{\prec_w}(I_{q^2}))} \end{array} \qquad \begin{array}{cccc} 5 & 3 & 2 & 1 \\ 8 & 6 & 4 & 2 \\ \multicolumn{4}{c}{\bar{\sigma}(P)} \end{array}$$

$\bar{\sigma}(P) = \#\{K \mid \exists N, (P, N) \text{ OWB } \operatorname{Im}(PN \text{ rem } \mathcal{G}) = K\}$

$L = \{1, X, Y, X^2\}$ then $C(I, L)$ is $[n, k, d] = [8, 4, 4]$

$\mathbb{F}_9[X,Y]/I, \quad I = \langle X^9 - X, Y^9 - Y, X^4 - Y^3 - Y \rangle$

$w(X) = 3, w(Y) = 4$

Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	X^6Y^2	X^7Y^2	X^8Y^2
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	X^6Y	X^7Y	X^8Y
1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

19	16	13	10	7	4	3	2	1
23	20	17	14	11	8	6	4	2
27	24	21	18	15	12	9	6	3

$$\begin{aligned}
\bar{\sigma}(X^4Y^2) &= \sigma(20) \\
&= \#\{20+0, 20+3, 20+4, \\
&\qquad 20+6, 20+8, 20+9, 20+12\} \\
&= 7
\end{aligned}$$

Hermite codes over $\mathbf{F}_9$

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

19	16	13	10	7	4	3	2	1
23	20	17	14	11	8	6	4	2
27	24	21	18	15	12	9	6	3

Observation: $n - w(P) \leq \bar{\sigma}(P)$ holds.

Hence, if $L = \mathrm{Span}_{\mathbf{F}_9}\{P + I_q \mid w(P) \leq s\}$ then $d\big(C(I, L)\big) \geq n - s$.

Better choice: $L' = \mathrm{Span}_{\mathbf{F}_9}\{P \mid \bar{\sigma}(P) \geq \delta\}$ then $d\big(C(I, L')\big) \geq \delta$.

$$C(I, L) \text{ with } s = 23: \quad d \geq 4, k = 21$$
$$C(I, L') \text{ with } \delta = 4: \quad d \geq 4, k = 22$$

Generalized weighted degree orderings

Definition:
Given numbers $w(X_1), \ldots, w(X_m) \in \mathbf{N}$ define $w(X_1^{\alpha_1} \cdots X_m^{\alpha_m}) = \sum_{i=1}^{m} \alpha_i w(X_i)$. The weighted degree lexicographic ordering $\prec_w$ is the ordering with $\vec{X}^{\vec{\alpha}} \prec_w \vec{X}^{\vec{\beta}}$ if (1) or (2) holds:

(1) $w(\vec{X}^{\vec{\alpha}}) < w(\vec{X}^{\vec{\beta}})$

(2) $w(\vec{X}^{\vec{\alpha}}) = w(\vec{X}^{\vec{\beta}})$ but $\vec{X}^{\vec{\alpha}} \prec_{lex} \vec{X}^{\vec{\beta}}$ holds

Note: One can replace $\prec_{lex}$ with any other monomial ordering. This is an example of a generalized weighted degree ordering.

Order domain theory

The order domain conditions: Let $\prec_w$ be a generalized weighted degree ordering on $\mathcal{M}(\vec{X})$. Let $I = \langle G_1(\vec{X}), \ldots, G_s(\vec{X})\rangle \subseteq \mathbf{F}_q[\vec{X}]$ be an ideal such that:

- $\{G_1, \ldots, G_s\}$ is a Gröbner basis for I w.r.t. $\prec_w$.
- For $i = 1, \ldots, s$ G_i has exactly two monomials of highest weight in its support.
- No two monomials in $\Delta_{\prec_w}(I)$ is of the same weight.

The order domain conditions guarantees that we can use the same tricks as with the Hermitian codes.

The generalized Reed-Muller code construction fits this description in the more general case where weights are not numerical.

Generalized Reed-Muller codes revisited

$w(X^i Y^j) = (i, j)$

$I = \langle 0 \rangle \subseteq \mathbf{F}_5[X, Y]$. $I_5 = \langle X^5 - X, Y^5 - Y \rangle$.

Y^4	$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$
Y^3	$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$
Y^2	$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$
Y	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$
1	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$
	1	X	X^2	X^3	X^4

Y^4	5	4	3	2	1
Y^3	10	8	6	4	2
Y^2	15	12	9	6	3
Y	20	16	12	8	4
1	25	20	15	10	5
	1	X	X^2	X^3	X^4

$$\begin{aligned}\sigma\big((2,3)\big) &= \#\{(2,3)+(0,0), (2,3)+(0,1), (2,3)+(1,0) \\ &\quad (2,3)+(1,1), (2,3)+(2,0), (2,3)+(2,1)\} = 6\end{aligned}$$

Order domain codes

Definition:
Let $\prec_w$ and I satisfy the order domain conditions. The semigroup $\Gamma := w(\Delta_{\prec_w}(I))$ is called the value semigroup.
For $\lambda \in w(\Delta_{\prec_w}(I_q)) \subseteq \Gamma$ define

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

Observation:
The above condition $\gamma - \lambda \in \Gamma$ can w.l.o.g. be replaced by $\gamma - \lambda \in w(\Delta_{\prec_w}(I_q))$.

Observation:
The value semigroup is generated by $w(X_1), \ldots, w(X_m)$. That is, $\Gamma = \langle w(X_1), \ldots, w(X_m)\rangle$.

Order domain codes

Definition:
Let $\prec_w$ and I satisfy the order domain conditions. Define

$$\begin{aligned} E(s) &= \{\mathrm{ev}(F(\vec{X} + I_q) \mid \mathrm{wdeg}(F) \leq s\} \\ &= C(I, L) \end{aligned}$$

where $L = \{M + I_q \mid M \in \Delta_{\prec_w}(I_q), w(M) \leq s\}$.
Define also

$$\begin{aligned} \tilde{E}(\delta) &= \mathrm{Span}_{\mathbf{F}_q}\{\mathrm{ev}(M + I_q) \mid \sigma(w(M)) \geq \delta\} \\ &= C(I, L') \end{aligned}$$

where $L' = \{M + I_q \mid M \in \Delta_{\prec_w}(I_q), \sigma(w(M)) = \bar{\sigma}(M) \geq \delta\}$.

Minimum distance of $E(s)$ and $\tilde{E}(\delta)$

According to theorem:

$d(E(s)) \geq \min\{\sigma(\lambda) \mid \lambda \leq s\}$

$d(\tilde{E}(\delta)) \geq \delta$.

Lemma:
If Γ is a numerical semigroup with finitely many gaps and $\lambda \in \Gamma$ then

$$\lambda = \#(\Gamma \backslash (\lambda + \Gamma))$$

where $\lambda + \Gamma = \{\lambda + \gamma \mid \gamma \in \Gamma\}$.

Observation:
For $\lambda \in w(\Delta_{\prec_w}(I_q))$, $\sigma(\lambda) = \# w(\Delta_{\prec_w}(I_q)) \cap (\lambda + \Gamma)$

Corollary:
Consider (numerical) weights. For $\lambda \in \Delta_{\prec_w}(I_q)$ we have $n - \lambda \leq \sigma(\lambda)$

Minimum distance of $E(s)$ - continued

Corollary:
For (numerical) weights and $\lambda \in \Delta_{\prec_w}(I_q)$ we have $n - \lambda \leq \sigma(\lambda)$

Theorem:
(For numerical weights) the minimum distance of $E(s)$ is at least $n - s$.

Well-behaving basis

$L \subseteq \mathbf{F}_q[\vec{X}]/I_q$.

Definition:
A basis $\{B_1 + I_q, \ldots, B_{\dim(L)} + I_q\}$ for $L \subseteq R_q$ where $\mathrm{Supp}(B_i) \subseteq \Delta_{\prec}(I_q)$ for $i = 1, \ldots, \dim(L)$ and where $\mathrm{lm}(B_1) \prec \cdots \prec \mathrm{lm}(B_{\dim(L)})$ is said to be well-behaving with respect to $\prec$.

Definition:

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

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

OWB

Definition:
Let $\mathcal{G}$ be a Gröbner basis for I_q with respect to $\prec$. Then (M_1, M_2), $M_1, M_2 \in \Delta_{\prec}(I_q)$ is said to be OWB if for all H with $\mathrm{Supp}(H) \subseteq \Delta_{\prec}(I_q)$ and $\mathrm{lm}(H) = M_1$

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

The Feng-Rao bound

Theorem:
Let $\prec$ be fixed. The minimum distance of $C(I,L)^{\perp}$ is at least

$$\min\Big\{\#\{P \in \Delta_{\prec}(I_q) \mid \exists N \in \Delta_{\prec}(I_q) \text{ such that } (P,N) \text{ is OWB} \\ \text{and } \operatorname{Im}(PN \text{ rem } \mathcal{G}) = K\}\Big| K \in \Delta_{\prec}(I_q)\backslash\Box_{\prec}(L)\Big\}. \quad (2)$$

$\mathbb{F}_9[X,Y]/I, \quad I = \langle X^9 - X, Y^9 - Y, X^4 - Y^3 - Y \rangle$

$w(X) = 3, w(Y) = 4$

Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	X^6Y^2	X^7Y^2	X^8Y^2
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	X^6Y	X^7Y	X^8Y
1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

3	6	9	12	15	18	21	24	27
2	4	6	8	11	14	17	20	23
1	2	3	4	7	10	13	16	19

$$\begin{aligned}
\bar{\mu}(X^4) &= \mu(12) \\
&= \#\{12-0, 12-3, 12-4, \\
&\qquad 12-6, 12-8, 12-9, 12-12\} \\
&= 7
\end{aligned}$$

Order domain theory

The order domain conditions: Let $\prec_w$ be a generalized weighted degree ordering on $\mathcal{M}(\vec{X})$. Let $I = \langle G_1(\vec{X}), \ldots, G_s(\vec{X})\rangle \subseteq \mathbf{F}_q[\vec{X}]$ be an ideal such that:

- $\{G_1, \ldots, G_s\}$ is a Gröbner basis for I w.r.t. $\prec_w$.
- For $i = 1, \ldots, s$ G_i has exactly two monomials of highest weight in its support.
- No two monomials in $\Delta_{\prec_w}(I)$ is of the same weight.

Definition:
Let $\prec_w$ and I satisfy the order domain conditions. The semigroup $\Gamma := w(\Delta_{\prec_w}(I))$ is called the value semigroup. For $\lambda \in w(\Delta_{\prec_w}(I_q)) \subseteq \Gamma$ define

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

Order domain codes

Definition:

Let $\prec_w$ and I satisfy the order domain conditions. Define

$$\begin{aligned} C(s) &= \{\vec{c} \mid \vec{c} \cdot \mathrm{ev}(F(\vec{X}) + I_q) = 0 \text{ for all } F \text{ with } \mathrm{wdeg}(F) \leq s\} \\ &= C^{\perp}(I, L) \end{aligned}$$

$$L = \mathrm{Span}_{\mathbf{F}_q}\{M + I_q \mid M \in \Delta_{\prec_w}(I_q), w(M) \leq s\}.$$

$$\begin{aligned} \tilde{C}(\delta) &= \{\vec{c} \mid \vec{c} \cdot \mathrm{ev}(M + I_q) = 0 \text{ for all } M \text{ with } \mu(w(M)) < \delta\} \\ &= C^{\perp}(I, L') \end{aligned}$$

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

By Feng-Rao theorem for general order domain code the minimum distance is at least $\min\{\mu(\lambda) \mid \lambda \in \Delta_{\prec_w}(I_q) \backslash \square_{\prec}(L)\}$.

$$d(C(s)) \geq \min\{\mu(\lambda) \mid \lambda \in \Delta_{\prec_w}(I_q), \lambda > s\}$$

$$d(\tilde{C}(\delta)) \geq \delta$$

Hermite codes over $\mathbf{F}_9$

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

3	6	9	12	15	18	21	24	27
2	4	6	8	11	14	17	20	23
1	2	3	4	7	10	13	16	19

$C^{\perp}(I, L)$ with $s = 7$: $d \geq 3, k = 22$
$C^{\perp}(I, L')$ with $\delta = 4$: $d \geq 4, k = 22$

GRM/Hyp codes over $\mathbf{F}_8$

Table below: σ/μ

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

Indeed, for appropriate choices of L and $\hat{L}$ we have $C(I,L) = C^{\perp}(I,\hat{L})$. This includes Generalized Reed-Muller codes and Hyperbolic codes.

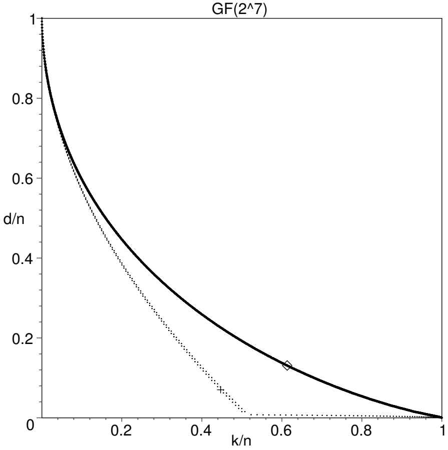
Hermite codes over $\mathbf{F}_9$

Table below: σ/μ

Y^2	$19/3$	$16/6$	$13/9$	$10/12$	$7/15$	$4/18$	$3/21$	$2/24$	$1/27$
Y	$23/2$	$20/4$	$17/6$	$14/8$	$11/11$	$8/14$	$6/17$	$4/20$	$2/23$
1	$27/1$	$24/2$	$21/3$	$18/4$	$15/7$	$12/10$	$9/13$	$6/16$	$3/19$
	1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

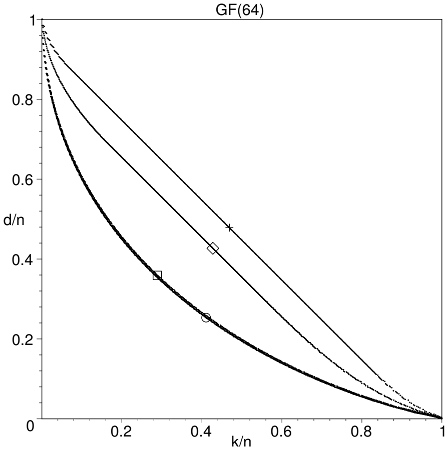
Indeed, for appropriate choices of L and $\hat{L}$ $C(I,L) = C^{\perp}(I,\hat{L})$.
Includes $E(s), \tilde{E}(\delta)$ versus $C(s), \tilde{C}(\delta)$.

$$I = \langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y \rangle \subseteq \mathbb{F}_{q^r}[X, Y]$$



Alphabet=$\mathbb{F}_{q^r} = \mathbb{F}_{2^7}$, $n = 2^{13}$ Improved versus non-improved.

$$I = \langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y \rangle \subseteq \mathbb{F}_{q^r}[X, Y]$$



Alphabet=$\mathbb{F}_{64}$. From above: $64 = 8^2$ gives $n = 2^9$, $64 = 4^3$ gives $n = 2^{10}$, $64 = 2^6$ gives $n = 2^{11}$, $\mathrm{Hyp}_{64}(s, 2)$ gives $n = 2^{12}$

A "non-duality example"

Consider the the generalized weighted degree ordering on $\mathcal{M}(X, Y, Z, U)$ with weights $w(X) = 64, w(Y) = 80, w(Z) = 100, w(U) = 125$. The ideal

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

and $\prec_w$ satisfies the order domain conditions. Expanding

$$\{X^{16}-X, Y^{16}-Y, Z^{16}-Z, U^{16}-U, X^5+Y^4+Y, Y^5+Z^4+Z, Z^5+U^4+U^2\}$$

to a Gröbner basis for I_q results in an awfully large basis. The leading monomials are:

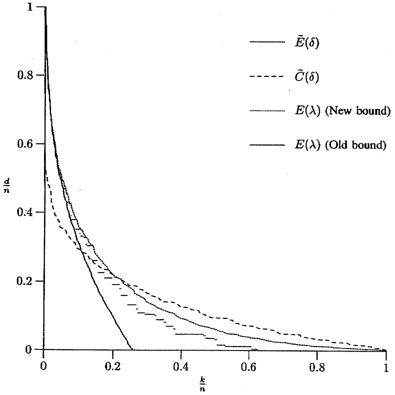
$$\{Y^4, Z^4, U^4, X^{10}Y^2Z^2, X^5Y^2ZU^2, X^{10}ZU^2, X^5Y^2Z^3, X^{10}Z^3, X^{10}Y^3, X^{15}, XY^3Z^3U^2, X^6Y^3U^2, X^{11}U^2, X^6Z^2U^2, X^6Y^3Z^2, X^{11}Y, X^{11}Z, X^6YZU^2, X^6YZ^3, X^{10}Y^2U^2, X^5YZ^2U^2\}.$$

The footprint does not have the shape of a box. By inspection $n = \Delta_{\prec_w}(I_q) = 512$.

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

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

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



Bad can be good...

$\vec{u} \cdot \vec{v} = \sum v_i u_i$ (usual inner product)

$\vec{u} * \vec{v} = (u_1 v_1, \ldots, u_m v_m)$ (Hadamard or "bad student" inner product).

$\vec{w} \cdot (\vec{v} * \vec{u}) = (\vec{w} * \vec{v}) \cdot \vec{u}$

$$\begin{aligned} & \vec{w} \cdot (\vec{v} * \vec{u}) \neq 0 \\ \Downarrow \quad & \\ & \vec{w} * \vec{v} \neq \vec{0} \end{aligned}$$

Proof of Feng-Rao bound

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

$$\vec{c} \cdot \mathrm{ev}(K + I_q) \neq 0 \tag{3}$$

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 (3) holds. By linearity of the inner product and the minimality of K we have $K \notin \square_\prec(L)$.

Proof of Feng-Rao bound - continued

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

$$\vec{c} \cdot \mathrm{ev}\left(\Big(\sum_{\substack{t = 1, \ldots, i \\ a_i \neq 0}} a_t P_t \Big) N_i \text{ rem } \mathcal{G} + I_q \right) \neq 0 \tag{4}$$

holds for any $i \in \{1, \ldots, \delta\}$.

Proof of Feng-Rao bound - continued

As

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

we conclude from (4) that

$$\vec{c} * \mathrm{ev}\Bigg(\Big(\sum_{\substack{t=1,\ldots,i\\ a_i\neq 0}} a_tP_t\Big)+I_q\Bigg) \neq \vec{0} \qquad \text{for any} \quad i \in \{1,\ldots,\delta\}$$

Proof of Feng-Rao bound - continued

Hence, $\vec{c} * \vec{e} \neq \vec{0}$ for all

$$\vec{e} \in \left\{ \mathrm{ev}\Big(\Big(\sum_{t=1}^{\delta} a_t P_t \Big) + I_q \Big) \Big| a_1, \ldots, a_\delta \in \mathbf{F}_q, \text{ not all } a_i \text{ equal } 0 \right\}. \tag{5}$$

The space consisting of (5) and $(0, \ldots, 0)$ is of dimension δ and therefore the Hamming weight of $\vec{c}$ needs to be at least δ.

Generalized weighted degree orderings

Definition:
Given $w(X_1), \ldots, w(X_m) \in \mathbf{N}_0^r$ define $w(X_1^{\alpha_1} \cdots X_m^{\alpha_m}) = \sum_{i=1}^m \alpha_i w(X_i)$. Let $\prec_{\mathbf{N}_0^r}$ be a monomial ordering on $\mathbf{N}_0^r$ and let $\prec_{\mathcal{M}}$ be a monomial ordering on $\mathcal{M}(X_1, \ldots, X_m)$. The generalized weighted degree ordering $\prec_w$ is the ordering with $\vec{X}^{\vec{\alpha}} \prec_w \vec{X}^{\vec{\beta}}$ if (1) or (2) holds:

(1) $w(\vec{X}^{\vec{\alpha}}) \prec_{\mathbf{N}_0^r} w(\vec{X}^{\vec{\beta}})$

(2) $w(\vec{X}^{\vec{\alpha}}) = w(\vec{X}^{\vec{\beta}})$ but $\vec{X}^{\vec{\alpha}} \prec_{\mathcal{M}} \vec{X}^{\vec{\beta}}$ holds

Order domain theory

The order domain conditions: Let $\prec_w$ be a generalized weighted degree ordering on $\mathcal{M}(\vec{X})$. Let $I = \langle G_1(\vec{X}), \ldots, G_s(\vec{X})\rangle \subseteq \mathbf{F}_q[\vec{X}]$ be an ideal such that:

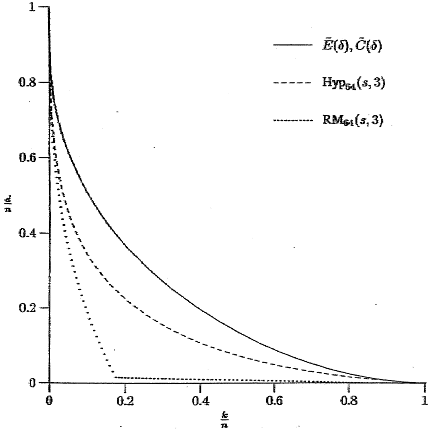
- $\{G_1, \ldots, G_s\}$ is a G¨röbner basis for I w.r.t. $\prec_w$.
- For $i = 1, \ldots, s$ G_i has exactly two monomials of highest weight (with respect to $\prec_{\mathbf{N}_0^r}$) in its support.
- No two monomials in $\Delta_{\prec_w}(I)$ is of the same weight.

The order domain conditions guarantees that we can use the same tricks as with the Hermitian codes (using the weights to determine OWB pairs).

$$I = \langle X^q + YZ^q - Y^q Z - X,\ U^q - Z^{q+1} + a X^q - a Y^q Z + b Y^{q+1} + U \rangle$$

$$\subseteq \mathbb{F}_{q^2}[X,Y,Z,U], \qquad a, b \in \mathbb{F}_q$$

$$w(X) = (q,1),\ w(Y) = (0,q),\ w(Z) = (q,0),\ w(U) = (q+1,0)$$



alphabet $= \mathbb{F}_{64}$, $n = 262144$

Tensor products of order domains

$R_1 = \mathbf{F}_q[\vec{X}]/I_1$
$I_1 = \langle F_1(\vec{X}), \ldots, F_{s_1}(\vec{X})\rangle$
$\prec_w^1$ is defined by weights in $\mathbf{N}_0^{r_1}$, $\prec_{\mathcal{M}(\vec{X})}$ and $\prec_{\mathbf{N}_o^{r_1}}$

$R_2 = \mathbf{F}_q[\vec{Y}]/I_2$
$I_2 = \langle G_1(\vec{Y}), \ldots, G_{s_2}(\vec{Y})\rangle$
$\prec_w^2$ is defined by weights in $\mathbf{N}_0^{r_1}$, $\prec_{\mathcal{M}(\vec{Y})}$ and $\prec_{\mathbf{N}_o^{r_2}}$

$R = \mathbf{F}_q[\vec{X}, \vec{Y}]/I$
$I = \langle F_1(\vec{X}), \ldots, F_{s_1}(\vec{X}), G_1(\vec{Y}), \ldots, G_{s_2}(\vec{Y})\rangle$
$\prec_w$ is defined by weights in $\mathbf{N}_0^{r_1+r_2}$ as follows
$w(\vec{X}^{\vec{\alpha}}\vec{Y}^{\vec{\beta}}) = (w(\vec{X}), w(\vec{Y}))$
Choose $\prec_{\mathcal{M}(\vec{X},\vec{Y})}$ and $\prec_{\mathbf{N}_0^{r_1+r_2}}$ with care.

Example: The structures supporting the generalized Reed Muller codes and the hyperbolic codes fits this general description.

Generalized Reed-Muller codes revisited

$w(X^iY^j) = (i,j)$

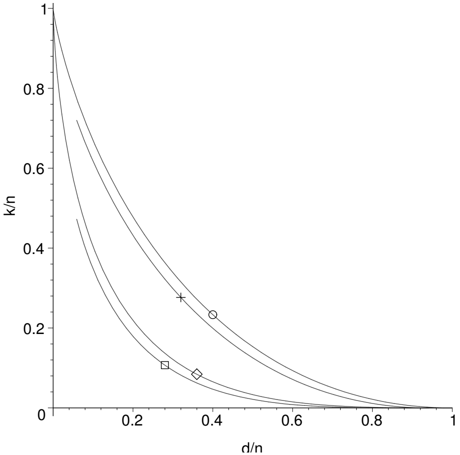
$I = \langle 0 \rangle \subseteq \mathbf{F}_5[X,Y]$. $I_5 = \langle X^5 - X, Y^5 - Y \rangle$.

$$\begin{array}{c|ccccc}
Y^4 & (0,4) & (1,4) & (2,4) & (3,4) & (4,4) \\
Y^3 & (0,3) & (1,3) & (2,3) & (3,3) & (4,3) \\
Y^2 & (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \\
Y & (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\
1 & (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \\
\hline
 & 1 & X & X^2 & X^3 & X^4
\end{array}$$

$$\begin{array}{c|ccccc}
Y^4 & 5 & 4 & 3 & 2 & 1 \\
Y^3 & 10 & 8 & 6 & 4 & 2 \\
Y^2 & 15 & 12 & 9 & 6 & 3 \\
Y & 20 & 16 & 12 & 8 & 4 \\
1 & 25 & 20 & 15 & 10 & 5 \\
\hline
 & 1 & X & X^2 & X^3 & X^4
\end{array}$$

$$\begin{aligned}
\sigma\big((2,3)\big) \quad = \quad & \#\{(2,3)+(0,0), (2,3)+(0,1), (2,3)+(1,0) \\
& (2,3)+(1,1), (2,3)+(2,0), (2,3)+(2,1)\} = 6
\end{aligned}$$

Tensor product of m Hermitian order domains involves weights in $\mathbf{N}_0^m$.



Alphabet=$\mathbb{F}_{256}$. From above: $\mathrm{Hyp}_{256}(s,2)$ of length $n = 65536$, $\mathrm{Herm}_{256}(s,2)$ of length $n = 16777216$, $\mathrm{Hyp}_{256}(s,3)$ of length $n = 16777216$, $\mathrm{Herm}_{256}(s,3)$ of length $n = 68719476736$.

Order functions

Definition:
Let $(\Gamma, <)$ be a well-order. An order function on an **F**-algebra R is a surjective function

$$\rho : R \to \Gamma \cup \{-\infty\}$$

such that

(O.0) $\rho(f) = -\infty$ iff $f = 0$

(O.1) $\rho(af) = \rho(f)$ for all nonzero $a \in \mathbf{F}$

(O.2) $\rho(f+g) \leq \max\{\rho(f), \rho(g)\}$

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

(O.4) If f and g are nonzero and $\rho(f) = \rho(g)$ then there exists a nonzero $a \in \mathbf{F}$ such that $\rho(f - ag) < \rho(g)$

Weight functions

An order function induces an operation $+$ on R by:

(O.5) $\rho(f) + \rho(g) = \rho(fg)$

Definition:
Let $(\Gamma, +)$ be a sub structure of $(\mathbf{N}_o^r, +)$ and assume $(O.0), \ldots, (O.5)$ are satisfied. Then ρ is called a weight function.

Theorem:
If Γ is finitely generated then ρ is a weight function and $R \simeq \mathbf{F}[\vec{X}]/I$ for some I satisfying the order domain conditions.

Some results

R is an integral domain.

Let ρ be a weight function. The smallest number r such that $\Gamma \subseteq \mathbf{N}_0^r$ (up to isomorphism) satisfies $r = \mathrm{trdg}(Quot(R))$

When weights are numerical we have: $R \subseteq \cup_{m=0}^{\infty} \mathcal{L}(mP)$ where P is a rational place (a point) in some algebraic function field of one variable (coming from a curve)
Given the description $R \simeq \mathbf{F}[\vec{X}]/I$ from the above theorem, all rational places (points) except P are affine!

Given an algebraic function field of one variable and a rational place (point) then any subring $R \subseteq \cup_{m=0}^{\infty} \mathcal{L}(mP)$ is an order domain.

The codes

Codes from order domains with numerical weights correspond to one-point geometric Goppa codes (and one-point geometric Reed-Solomon codes). We do not need Riemann-Roch. Improvements easily handled. Treatment of more point codes requires generalization of order function.

We have an easy generalization of one-point codes to structures of higher transcendence degree.

Warning

Given algebraic function field and place (point) it is not in general easy to find

$$R = \cup_{m=0}^{\infty} \mathcal{L}(mP)$$

Neither is it easy to find the ideal I such that $R = \mathbf{F}_q[\vec{X}]/I$.

But, such an I exists and allows for theoretical treatment.

A non order-domain example

$$I = \langle X^3Y + Y^3 + X \rangle \subseteq \mathbf{F}_8[X, Y]$$
$$I_8 = \langle X^3Y + Y^3 + X, X^8 + X, Y^8 + Y \rangle$$
$w(X) = 2$ and $w(Y) = 3$.

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

with corresponding weights

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

Can still determine OWB pairs. However, more involved.

Decoding

General affine variety code:

- Fitzgerald and Lax
- Farr and Gao

Order domain codes:

- Høholdt, van Lint and Pellikaan via improved BMS-algorithm
- Improvements to above algorithm
- Attempt to Sudan-likde decode (Matsumoto and G)

When order domains are of transcendence degree 1, well-known and strong decoding algorithms from theory of AG codes exists.

Minimum distance decoding of Reed-Solomon codes

Consider a Reed-Solomon code
$\mathrm{RS}_q(k) = \{(F(P_1), \ldots, F(P_q)) \mid \deg(F) < k\}$.
Define $t = \lfloor (d-1)/2 \rfloor = \lfloor (q-k)/2 \rfloor$.

If we receive $\vec{r} = (r_1, \ldots, r_q)$ then we determine a non zero polynomial

$$Q(X,Y) = Q_0(X) + YQ_1(X)$$

that satisfies the following

- $Q(P_1, r_1) = 0$, $Q(P_2, r_2) = 0, \ldots, Q(P_q, r_q) = 0$
- $\deg(Q_0) \leq q - 1 - t = l_0$
- $\deg(Q_1) \leq t = l_1$

How can we be sure that such a polynomial $Q(X, Y)$ exists?

Let $Q_0(X) = Q_{0,0} + Q_{0,1}X + Q_{0,2}X^2 + \cdots + Q_{0,l_0}X^{l_0}$ and $Q_1(X) = Q_{1,0} + Q_{1,1}X + \cdots + Q_{1,l_1}X^{l_1}$. We get

$$
\begin{aligned}
& Q(P_1, r_1) = 0 \\
\Updownarrow \quad & \\
& Q_{0,0} + Q_{0,1}P_1 + Q_{0,2}P_1^2 + \cdots + Q_{0,l_0}P_1^{l_0} \\
& \qquad + Q_{1,0}r_1 + Q_{1,1}r_1P_1 + \cdots + Q_{1,l_1}r_1P_1^{l_1} = 0
\end{aligned}
$$

This is a homogeneous equation with $(l_0 + 1) + (l_1 + 1) = q + 1$ unknown (the $Q_{i,j}$'s).

There are q such equations. A homogeneous system of linear equations with more unknowns than equations possesses a non zero solution.

In matrix form we have:

$$\begin{bmatrix} 1 & P_1 & P_1^2 & \cdots & P_1^{l_0} & r_1 & r_1P_1 & \cdots & r_1P_1^{l_1} \\ 1 & P_2 & P_2^2 & \cdots & P_2^{l_0} & r_2 & r_2P_2 & \cdots & r_2P_2^{l_1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & P_q & P_q^2 & \cdots & P_q^{l_0} & r_q & r_qP_q & \cdots & r_qP_q^{l_1} \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ \vdots \\ Q_{0,l_0} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Assume $\vec{c} = (F(P_1), F(P_2), \ldots, F(P_q))$ was send (it is unknown to us) and assume that at most t errors occurred under transmission.

We have $Q(P_1, r_1) = Q(P_2, r_2) = \cdots = Q(P_q, r_q) = 0$ and as at most t errors occurred at least $q - t$ zeros among

$$Q(P_1, F(P_1)), Q(P_2, F(P_2)), \ldots, Q(P_q, F(P_q))$$

Interpret $Q(X, F(X)) = Q_0 + F(X)Q_1(X)$ as a polynomial in X. It is of degree at most max$\{q - 1 - t, (k - 1) + t\} = q - 1 - t$. A polynomial of degree at most $q - 1 - t$, that has at least $q - t$ zeros is the zero-polynomial 0. We get

$$Q(X, F(X)) = 0$$

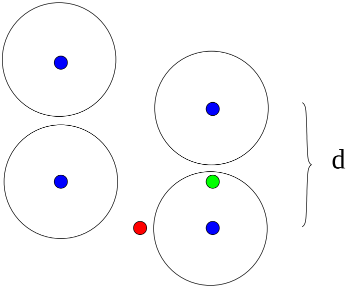
$$\Updownarrow$$

$$Q_0(X) + F(X)Q_1(X) = 0$$

$$\Updownarrow$$

$$F(X) = -\frac{Q_0(X)}{Q_1(X)}$$

List decoding



There does not always exists a code word within the distance $t = \lfloor (d-1)/2 \rfloor$ from the received word $\vec{r}$. In such a case we would like to investigate greater radii than t. Using such a method we must accept to sometimes find more candidates for the send word.

The minimum distance decoding method is generalized to list decoding as follows:

Look for $Q(X,Y) = Q_0(X) + Q_1(X)Y + \cdots + Q_m(X)Y^m$ such that

- $Q(P_i, r_i) = 0$ for $i = 1, \ldots, q$
- Certain degree conditions on the Q_i's must be satisfied

Determine all factors $Y - F(X)$ i $Q(X,Y)$. There can at most be m such factors (in by far most cases only one factor).

The method can be further improved, if zeros are counted with multiplicity. Multiplicity of polynomials in more variables is not a trivial thing. Many different definitions exist.

Above method can be generalized to work also for order domain codes: Arguments involves the σ function. We cannot yet deal with multiplicities. (Except in the case of one-point geometric Goppa codes and generalized Reed-Muller codes).