Order Domain Codes

O. Geil

Aalborg University

Special Semester on Gröbner Bases and Related Methods, 2006

Outline

What are we aiming at?

Order domain codes - part I (generator matrix)

- Motivating examples
- The general set-up

Order domain codes - part II (parity check matrix)

- Motivating examples
- The general set-up

More examples

Conlusion remarks

Reed-Solomon Codes

$$R = F_q[X], \quad R_s = \{F \in \mathbb{F}_q[X] \mid \deg(F) \le s\}$$

$$\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$$

$$\varphi : \begin{cases} R & \rightarrow & \mathbb{F}_q^n \\ F & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$C(s) = \varphi(R_s) = (C(n-s-2))^{\perp}, \quad s \in \{0, \ldots, n-1\}$$

+ Large minimum distance
+ Well-structured
+ Simple description
- Short

Reed-Solomon Codes

$$R = F_q[X], \quad R_s = \{F \in \mathbb{F}_q[X] \mid \deg(F) \leq s\}$$

$$\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$$

$$\varphi : \begin{cases} R & \longrightarrow & \mathbb{F}_q^n \\ F & \longmapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$C(s) = \varphi(R_s) = (C(n-s-2))^{\perp}, \quad s \in \{0, \ldots, n-1\}$$

- + Large minimum distance
- + Well-structured
- + Simple description
- \- Short

Reed-Solomon Codes

$$R = F_q[X], \quad R_s = \{F \in \mathbb{F}_q[X] \mid \deg(F) \leq s\}$$

$$\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$$

$$\varphi : \left\{ \begin{array}{ccc} R & \longrightarrow & \mathbb{F}_q^n \\ F & \longmapsto & (F(P_1), \ldots, F(P_n)) \end{array} \right.$$

$$C(s) = \varphi(R_s) = (C(n-s-2))^{\perp}, \quad s \in \{0, \ldots, n-1\}$$

+ Large minimum distance
+ Well-structured
+ Simple description
- Short

Reed-Solomon Codes

$$R = F_q[X], \quad R_s = \{F \in \mathbb{F}_q[X] \mid \deg(F) \leq s\}$$

$$\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$$

$$\varphi : \begin{cases} R & \longrightarrow & \mathbb{F}_q^n \\ F & \longmapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$C(s) = \varphi(R_s) = (C(n - s - 2))^{\perp}, \quad s \in \{0, \ldots, n - 1\}$$

+ Large minimum distance
+ Well-structured
+ Simple description
- Short

Reed-Solomon Codes

$$R = F_q[X], \quad R_s = \{F \in \mathbb{F}_q[X] \mid \deg(F) \leq s\}$$

$$\{P_1, \ldots, P_n\} \subseteq \mathbb{F}_q$$

$$\varphi : \left\{ \begin{array}{ccc} R & \longrightarrow & \mathbb{F}_q^n \\ F & \longmapsto & (F(P_1), \ldots, F(P_n)) \end{array} \right.$$

$$C(s) = \varphi(R_s) = (C(n - s - 2))^{\perp}, \quad s \in \{0, \ldots, n - 1\}$$

- + Large minimum distance
- + Well-structured
- + Simple description
- \- Short

Generalizing Reed-Solomon Codes

- Well-established theory
  - (Generalized) Reed-Muller codes
  - Geometric Goppa codes
- New theory
  - Order domain codes
  - Affine variety codes

Generalizing Reed-Solomon Codes

- Well-established theory
  - (Generalized) Reed-Muller codes
  - Geometric Goppa codes
- New theory
  - Order domain codes
  - Affine variety codes

Gröbner basis tools

Footprint (Δ-set):

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

$\{M + I \mid M \in \Delta_{\prec}(I)\}$ a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$.

$\#\mathbb{V}_{\mathbb{F}}(I) \leq \#\Delta_{\prec}(I)$ with equality if $\mathbb{F}$ is algebraically closed and I radical

Gröbner basis tools

Footprint (Δ-set):

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

$\{M + I \mid M \in \Delta_{\prec}(I)\}$ a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$.

$\#\mathbb{V}_{\mathbb{F}}(I) \leq \#\Delta_{\prec}(I)$ with equality if $\mathbb{F}$ is algebraically closed and I radical

Gröbner basis tools

Footprint (Δ-set):

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

$\{M + I \mid M \in \Delta_{\prec}(I)\}$ a basis for $\mathbb{F}[X_1, \ldots, X_m]/I$.

$\#\mathbb{V}_{\mathbb{F}}(I) \leq \#\Delta_{\prec}(I)$ with equality if $\mathbb{F}$ is algebraically closed and I radical

Reed-Muller codes and hyperbolic codes

$$R := \mathbb{F}_5[X,Y]/\langle X^5 - X, Y^5 - Y\rangle$$

$\Delta_\prec(\langle X^5 - X, Y^5 - Y\rangle)$ $\quad$ $\#\Delta_\prec(\langle X^5, Y^5, X^iY^j\rangle)$

Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4	20	21	22	23	24
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3	15	17	19	21	23
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	10	13	16	19	22
Y	XY	X^2Y	X^3Y	X^4Y	5	9	13	17	21
1	X	X^2	X^3	X^4	0	5	10	15	20

$$G(X,Y) = XY + aX^2 + bY + cX + d$$

$$\begin{aligned}\#\Delta_\prec(\langle X^5 - X, Y^5 - Y, G(X,Y)\rangle) &\leq \#\Delta_\prec(\langle X^5, Y^5, XY\rangle)\\ &\leq 9\end{aligned}$$

$\mathbb{F}_5^2 = \{P_1 \ldots P_{25}\}$ $\varphi(F + \langle X^5 - X, Y^5 - Y\rangle) = (F(P_1), \ldots, F(P_{25}))$
$w_H(\varphi(G)) \geq 25 - 9 = 16$

Reed-Muller codes and hyperbolic codes

$$R := \mathbb{F}_5[X,Y]/\langle X^5 - X, Y^5 - Y\rangle$$

$$\Delta_{\prec}(\langle X^5 - X, Y^5 - Y\rangle) \qquad \#\Delta_{\prec}(\langle X^5, Y^5, X^iY^j\rangle)$$

$$\begin{array}{ccccc} Y^4 & XY^4 & X^2Y^4 & X^3Y^4 & X^4Y^4 \\ Y^3 & XY^3 & X^2Y^3 & X^3Y^3 & X^4Y^3 \\ Y^2 & XY^2 & X^2Y^2 & X^3Y^2 & X^4Y^2 \\ Y & XY & X^2Y & X^3Y & X^4Y \\ 1 & X & X^2 & X^3 & X^4 \end{array} \qquad \begin{array}{ccccc} 20 & 21 & 22 & 23 & 24 \\ 15 & 17 & 19 & 21 & 23 \\ 10 & 13 & 16 & 19 & 22 \\ 5 & 9 & 13 & 17 & 21 \\ 0 & 5 & 10 & 15 & 20 \end{array}$$

$$G(X,Y) = XY + aX^2 + bY + cX + d$$

$$\begin{aligned} \#\Delta_{\prec}(\langle X^5 - X, Y^5 - Y, G(X,Y)\rangle) &\leq \#\Delta_{\prec}(\langle X^5, Y^5, XY\rangle) \\ &\leq 9 \end{aligned}$$

$\mathbb{F}_5^2 = \{P_1 \ldots P_{25}\}$ $\varphi(F + \langle X^5 - X, Y^5 - Y\rangle) = (F(P_1), \ldots, F(P_{25}))$
$w_H(\varphi(G)) \geq 25 - 9 = 16$

Reed-Muller codes and hyperbolic codes

$$R := \mathbb{F}_5[X,Y]/\langle X^5 - X, Y^5 - Y\rangle$$

$\Delta_\prec(\langle X^5 - X, Y^5 - Y\rangle)$ and $\#\Delta_\prec(\langle X^5, Y^5, X^iY^j\rangle)$:

Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4	20	21	22	23	24
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3	15	17	19	21	23
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	10	13	16	19	22
Y	XY	X^2Y	X^3Y	X^4Y	5	9	13	17	21
1	X	X^2	X^3	X^4	0	5	10	15	20

$$G(X,Y) = XY + aX^2 + bY + cX + d$$

$$\begin{aligned} \#\Delta_\prec(\langle X^5 - X, Y^5 - Y, G(X,Y)\rangle) &\leq \#\Delta_\prec(\langle X^5, Y^5, XY\rangle) \\ &\leq 9 \end{aligned}$$

$\mathbb{F}_5^2 = \{P_1 \ldots P_{25}\}$ $\varphi(F + \langle X^5 - X, Y^5 - Y\rangle) = (F(P_1), \ldots, F(P_{25}))$

$w_H(\varphi(G)) \geq 25 - 9 = 16$

Reed-Muller codes and hyperbolic codes

$$R := \mathbb{F}_5[X,Y]/\langle X^5 - X, Y^5 - Y\rangle$$

$$\Delta_{\prec}(\langle X^5 - X, Y^5 - Y\rangle) \qquad \#\Delta_{\prec}(\langle X^5, Y^5, X^iY^j\rangle)$$

Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4	20	21	22	23	24
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3	15	17	19	21	23
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	10	13	16	19	22
Y	XY	X^2Y	X^3Y	X^4Y	5	9	13	17	21
1	X	X^2	X^3	X^4	0	5	10	15	20

$$G(X,Y) = XY + aX^2 + bY + cX + d$$

$$\begin{aligned}\#\Delta_{\prec}(\langle X^5 - X, Y^5 - Y, G(X,Y)\rangle) &\leq \#\Delta_{\prec}(\langle X^5, Y^5, XY\rangle)\\ &\leq 9\end{aligned}$$

$\mathbb{F}_5^2 = \{P_1 \ldots P_{25}\}$ $\varphi(F + \langle X^5 - X, Y^5 - Y\rangle) = (F(P_1), \ldots, F(P_{25}))$
$w_H(\varphi(G)) \geq 25 - 9 = 16$

(Generalized) Reed-Muller codes

$$\mathrm{RM}_5(4,2) = \{\mathrm{Span}_{\mathbb{F}_5}\{\varphi(X^iY^j) \mid i+j \leq 4\}$$

$$\Delta_{\prec}(\langle X^5 - X, Y^5 - Y\rangle) \qquad \#\Delta_{\prec}(\langle X^5, Y^5, X^iY^j\rangle)$$

$$\begin{array}{ccccc}
Y^4 & * & * & * & * \\
Y^4 & XY^3 & * & * & * \\
Y^2 & XY^2 & X^2Y^2 & * & * \\
Y & XY & X^2Y & X^3Y & * \\
1 & X & X^2 & X^3 & X^4
\end{array}
\qquad
\begin{array}{ccccc}
20 & * & * & * & * \\
15 & 17 & * & * & * \\
10 & 13 & 16 & * & * \\
5 & 9 & 13 & 17 & * \\
0 & 5 & 10 & 15 & 20
\end{array}$$

Worstcase code word: $\mathrm{Im} = Y^4$ or $\mathrm{Im} = X^4$

$w_H(Y^4 + \cdots) \geq 25 - 20 = 5$

$[n,k,d] = [25,15,5]$

(Generalized) Reed-Muller codes

$$\mathrm{RM}_5(4,2) = \{\mathrm{Span}_{\mathbb{F}_5}\{\varphi(X^iY^j) \mid i+j \leq 4\}$$

$$\Delta_{\prec}(\langle X^5 - X, Y^5 - Y\rangle) \qquad \#\Delta_{\prec}(\langle X^5, Y^5, X^iY^j\rangle)$$

Y^4	$*$	$*$	$*$	$*$	20	$*$	$*$	$*$	$*$
Y^4	XY^3	$*$	$*$	$*$	15	17	$*$	$*$	$*$
Y^2	XY^2	X^2Y^2	$*$	$*$	10	13	16	$*$	$*$
Y	XY	X^2Y	X^3Y	$*$	5	9	13	17	$*$
1	X	X^2	X^3	X^4	0	5	10	15	20

Worstcase code word: $\mathrm{lm} = Y^4$ or $\mathrm{lm} = X^4$
$w_H(Y^4 + \cdots) \geq 25 - 20 = 5$
$[n, k, d] = [25, 15, 5]$

Hyperbolic codes

Choose X^iY^j's with $\#\Delta(\langle X^5, Y^5, X^iY^j\rangle)$ small.

$[25, 17, 5]$

20	$*$	$*$	$*$	$*$
15	17	19	$*$	$*$
10	13	16	19	$*$
5	9	13	17	$*$
0	5	10	15	20

$[25, 15, 6]$

$*$	$*$	$*$	$*$	$*$
15	17	19	$*$	$*$
10	13	16	19	$*$
5	9	13	17	$*$
0	5	10	15	$*$

Hyperbolic codes

Choose X^iY^j's with $\#\Delta(\langle X^5, Y^5, X^iY^j\rangle)$ small.

$[25, 17, 5]$

20	$*$	$*$	$*$	$*$
15	17	19	$*$	$*$
10	13	16	19	$*$
5	9	13	17	$*$
0	5	10	15	20

$[25, 15, 6]$

$*$	$*$	$*$	$*$	$*$
15	17	19	$*$	$*$
10	13	16	19	$*$
5	9	13	17	$*$
0	5	10	15	$*$

$\mathbb{F}_8[X, Y]/\langle X^8 - X, Y^8 - Y\rangle$

56	57	58	59	60	61	62	63
48	50	52	54	56	58	60	62
40	43	46	49	52	55	58	61
32	36	40	44	48	52	56	60
24	29	34	39	44	49	54	59
16	22	28	34	40	46	52	58
8	15	22	29	36	43	50	57
0	8	16	24	32	40	48	56

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

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

Codes from Hermitian curve

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

Let $w(X^iY^j) = i2 + j3$ and define $\prec_w$ by: $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X^\alpha Y^\beta) < w(X^\gamma Y^\beta) \\ (2) & w(X^\alpha Y^\beta) = w(X^\gamma Y^\beta) \text{ and } \beta < \delta \end{array}$$

$\Delta_{\prec_w}(I)$				$w(X^iY^j)$				$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
Y	XY	X^2Y	X^3Y	3	5	7	9	3	5	6	7
1	X	X^2	X^3	0	2	4	6	0	2	4	6

$$\begin{aligned} & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \\ \leq\ & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y, X^3\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3 \\ =\ & \#\Delta_{\prec_w}(I) - \#\{3+0, 3+2, 3+3, 3+4, 3+6\} \end{aligned}$$

Codes from Hermitian curve

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

Let $w(X^iY^j) = i2 + j3$ and define $\prec_w$ by: $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X^\alpha Y^\beta) < w(X^\gamma Y^\beta) \\ (2) & w(X^\alpha Y^\beta) = w(X^\gamma Y^\beta) \text{ and } \beta < \delta \end{array}$$

$\Delta_{\prec_w}(I)$				$w(X^iY^j)$				$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
Y	XY	X^2Y	X^3Y	3	5	7	9	3	5	6	7
1	X	X^2	X^3	0	2	4	6	0	2	4	6

$$\begin{aligned} & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \\ \leq\ & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y, X^3\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3 \\ =\ & \#\Delta_{\prec_w}(I) - \#\{3+0, 3+2, 3+3, 3+4, 3+6\} \end{aligned}$$

Codes from Hermitian curve

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

Let $w(X^iY^j) = i2 + j3$ and define $\prec_w$ by: $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X^\alpha Y^\beta) < w(X^\gamma Y^\beta) \\ (2) & w(X^\alpha Y^\beta) = w(X^\gamma Y^\beta) \text{ and } \beta < \delta \end{array}$$

$$\begin{array}{cccc} \multicolumn{4}{c}{\Delta_{\prec_w}(I)} \\ Y & XY & X^2Y & X^3Y \\ 1 & X & X^2 & X^3 \end{array} \qquad \begin{array}{cccc} \multicolumn{4}{c}{w(X^iY^j)} \\ 3 & 5 & 7 & 9 \\ 0 & 2 & 4 & 6 \end{array} \qquad \begin{array}{cccc} \multicolumn{4}{c}{\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)} \\ 3 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 \end{array}$$

$$\begin{aligned} & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \\ \leq\ & \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y, X^3\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3 \\ =\ & \#\Delta_{\prec_w}(I) - \#\{3+0, 3+2, 3+3, 3+4, 3+6\} \end{aligned}$$

$G(X,Y) = Y + aX + b$
$\#\Delta_{\prec_w}(I \cup \langle G(X,Y)\rangle) \leq \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3$

$\mathbb{V}_{\mathbb{F}_4}(I) = \{P_1, \ldots, P_8\}$ $\varphi(F+I) = (F(P_1), \ldots, F(P_8))$
$w_H(\varphi(G)) \geq 8 - 3 = 5$

$w(X^iY^j)$				$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
3	5	7	9	3	5	6	7
0	2	4	6	0	2	4	6

$E(0)$ is $[8,1,8]$, $E(2)$ is $[8,2,6]$,...,$E(6)$ is $[8,6,2]$, $E(7)$ is $[8,7,2]$ and $E(9]$ is $[8,8,1]$

..., $\tilde{E}(5)$ is $[8,5,3]$, $\tilde{E}(6)$ is $[8,7,2]$, ...

$G(X,Y) = Y + aX + b$
$\#\Delta_{\prec_w}(I \cup \langle G(X,Y)\rangle) \leq \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3$

$\mathbb{V}_{\mathbb{F}_4}(I) = \{P_1, \ldots, P_8\} \quad \varphi(F + I) = (F(P_1), \ldots, F(P_8))$
$w_H(\varphi(G)) \geq 8 - 3 = 5$

$w(X^iY^j)$				$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
3	5	7	9	3	5	6	7
0	2	4	6	0	2	4	6

$E(0)$ is $[8,1,8]$, $E(2)$ is $[8,2,6]$,...,$E(6)$ is $[8,6,2]$, $E(7)$ is $[8,7,2]$ and $E(9]$ is $[8,8,1]$

..., $\tilde{E}(5)$ is $[8,5,3]$, $\tilde{E}(6)$ is $[8,7,2]$, ...

$G(X,Y) = Y + aX + b$
$\#\Delta_{\prec_w}(I \cup \langle G(X,Y)\rangle) \leq \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3$

$\mathbb{V}_{\mathbb{F}_4}(I) = \{P_1, \ldots, P_8\} \quad \varphi(F + I) = (F(P_1), \ldots, F(P_8))$
$w_H(\varphi(G)) \geq 8 - 3 = 5$

$w(X^iY^j)$			
3	5	7	9
0	2	4	6

$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
3	5	6	7
0	2	4	6

$E(0)$ is $[8,1,8]$, $E(2)$ is $[8,2,6]$,...,$E(6)$ is $[8,6,2]$, $E(7)$ is $[8,7,2]$ and $E(9]$ is $[8,8,1]$

..., $\tilde{E}(5)$ is $[8,5,3]$, $\tilde{E}(6)$ is $[8,7,2]$, ...

$G(X,Y) = Y + aX + b$
$\#\Delta_{\prec_w}(I \cup \langle G(X,Y)\rangle) \leq \#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, Y\rangle) \cap \Delta_{\prec_w}(I)\right) \leq 3$

$\mathbb{V}_{\mathbb{F}_4}(I) = \{P_1, \ldots, P_8\}$ $\quad \varphi(F + I) = (F(P_1), \ldots, F(P_8))$
$w_H(\varphi(G)) \geq 8 - 3 = 5$

$w(X^iY^j)$				$\#\left(\Delta_{\prec_w}(\langle X^3 - Y^2, X^iY^j\rangle) \cap \Delta_{\prec_w}(I)\right)$			
3	5	7	9	3	5	6	7
0	2	4	6	0	2	4	6

$E(0)$ is $[8,1,8]$, $E(2)$ is $[8,2,6]$,...,$E(6)$ is $[8,6,2]$, $E(7)$ is $[8,7,2]$ and $E(9]$ is $[8,8,1]$

..., $\tilde{E}(5)$ is $[8,5,3]$, $\tilde{E}(6)$ is $[8,7,2]$, ...

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

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

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

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

$\#\left(\Delta_{\prec_w}(\langle X^4 - Y^3, X^4Y^2 \rangle) \cap \Delta_{\prec_w}(I)\right) =$
$27 - \#\{20+0, 20+3, 20+4, 20+6, 20+8, 20+9, 20+12\} = 20$

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

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

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

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

$\#\left(\Delta_{\prec_w}(\langle X^4 - Y^3, X^4Y^2\rangle) \cap \Delta_{\prec_w}(I)\right) =$
$27 - \#\{20+0, 20+3, 20+4, 20+6, 20+8, 20+9, 20+12\} = 20$

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

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

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

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

$$\#\left(\Delta_{\prec_w}(\langle X^4 - Y^3, X^4Y^2\rangle) \cap \Delta_{\prec_w}(I)\right) =$$
$$27 - \#\{20+0, 20+3, 20+4, 20+6, 20+8, 20+9, 20+12\} = 20$$

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

$E(23)$ is $[27, 21, 4]$
but
$\tilde{E}(4)$ is $[27, 22, 4]$

Reed-Muller codes revisited

$w(X^iY^j) = (i,j) \in \mathbb{N}_0^2$. Choose some monomial ordering $\prec_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$. Choose some monomial ordering $\prec_{\mathcal{M}}$ on $\mathcal{M}(X,Y)$ and define $\prec_w$ by: $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X^\alpha Y^\beta) \prec_{\mathbb{N}_0^2} w(X^\gamma Y^\beta) \\ (2) & w(X^\alpha Y^\beta) = w(X^\gamma Y^\beta) \text{ and } X^\alpha Y^\beta \prec_{\mathcal{M}} X^\gamma Y^\delta \end{array}$$

$w(X^i, Y^j)$					$\#\Delta_\prec(\langle X^5, Y^5, X^iY^j\rangle)$				
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	20	21	22	23	24
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	15	17	19	21	23
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	10	13	16	19	22
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	5	9	13	17	21
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	0	5	10	15	20

$\#\Delta(\langle X^5, Y^5, X^3Y^3\rangle) =$
$25 - \#\{(3,3)+(0,0), (3,3)+(1,0), (3,3)+(0,1), (3,3)+(1,1)\}$

Reed-Muller codes revisited

$w(X^iY^j)=(i,j)\in\mathbb{N}_0^2$. Choose some monomial ordering $\prec_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$. Choose some monomial ordering $\prec_{\mathcal{M}}$ on $\mathcal{M}(X,Y)$ and define $\prec_w$ by: $X^\alpha Y^\beta \prec_w X^\gamma Y^\delta$ if (1) or (2) holds

$$\begin{array}{ll} (1) & w(X^\alpha Y^\beta) \prec_{\mathbb{N}_0^2} w(X^\gamma Y^\beta) \\ (2) & w(X^\alpha Y^\beta) = w(X^\gamma Y^\beta) \text{ and } X^\alpha Y^\beta \prec_{\mathcal{M}} X^\gamma Y^\delta \end{array}$$

$$\begin{array}{ccccc} & & w(X^i,Y^j) & & \\ (0,4) & (1,4) & (2,4) & (3,4) & (4,4) \\ (0,3) & (1,3) & (2,3) & (3,3) & (4,3) \\ (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \\ (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\ (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \end{array} \qquad \begin{array}{ccccc} & & \#\Delta_\prec(\langle X^5,Y^5,X^iY^j\rangle) & & \\ 20 & 21 & 22 & 23 & 24 \\ 15 & 17 & 19 & 21 & 23 \\ 10 & 13 & 16 & 19 & 22 \\ 5 & 9 & 13 & 17 & 21 \\ 0 & 5 & 10 & 15 & 20 \end{array}$$

$\#\Delta(\langle X^5,Y^5,X^3Y^3\rangle)=$
$25-\#\{(3,3)+(0,0),(3,3)+(1,0),(3,3)+(0,1),(3,3)+(1,1)\}$

Some observations

- $$\begin{aligned} w_H(\vec{c}) &\geq n - \#\Delta(\cdots) = n - (n - \#\text{“what the weight hits”}) \\ &= \#\text{“what the weight hits”} \end{aligned}$$
- Monomials in the footprint are of different weights which makes the counting simple.

Some observations

- $$\begin{aligned} w_H(\vec{c}) &\geq n - \#\Delta(\cdots) = n - (n - \#\text{“what the weight hits”}) \\ &= \#\text{“what the weight hits”} \end{aligned}$$
- Monomials in the footprint are of different weights which makes the counting simple.

Forgetting about the $X^q - X, Y^q - Y$-part. Case $\mathbb{F}_4[X,Y]/\langle 0\rangle$

$$\begin{array}{cccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & . \\
Y^4 & XY^4 & X^2Y^4 & X^3Y^4 & X^4Y^4 & \cdots \\
Y^3 & XY^3 & X^2Y^3 & X^3Y^3 & X^4Y^3 & \cdots \\
Y^2 & XY^2 & X^2Y^2 & X^3Y^2 & X^4Y^2 & \cdots \\
Y & XY & X^2Y & X^3Y & X^4Y & \cdots \\
1 & X & X^2 & X^3 & X^4 & \cdots
\end{array}$$

$$\begin{array}{cccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & . \\
(0,4) & (1,4) & (2,4) & (3,4) & (4,4) & \cdots \\
(0,3) & (1,3) & (2,3) & (3,3) & (4,3) & \cdots \\
(0,2) & (1,2) & (2,2) & (3,2) & (4,2) & \cdots \\
(0,1) & (1,1) & (2,1) & (3,1) & (4,1) & \cdots \\
(0,0) & (1,0) & (2,0) & (3,0) & (4,0) & \cdots
\end{array}$$

Forgetting about the $X^q - X, Y^q - Y$-part. Case $\mathbb{F}_4[X,Y]/\langle X^3 - Y^2 - Y\rangle$

$$\begin{array}{cccccc} Y & XY & X^2Y & X^3Y & X^4Y & \cdots \\ 1 & X & X^2 & X^3 & X^4 & \cdots \end{array}$$

$$\begin{array}{cccccc} 3 & 5 & 7 & 9 & 11 & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \end{array}$$

Forgetting about the $X^q - X$, $Y^q - Y$

- The set of defining polynomials are $\emptyset$ respectively $\{X^{q+1} - Y^q - Y\}$. “All” defining polynomials have exactly two monomials of the same highest weight.
- Monomials in the big footprint are of different weights implying that so are the monomials in the small footprint.
- $\emptyset$ is a Gröbner basis for $\langle 0 \rangle$ and $\{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for $\langle X^{q+1} - Y^q - Y \rangle$.
- $\mathbb{F}_q[X, Y]$ and $\mathbb{F}_{q^2}[X, Y]/\langle X^{q+1} - Y^q - Y \rangle$ are examples of order domains.

Forgetting about the $X^q - X, Y^q - Y$

- The set of defining polynomials are $\emptyset$ respectively $\{X^{q+1} - Y^q - Y\}$. "All" defining polynomials have exactly two monomials of the same highest weight.
- Monomials in the big footprint are of different weights implying that so are the monomials in the small footprint.
- $\emptyset$ is a Gröbner basis for $\langle 0 \rangle$ and $\{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for $\langle X^{q+1} - Y^q - Y \rangle$.
- $\mathbb{F}_q[X, Y]$ and $\mathbb{F}_{q^2}[X, Y]/\langle X^{q+1} - Y^q - Y \rangle$ are examples of order domains.

Forgetting about the $X^q - X, Y^q - Y$

- The set of defining polynomials are $\emptyset$ respectively $\{X^{q+1} - Y^q - Y\}$. "All" defining polynomials have exactly two monomials of the same highest weight.
- Monomials in the big footprint are of different weights implying that so are the monomials in the small footprint.
- $\emptyset$ is a Gröbner basis for $\langle 0 \rangle$ and $\{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for $\langle X^{q+1} - Y^q - Y \rangle$.
- $\mathbb{F}_q[X, Y]$ and $\mathbb{F}_{q^2}[X, Y]/\langle X^{q+1} - Y^q - Y \rangle$ are examples of order domains.

Forgetting about the $X^q - X, Y^q - Y$

- The set of defining polynomials are $\emptyset$ respectively $\{X^{q+1} - Y^q - Y\}$. "All" defining polynomials have exactly two monomials of the same highest weight.
- Monomials in the big footprint are of different weights implying that so are the monomials in the small footprint.
- $\emptyset$ is a Gröbner basis for $\langle 0 \rangle$ and $\{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for $\langle X^{q+1} - Y^q - Y \rangle$.
- $\mathbb{F}_q[X, Y]$ and $\mathbb{F}_{q^2}[X, Y]/\langle X^{q+1} - Y^q - Y \rangle$ are examples of order domains.

Definition:
$w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^r \backslash \{\vec{0}\}$, $\prec_{\mathbb{N}_0^r}$ a monomial ordering on $\mathbb{N}_0^r$, $\prec_{\mathcal{M}}$ a monomial ordering on $\mathcal{M}(X_1, \ldots, X_m)$. The generalized weighted degree ordering $\prec_w$ is given by: $M_1 \prec_w M_2$ if and only if one of the following two conditions holds:

(1) $w(M_1) \prec_{\mathbb{N}_0^r} w(M_2)$ (2) $w(M_1) = w(M_2)$ and $M_1 \prec_{\mathcal{M}} M_2$.

$\mathrm{wdeg}(F) = \max_{\prec_{\mathbb{N}_0^r}} \{w(M) \mid M \in \mathrm{Sup}(F)\}$

Theorem:
Given $\prec_w$, $I \subset \mathbb{F}[X_1, X_2, \ldots, X_m]$ and corresponding Gröbner basis $\mathcal{G}$. Suppose that the elements of the footprint $\Delta_{\prec_w}(I)$ have mutually distinct weights and that every element of $\mathcal{G}$ has exactly two monomials of highest weight in its support. Then $R = \mathbb{F}[X_1, X_2, \ldots, X_m]/I$ has a weight function defined as follows. Given a nonzero $f \in \mathbb{F}[X_1, X_2, \ldots, X_m]/I$ write $f = F + I$ where $F \in \mathrm{Span}_{\mathbb{F}}\{M \mid M \in \Delta_{\prec_w}(I)$. We have $\rho(f) = \mathrm{wdeg}(F)$ and $\rho(0) = -\infty$.

Any finitely generated order domain can be described as above.

Example:

Let $I = \langle X^3 - Y^2 - Y \rangle$ then
$R = \mathbb{F}_4[X,Y]/I = \mathrm{Span}_{\mathbb{F}_4}\{X^\alpha Y^\beta + I \mid \beta < 2\}$ has a weight function $\rho(X^\alpha Y^\beta + I) = 2\alpha + 3\beta$ for $\alpha < 2$.

Y	XY	X^2Y	X^3Y	X^4Y	$\cdots$
1	X	X^2	X^3	X^4	$\cdots$
3	5	7	9	11	$\cdots$
0	2	4	6	8	$\cdots$
f_3	f_5	f_7	f_9	f_{11}	$\cdots$
f_0	f_2	f_4	f_6	f_8	$\cdots$

Example:

$\mathbb{F}_q[X_1,\ldots,X_m]$ (here $I = \langle 0 \rangle$) has a weight function given by $\rho(X_1^{i_1}\cdots X_m^{i_m}) = (i_1,\ldots,i_m)$. $f_{(i,j)} = X^iY^j$.

Example:
Let $I = \langle X^3 - Y^2 - Y \rangle$ then
$R = \mathbb{F}_4[X, Y]/I = \mathrm{Span}_{\mathbb{F}_4}\{X^\alpha Y^\beta + I \mid \beta < 2\}$ has a weight function $\rho(X^\alpha Y^\beta + I) = 2\alpha + 3\beta$ for $\alpha < 2$.

$$\begin{array}{cccccc} Y & XY & X^2Y & X^3Y & X^4Y & \cdots \\ 1 & X & X^2 & X^3 & X^4 & \cdots \\ \\ 3 & 5 & 7 & 9 & 11 & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \\ \\ f_3 & f_5 & f_7 & f_9 & f_{11} & \cdots \\ f_0 & f_2 & f_4 & f_6 & f_8 & \cdots \end{array}$$

Example:
$\mathbb{F}_q[X_1, \ldots, X_m]$ (here $I = \langle 0 \rangle$) has a weight function given by $\rho(X_1^{i_1} \cdots X_m^{i_m}) = (i_1, \ldots, i_m)$. $f_{(i,j)} = X^i Y^j$.

Definition:

R be an $\mathbb{F}_q$-algebra, Γ a subsemigroup of $\mathbb{N}_0^r$, $\prec$ be a monomial ordering on $\mathbb{N}_0^r$. A surjective map $\rho : R \to \Gamma_{-\infty} := \Gamma \cup \{-\infty\}$ that satisfies the following conditions is called a weight function

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

Example:

$\mathcal{X}$ a curve and P a rational place then $\mathcal{L}_{m=0}^{\infty} mP$ has a weight function $\rho(f) = -v_P(f)$.

Definition:
R be an $\mathbb{F}_q$-algebra, Γ a subsemigroup of $\mathbb{N}_0^r$, $\prec$ be a monomial ordering on $\mathbb{N}_0^r$. A surjective map $\rho : R \to \Gamma_{-\infty} := \Gamma \cup \{-\infty\}$ that satisfies the following conditions is called a weight function

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

Example:
$\mathcal{X}$ a curve and P a rational place then $\mathcal{L}_{m=0}^{\infty} mP$ has a weight function $\rho(f) = -v_P(f)$.

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

Example:
$R = \mathbb{F}_q[X_1, \ldots, X_m]/I$, $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and

$$\varphi : \begin{cases} R & \to & \mathbb{F}_q^n \\ F + I & \mapsto & (F(P_1) \ldots, F(P_n)) \end{cases}$$

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

Example:
$R = \mathbb{F}_q[X_1, \ldots, X_m]/I$, $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and

$$\varphi : \begin{cases} R & \to & \mathbb{F}_q^n \\ F + I & \mapsto & (F(P_1) \ldots, F(P_n)) \end{cases}$$

Putting $X^q - X$, $Y^q - Y$ back in place

Definition: Write $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$
Let $\alpha(1) := \vec{0}$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.

Example: $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$, $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and $\varphi(F + I) = (F(P_1) \ldots, F(P_n))$. $\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q))$ where $I_q = I \cup \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X, Y]/I$

$$\begin{array}{cccccc} 3 & 5 & 7 & 9 & 11 & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \end{array}$$

$$\alpha(1) = 0, \alpha(2) = 2, \alpha(3) = 3, \ldots, \alpha(7) = 7, \alpha(8) = 9$$

Putting $X^q - X, Y^q - Y$ back in place

Definition: Write $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$
Let $\alpha(1) := \vec{0}$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.

Example: $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$, $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and $\varphi(F + I) = (F(P_1) \ldots, F(P_n))$. $\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q))$ where $I_q = I \cup \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X, Y]/I$

$$\begin{array}{cccccc} 3 & 5 & 7 & 9 & 11 & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \end{array}$$

$$\alpha(1) = 0, \alpha(2) = 2, \alpha(3) = 3, \ldots, \alpha(7) = 7, \alpha(8) = 9$$

Putting $X^q - X, Y^q - Y$ back in place

Definition: Write $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$
Let $\alpha(1) := \vec{0}$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$ for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.

Example: $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$, $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ and $\varphi(F + I) = (F(P_1) \ldots, F(P_n))$. $\Delta(R, \rho, \varphi) = w(\Delta_{\prec_w}(I_q))$ where $I_q = I \cup \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X, Y]/I$

$$\begin{matrix} 3 & 5 & 7 & 9 & 11 & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \end{matrix}$$

$$\alpha(1) = 0, \alpha(2) = 2, \alpha(3) = 3, \ldots, \alpha(7) = 7, \alpha(8) = 9$$

Definition:
For $\eta \in \Delta(R,\rho,\varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define $M(\eta) := \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists \beta \in \Delta(R,\rho,\varphi) \text{ with } \eta + \beta = \gamma\}$. Let $\sigma(\eta) := \# M(\eta)$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X,Y]/I$

$\Delta(R,\rho,\varphi)$				$\sigma(\eta)$			
3	5	7	9	5	3	2	1
0	2	4	6	8	6	4	2

Definition:

$$\begin{aligned} E(\lambda) &:= \varphi(R_\lambda) \\ \tilde{E}(\delta) &:= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R,\rho,\varphi) \text{ and } \sigma(\alpha(i)) \geq \delta\} \end{aligned}$$

Theorem:

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

Definition:
For $\eta \in \Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define $M(\eta) := \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \eta + \beta = \gamma\}$. Let $\sigma(\eta) := \# M(\eta)$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X, Y]/I$

$\Delta(R, \rho, \varphi)$				$\sigma(\eta)$			
3	5	7	9	5	3	2	1
0	2	4	6	8	6	4	2

Definition:

$$\begin{aligned} E(\lambda) &:= \varphi(R_\lambda) \\ \tilde{E}(\delta) &:= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \text{ and } \sigma(\alpha(i)) \geq \delta\} \end{aligned}$$

Theorem:

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

Definition:
For $\eta \in \Delta(R,\rho,\varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define $M(\eta) := \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists \beta \in \Delta(R,\rho,\varphi) \text{ with } \eta + \beta = \gamma\}$. Let $\sigma(\eta) := \# M(\eta)$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X,Y]/I$

$\Delta(R,\rho,\varphi)$				$\sigma(\eta)$			
3	5	7	9	5	3	2	1
0	2	4	6	8	6	4	2

Definition:

$$\begin{aligned} E(\lambda) &:= \varphi(R_\lambda) \\ \tilde{E}(\delta) &:= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R,\rho,\varphi) \text{ and } \sigma(\alpha(i)) \geq \delta\} \end{aligned}$$

Theorem:

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

Definition:
For $\eta \in \Delta(R,\rho,\varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define $M(\eta) := \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists \beta \in \Delta(R,\rho,\varphi) \text{ with } \eta + \beta = \gamma\}$. Let $\sigma(\eta) := \# M(\eta)$.

Example: $I = \langle X^3 - Y^2 - Y \rangle$ and $R = \mathbb{F}_4[X,Y]/I$

$\Delta(R,\rho,\varphi)$				$\sigma(\eta)$			
3	5	7	9	5	3	2	1
0	2	4	6	8	6	4	2

Definition:

$$\begin{aligned} E(\lambda) &:= \varphi(R_\lambda) \\ \tilde{E}(\delta) &:= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R,\rho,\varphi) \text{ and } \sigma(\alpha(i)) \geq \delta\} \end{aligned}$$

Theorem:

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

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

$$w: \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}$$

$$\sigma: \begin{array}{ccccccccc} 19 & 16 & 13 & 10 & 7 & 4 & 3 & 2 & 1 \\ 23 & 20 & 17 & 14 & 11 & 8 & 6 & 4 & 2 \\ 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \end{array}$$

$$\mu: \begin{array}{ccccccccc} 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\ 2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\ 1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}$$

$\mu(6) = 3$ as $6 = 0+6 = 3+3 = 6+0$

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

$$w: \quad \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}$$

$$\sigma: \quad \begin{array}{ccccccccc} 19 & 16 & 13 & 10 & 7 & 4 & 3 & 2 & 1 \\ 23 & 20 & 17 & 14 & 11 & 8 & 6 & 4 & 2 \\ 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \end{array}$$

$$\mu: \quad \begin{array}{ccccccccc} 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\ 2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\ 1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}$$

$$\mu(6) = 3 \ \text{ as } \ 6 = 0 + 6 = 3 + 3 = 6 + 0$$

$$
w: \quad \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}
$$

$$
\mu: \quad \begin{array}{ccccccccc} 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\ 2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\ 1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}
$$

Codes defined by their parity checks:

Lowest μ-value that is NOT used "gives" Hamming weight.

$C(7)$ is $[27, 22, 3]$ and $C(8)$ is $[27, 21, 4]$

but

$\tilde{C}(4)$ is $[27, 22, 4]$

	8	11	14	17	20	23	26	29	32
w :	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
μ :	2	4	6	8	11	14	17	20	23
	1	2	3	4	7	10	13	16	19

Codes defined by their parity checks:

Lowest μ-value that is NOT used "gives" Hamming weight.

$C(7)$ is $[27, 22, 3]$ and $C(8)$ is $[27, 21, 4]$

but

$\tilde{C}(4)$ is $[27, 22, 4]$

$$w: \quad \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}$$

$$\mu: \quad \begin{array}{ccccccccc} 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\ 2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\ 1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}$$

Codes defined by their parity checks:

Lowest μ-value that is NOT used "gives" Hamming weight.

$C(7)$ is $[27, 22, 3]$ and $C(8)$ is $[27, 21, 4]$

but

$\tilde{C}(4)$ is $[27, 22, 4]$

$$
w: \quad \begin{array}{ccccccccc}
8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\
4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\
0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24
\end{array}
$$

$$
\mu: \quad \begin{array}{ccccccccc}
3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\
2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\
1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19
\end{array}
$$

Codes defined by their parity checks:

Lowest μ-value that is NOT used “gives” Hamming weight.

$C(7)$ is $[27, 22, 3]$ and $C(8)$ is $[27, 21, 4]$

but

$\tilde{C}(4)$ is $[27, 22, 4]$

Reed-Solomon codes revisited

$\mathbb{F}_q = \{P_1, \ldots, P_q\}$
Consider $\vec{0} \neq \vec{c} \in (\{(F(P_1), \ldots, F(P_q)) \mid \deg(F) \leq s\})^{\perp}$.
$\exists l$ with $\vec{c} \cdot \varphi(X^l) \neq 0$ but $\vec{c} \cdot \varphi(X^i) = 0$, $\forall i < l$.

$$\#\text{what hits } l \quad = \#\{i \mid \exists j \ \text{ with } \ i + j = l\} = l + 1$$

To see $w_H(\vec{c}) \geq l + 1$ consider all linear combinations of monomials that "hits" X^l:

$$\Sigma_{i=0}^{l} a_i X^i = \Sigma_{i=0}^{h} a_i X^i, \ \ a_h \neq 0$$

$$\begin{aligned}
\vec{c} \cdot \varphi\left((\Sigma_{i=0}^{h} a_i X^i) X^{l-h}\right) &= \vec{c} \cdot \varphi(a_h X^h) + \vec{c} \cdot \varphi\left(\Sigma_{i=0}^{h-1} a_i X^{l-h+i}\right) \\
&= \vec{c} \cdot \varphi(a_h X^h) + 0 \neq 0
\end{aligned}$$

Hence,

$$\left(\vec{c} * \varphi\left(\Sigma_{i=0}^{h} a_i X^i\right)\right) \cdot \varphi(X^{l-h}) \neq 0$$
$$\Downarrow$$
$$\vec{c} * \varphi\left(\Sigma_{i=0}^{h} a_i X^i\right) \neq \vec{0}$$

Space of possible $\left(\Sigma_{i=0}^{h} a_i X^i\right)$'s is of dimension $l + 1$

Definition:
For $\lambda \in \Gamma$ define $N(\lambda) := \{(\alpha, \beta) \in \Gamma^2 \mid \alpha + \beta = \lambda\}$. Let $\mu(\lambda) := \# N(\lambda)$ if $N(\lambda)$ is a finite set and $\mu(\lambda) = \infty$ if not.

Definition:

$$\begin{aligned} C(\lambda) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\} \\ \tilde{C}(\delta) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_{\alpha(i)}) = 0 \\ &\qquad \text{for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\} \end{aligned}$$

Theorem:

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

Definition:
For $\lambda \in \Gamma$ define $N(\lambda) := \{(\alpha, \beta) \in \Gamma^2 \mid \alpha + \beta = \lambda\}$. Let $\mu(\lambda) := \# N(\lambda)$ if $N(\lambda)$ is a finite set and $\mu(\lambda) = \infty$ if not.

Definition:

$$\begin{aligned} C(\lambda) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\} \\ \tilde{C}(\delta) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_{\alpha(i)}) = 0 \\ &\qquad \text{for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\} \end{aligned}$$

Theorem:

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

Definition:
For $\lambda \in \Gamma$ define $N(\lambda) := \{(\alpha, \beta) \in \Gamma^2 \mid \alpha + \beta = \lambda\}$. Let $\mu(\lambda) := \# N(\lambda)$ if $N(\lambda)$ is a finite set and $\mu(\lambda) = \infty$ if not.

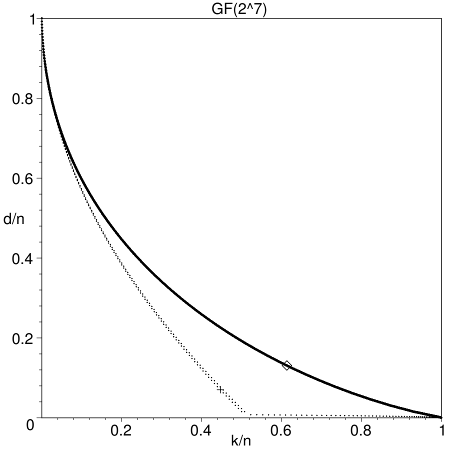
Definition:

$$\begin{aligned} C(\lambda) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\} \\ \tilde{C}(\delta) &:= \{\vec{c} \in \mathbb{F}_q^n \mid \vec{c} \cdot \varphi(f_{\alpha(i)}) = 0 \\ &\qquad \text{for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\} \end{aligned}$$

Theorem:

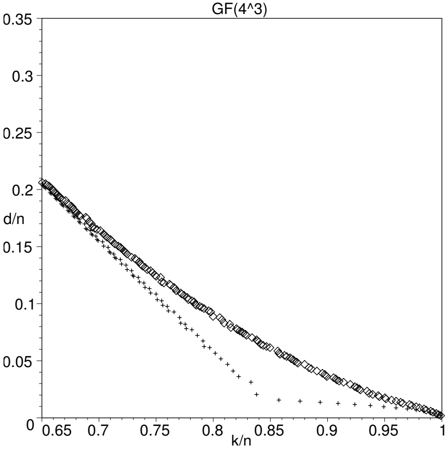
$$\begin{aligned} d(C(\lambda)) &\geq \min\{\mu(\eta) \mid \lambda \prec \eta, \eta \in \Delta(R, \rho, \varphi)\} \geq \min\{\mu(\eta) \mid \lambda \prec \eta\} \\ d(\tilde{C}(\delta)) &\geq \delta. \end{aligned}$$

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



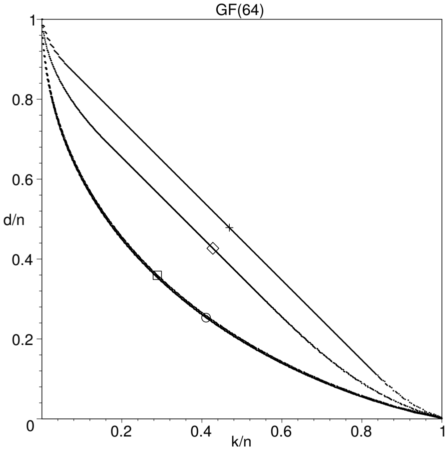
Alphabet=$\mathbb{F}_{q^r} = \mathbb{F}_{2^7}$, $n = 2^{13}$ Improved versus non-improved.

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



Alphabet=$\mathbb{F}_{q^r} = \mathbb{F}_{4^3}$, $n = 4^5$ Improved versus non-improved.

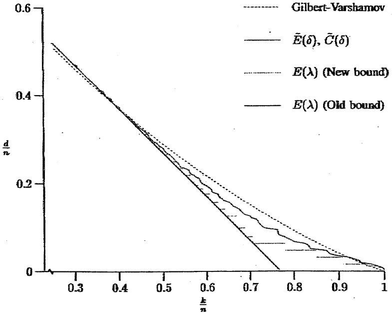
$$I = \langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y \rangle \subseteq \mathbb{F}_{q^r}[X, Y]$$



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

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

$w(X) = 16, \quad w(Y) = 20, \quad w(Z) = 25$

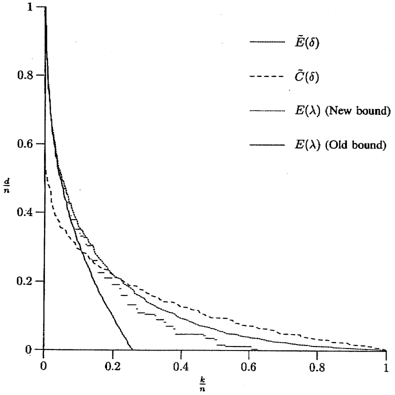


alphabet $= \mathbb{F}_{16}$, $n = 256$

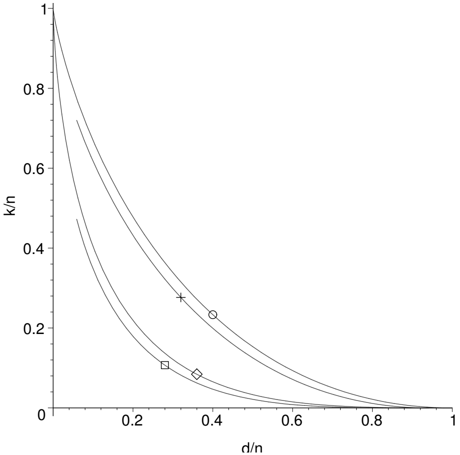
$$I = \langle x^5 - Y^4 - Y,\; Y^5 - Z^4 - Z,\; Z^5 - U^4 - U^2 \rangle \subseteq \mathbb{F}_{16}[X, Y, Z, U]$$

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

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



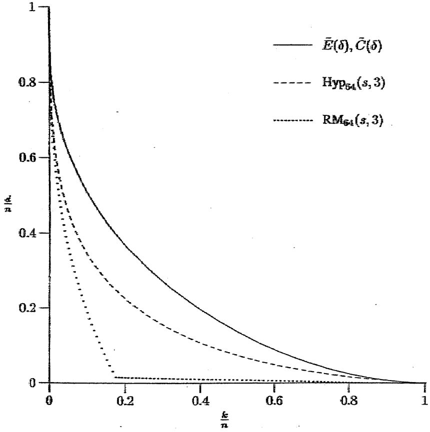
Tensor product of m Hermitian order domains involves weights in $\mathbb{N}_0^m$.



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 $n = 68719476736$.

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

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



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

Garcia-Stichtenoth towers

Code constructions related to some of the asymptotic good towers are one-point geometric Goppa codes.

That is, order domain codes.

Invitation 1: Is it possible to find defining equations for corresponding I and corresponding I_q?

Garcia-Stichtenoth towers

Code constructions related to some of the asymptotic good towers are one-point geometric Goppa codes.

That is, order domain codes.

Invitation 1: Is it possible to find defining equations for corresponding I and corresponding I_q?

Garcia-Stichtenoth towers

Code constructions related to some of the asymptotic good towers are one-point geometric Goppa codes.

That is, order domain codes.

Invitation 1: Is it possible to find defining equations for corresponding I and corresponding I_q?

Garcia-Stichtenoth towers

Code constructions related to some of the asymptotic good towers are one-point geometric Goppa codes.

That is, order domain codes.

Invitation 1: Is it possible to find defining equations for corresponding I and corresponding I_q?

Where did it all come from?

Feng-Rao theory:

- Provides simplified descriptions of a large class of algebraically defined codes
- Improved estimation of minimum distance
- Improved code constructions
- Improved decoding algorithms
- Natural tool is Gröbner basis theory

Order domains designed by Høholdt, van Lint and Pellikaan to support much of the Feng-Rao theory.

Invitation 2: Only a few have looked at codes from surfaces...

Where did it all come from?

Feng-Rao theory:

- Provides simplified descriptions of a large class of algebraically defined codes
- Improved estimation of minimum distance
- Improved code constructions
- Improved decoding algorithms
- Natural tool is Gröbner basis theory

Order domains designed by Høholdt, van Lint and Pellikaan to support much of the Feng-Rao theory.

Invitation 2: Only a few have looked at codes from surfaces...

Where did it all come from?

Feng-Rao theory:

- Provides simplified descriptions of a large class of algebraically defined codes
- Improved estimation of minimum distance
- Improved code constructions
- Improved decoding algorithms
- Natural tool is Gröbner basis theory

Order domains designed by Høholdt, van Lint and Pellikaan to support much of the Feng-Rao theory.

Invitation 2: Only a few have looked at codes from surfaces...

- H. E. Andersen, O. Geil, The Missing Evaluation Codes from Order Domain Theory, (2004), submitted.
- G.-L. Feng and T.R.N. Rao, Improved Geometric Goppa Codes, Part I:Basic theory, *IEEE Trans. Inf. Theory*, **41**, (1995), 1678-1693.
- O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields and their Applications*, **8**, (2002), 369-396.
- T. Høholdt, J. van Lint and R. Pellikaan, Algebraic Geometry Codes, Chapter 10 in “Handbook of Coding Theory,” (V.S. Pless and W.C. Huffman, Eds.), vol. 1, Elsevier, Amsterdam, 1998, 871-961.
- R. Pellikaan, On the existence of order functions, *Journal of Statistical Planning and Inference,* **94**, no. 2 (2001), 287-301.