Generalizations of the Reed-Solomon Codes Via Gröbner Basis Theory

Olav Geil

Department of Mathematical Sciences
Aalborg University
Denmark

Tokyo Institute of Technology, August 8, 2006

Thanks to

Professor Tomohiko Uyematsu
and
Professor Ryutaroh Matsumoto

for invitation
and for great hospitality

Outline

Model

$$
\begin{array}{ccccccccc}
\vec{m} & & \vec{c} & & \vec{r} = \vec{c} + \vec{e} & & \vec{m}' \\
\rightarrow & \text{Encoder} & \rightarrow & \text{Channel} & \rightarrow & \text{Decoder} & \rightarrow \\
 & & & \uparrow & & & \\
 & & & \vec{e} & & &
\end{array}
$$

$\vec{m} = (m_1, \dots, m_k) \in \mathbb{F}_q^k$, $k < n$, $\vec{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n$
$\vec{e} = (e_1, \dots, e_n) \in \mathbb{F}_q^n$, $\vec{m}' \in \mathbb{F}_q^k$

$P_i(e_i = 0) = p$ is large, $P_i(e_i = \alpha) = (1 - P)/(1 - q)$ for $\alpha \neq 0$ and P_i, P_j are independent

Linear code

A (linear) code C is a subspace $C \subseteq \mathbb{F}_q^n$
$k = \dim(C)$, $C \simeq \mathbb{F}_q^k$.

Encoding:
Choose basis $\{\vec{g}_1, \ldots, \vec{g}_k\}$ for C. The generator matrix is

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

Encode by $\vec{c} = \vec{m}G$.

Minimum distance

$$w_H((w_1, \ldots, w_n)) = \#\{i \mid w_i \neq 0\}$$

$$\mathrm{dist}_H(\vec{w}_1, \vec{w}_2) = w_H(\vec{w}_1 - \vec{w}_2)$$

$$d = \min\{\mathrm{dist}_H(\vec{c}_1, \vec{c}_2) \mid \vec{c}_1, \vec{c}_2 \in C, \vec{c}_1 \neq \vec{c}_2\}$$

Within the distance $\left\lfloor \frac{d-1}{2} \right\rfloor$ of a word $\vec{w}$ there can be at most one codeword.

If at most $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors occurs we can correct them by choosing the nearest code word to the received word.

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

The three parameters

The length n, the dimension k and the minimum distance d.
$[n, k, d]$

If $\frac{k}{n}$ is high then fast transmission.
If $\frac{d}{n}$ is high then good protection against noise.

The challenge is to get $\frac{k}{n}$ as well as $\frac{d}{n}$ high simultaneously.

Reed-Solomon code - generator matrix description

$\mathrm{RS}_q(k)$ over $\mathbb{F}_q = \{P_1, P_2, \ldots, P_q\}$.

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

$\mathrm{RS}_q(k)$ consists of the code words $\vec{c} = \vec{i}G$, where $\vec{i} = (i_0, \ldots, i_{k-1}) \in \mathbb{F}_q^k$.

$$\mathrm{RS}_q(k) = \{(f(P_1), f(P_2), \ldots, f(P_q)) \mid \deg(f) < k\}.$$

Parameters of Reed-Solomon code

Length: $n = q$.

Key observation 1:
$d = n - (k-1) = n - k + 1$ as a polynomial of degree at most $k-1$ can have at most $k-1$ zeros.

Key observation 2:

$$(1, 1, \dots, 1), (P_1, P_2, \dots, P_n), \dots, (P_1^{n-1}, P_2^{n-1}, \dots, P_n^{n-1})$$

are linearly independent. Hence, for $k < q$ we have $\dim(\mathrm{RS}_q(k)) = k$.

$\mathrm{RS}_q(k)$ is $[n = q, k, d = n - k + 1]$.

Some properties of the Reed-Solomon code

Advantages:

- Large minimum distance
- A lot of structure
- More efficient decoding algorithms including list decoding
- Useful as outer code in concatenated codes

Disadvantage:

- ... but very short

The goal

Want to construct long codes with a lot of structure and with high minimum distance.

Strategy:
Reed-Solomon like generator matrices that support generalizations of Key observation 1 and Key observation 2.

Mathematical language (theory)

Traditional: Algebraic geometry or function field theory.
In particular the Riemann-Roch Theorem.

More recent: Gröbner basis theory (much simpler)

Monomials and polynomials

One variable:

$$\mathcal{M}(X) = \{1, X, X^2, X^3, \ldots\} = \{X^i \mid i \in \mathbb{N}_0\}$$

Two variables:

$$\mathcal{M}(X, Y) = \{X^i Y^j \mid i, j \in \mathbb{N}_0\}$$

Example: $X^3 Y^4$

More variables:

$$\mathcal{M}(X_1, X_2, \ldots, X_m) = \{X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m} \mid i_1, i_2, \ldots, i_m \in \mathbb{N}_0\}$$

Polynomial is linear combination of monomials.

Example: $F(X, Y) = X^3 Y + 2XY + 1$

Monomial orderings

One variable:

$$1 < X < X^2 < X^3 < \cdots$$

More variables:
$\prec$ is a monomial ordering on $\mathcal{M}(X_1, X_2, \ldots, X_m)$ if the following hold

1. If $K \prec M$ and $M \prec N$ then also $K \prec N$.
2. If $K \prec M$ then also $KN \prec MN$.
3. Any set of monomials in $\mathcal{M}(X_1, X_2, \ldots, X_m)$ has a (unique) smallest element.

Monomial orderings - continued

The lexicographic ordering:
$X_1^{i_1} \cdots X_m^{i_m} \prec_{lex} X_1^{j_1} \cdots X_m^{j_m}$ if leftmost nonzero entry of $(j_1 - i_1, \ldots, j_m - i_m)$ is positive.

Example:
$X_1 X_2^4 \prec_{lex} X_1^2 X_2$ as $(2,1) - (1,4) = (1,-3)$ has leftmost nonzero entry positive.
If we choose $X_1 = X$ and $X_2 = Y$ then $XY^4 \prec_{lex} X^2Y$.
If we choose $X_1 = Y$ and $X_2 = X$ then $X^2Y \prec_{lex} XY^4$.

Monomial orderings - continued

The graded lexicographic ordering:
$X_1^{i_1} \cdots X_m^{i_m} \prec_{deg} X_1^{j_1} \cdots X_m^{j_m}$ if either (1) or (2) below holds:

(1) $i_1 + \cdots + i_m < j_1 + \cdots + j_m$

(2) $i_1 + \cdots + i_m = j_1 + \cdots + j_m$
and leftmost nonzero entry of $(j_1 - i_1, \ldots, j_m - i_m)$
is positive

Example: $X^2YZ^2 \prec_{deg} X^4YZ$ and $X^3Y^2Z \prec_{deg} X^4YZ$

Monomomial orderings - continued

The weighted graded lexicographic ordering:
Given $w_1, \ldots, w_m \in \mathbb{R}_+$ then $X_1^{i_1} \cdots X_m^{i_m} \prec_w X_1^{j_1} \cdots X_m^{j_m}$ if either (1) or (2) below holds:

(1) $w_1 i_1 + \cdots + w_m i_m < w_1 j_1 + \cdots + w_m j_m$

(2) $w_1 i_1 + \cdots w_m i_m = w_1 j_1 + \cdots + w_m j_m$
and leftmost nonzero entry of $(j_1 - i_1, \ldots, j_m - i_m)$ is positive

Example: $w_1 = w(X) = 2$ and $w_2 = w(Y) = 3$.
$X^4 Y \prec_w Y^4$ as $w(X^4 Y) = 11 < 12 = w(Y^4)$
$X_1 = Y$ and $X_2 = X$ gives $X^3 \prec_w Y^2$ as $w(X^3) = w(Y^2) = 6$ and $(2,0) - (0,3) = (2,-3)$.

Zeros of a polynomial

One variable:
$2 \in \mathbb{Z}_5 = \mathbb{F}_5$ is a zero of $F(X) = X^2 + X + 4$ as $2^2 + 2 + 4 \equiv 0 \mod 5$

More variables:
$(2, 3) \in \mathbb{Z}_5 \times \mathbb{Z}_5$ is a zero of $F(X, Y) = XY + X + 3Y + 3$ as $2 \cdot 3 + 2 + 3 \cdot 3 + 3 \equiv 0 \mod 5$.

Main question:
How do we estimate how many zeros a given polynomial in more variables can have?

Zeros of a polynomial - continued

Example:
$X^3 - Y^2 - Y$ has infinitely many zeros in $\mathbb{R} \times \mathbb{R}$. For every choice of b let $\sqrt[3]{b^2 + b}$ then (a, b) is a zero.

Example:
$X^3 - Y^2 - Y$ and $Y^4 - Y$ has only finitely many zeros in common in $\mathbb{R} \times \mathbb{R}$.

The footprint bound

One variable case:
$F(X) = X^3 + X + 7$ has at most 3 zeros as $\deg(F) = 3$. Note that $\mathrm{lm}(F) = X^3$ and that also number of $*$'s is 3.

$$\begin{array}{ccccccc} * & * & * & \square & \cdot & \cdot & \cdot \\ 1 & X & X^2 & X^3 & X^4 & X^5 & X^6 \end{array}$$

To deal with more variables and more polynomials we will draw pictures as above.

The footprint bound - continued

Example:
We look for solutions (a, b) to $X^2Y - XY$ in $\mathbb{F}_3 \times \mathbb{F}_3$. If $(a, b) \in \mathbb{F}_3 \times \mathbb{F}_3$ then solution to $X^3 - X$ and $Y^3 - Y$ as well.
We have the zeros

$$(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0).$$

Consider the lexicographic ordering. We have the leading monomials $\mathrm{lm}(X^2Y - XY) = X^2Y$, $\mathrm{lm}(X^3 - X) = X^3$ and $\mathrm{lm}(Y^3 - Y) = Y^3$ giving us the picture

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

Certainly, $\#$ zeros equals $\#$ of $*$'s.

The footprint bound - continued

Example:
By inspection $X^3 - Y^2 - Y$ has 8 zeros in $\mathbb{F}_4 \times \mathbb{F}_4$. Consider the weighted graded lexicographic ordering $\prec_w$ with $w(X) = 2$ and $w(Y) = 3$ and $X_1 = X$ and $X_2 = Y$. We have the leading monomials $\mathrm{lm}(X^3 - Y^2 - Y) = X^3$, $\mathrm{lm}(X^4 - X) = X^4$ and $\mathrm{lm}(Y^4 - Y) = Y^4$ giving us the picture

$$\begin{array}{ccccccc}
Y^5 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^4 & \square & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^3 & * & * & * & \cdot & \cdot & \cdot \\
Y^2 & * & * & * & \cdot & \cdot & \cdot \\
Y & * & * & * & \cdot & \cdot & \cdot \\
1 & * & * & * & \square & \square & \cdot \\
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}$$

...Ups...now more $*$'s than zeros. What is wrong?

The footprint bound - continued

If (a, b) is a common zero of $X^3 - Y^2 - Y, X^4 - X, Y^4 - Y$ then certainly also a zero of

$$X(X^3 - Y^2 - Y) + (X^4 - X) = XY^2 + XY + X.$$

This polynomial has leading monomial XY^2.

$$\begin{array}{ccccccc}
Y^5 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^4 & \Box & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^3 & * & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^2 & * & \Box & \cdot & \cdot & \cdot & \cdot \\
Y & * & * & * & \cdot & \cdot & \cdot \\
1 & * & * & * & \Box & \Box & \cdot \\
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}$$

Now, $\#$ zeros equals $\# *$'s.

Conclusion: we need to consider not only polynomials but also their consequences.

The footprint bound - continued

Definition:
Let $F_1, F_2, \ldots, F_s$ be polynomials. The set

$$\{K_1F_1 + K_2F_2 + \cdots + K_sF_s \mid K_1, K_2, \ldots, K_s \text{ are polynomials } \}$$

is called the ideal generated by $F_1, F_2, \ldots, F_s$. It is denoted $\langle F_1, F_2, \ldots, F_s \rangle$.

Example:
$XY^2+XY+X = X(X^3-Y^2-Y)+(X^4-X) \in \langle X^3-Y^2-Y, X^4-X, Y^4-Y \rangle = \langle X^3-Y^2-Y, X^4-X, Y^4-Y, XY^2+XY+X \rangle$.

Conclusion: The concept of an ideal plays a central role for estimating zeros.

The footprint bound - continued

Definition:
Given an ideal $I = \langle F_1, F_2, \ldots, F_s \rangle$ and a monomial ordering the footprint of I is:

$$\begin{aligned}\Delta_{\prec}(I) \quad = \quad \{M \text{ is a monomial } &\mid M \text{ can not be found as} \\ &\text{the leading monomial of any polynomial in } I\}\end{aligned}$$

Buchberger's algorithm add more polynomials (consequences) to the list $\{F_1, \ldots, F_s\}$ so that the footprint can be easily read of. Such an enlarged set is called a Gröbner basis.

The footprint bound - continued

Example:

$I = \langle X^3 - Y^2 - Y, X^4 - X, Y^4 - Y \rangle$ has as leading monomials

$\mathrm{lm}(X^iY^j(X^3 - Y^2 - Y)) = X^{3+i}Y^j$,
$\mathrm{lm}(X^iY^j(X^4 - X)) = X^{4+i}$,
$\mathrm{lm}(X^iY^j(Y^4 - Y)) = X^iY^{4+j}$ and
$\mathrm{lm}(X^iY^j(XY^2 + XY + X)) = X^{i+1}Y^{2+j}$

where (i, j) runs through all possibilities.

$$
\begin{array}{ccccccc}
Y^5 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^4 & \square & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^3 & * & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^2 & * & \square & \cdot & \cdot & \cdot & \cdot \\
Y & * & * & * & \cdot & \cdot & \cdot \\
1 & * & * & * & \square & \square & \cdot \\
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}
$$

The footprint bound - continued

Example:
As seen $X^3 - Y^2 - Y$ has 8 zeros in $\mathbb{F}_4 \times \mathbb{F}_4$.
Consider weighted graded lexicographic ordering with $w(X) = 2$, $w(Y) = 3$ and $X_1 = Y$, $X_2 = X$. The leading monomials with respect to $\prec_w$ are:
$\text{lm}(X^4 - X) = X^4$, $\text{lm}(Y^4 - Y) = Y^4$ and $\text{lm}(X^3 - Y^2 - Y) = Y^2$.

$$
\begin{array}{ccccccc}
Y^5 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^3 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y^2 & \square & \cdot & \cdot & \cdot & \cdot & \cdot \\
Y & * & * & * & * & \cdot & \cdot \\
1 & * & * & * & * & \square & \cdot \\
 & 1 & X & X^2 & X^3 & X^4 & X^5
\end{array}
$$

$\#$ zeros equals $\#*$'s.

Key observation 1 generalized

Theorem (The footprint bound):
The number of common zeros of $F_1, F_2, \ldots, F_s$ is at most equal to $\#\Delta_{\prec}(\langle F_1, F_2, \ldots, F_s \rangle)$. (If $X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m$ are among $F_1, F_2, \ldots, F_s$ then equality holds.)

Hence, if $\{P_1, \ldots, P_n\}$ is the common zeros of $F_1, \ldots, F_s$ and G is a polynomial then $w_H\left((G(P_1), \ldots, G(P_n)\right)$ is at least equal to $n - \#\Delta_{\prec}(\langle G, F_1, \ldots, F_s \rangle)$.

Key observation 2 generalized

Theorem:
Assume $X_1^q - X_1, X_2^q - X_2, \ldots, X_m^q - X_m$ are among $F_1, F_2, \ldots, F_s$. Let $P_1, P_2, \ldots, P_n$ be the common zeros of $F_1, F_2, \ldots, F_s$. The set

$$\{(M(P_1), M(P_2), \ldots, M(P_n)) \mid M \in \Delta_{\prec}(\langle F_1, F_2, \ldots, F_s \rangle)\}$$

constitutes a basis for $\mathbb{F}_q^n$ as a vectorspace over $\mathbb{F}_q$.

Key observation 2 - continued

Example:

The common solutions of $X^2Y - XY$, $X^3 - X$ and $Y^3 - Y$ are

$$P_1 = (0,0), P_2 = (0,1), P_3 = (0,2), P_4 = (1,0),$$

$$P_5 = (1,1), P_6 = (1,2), P_7 = (2,0).$$

And the footprint (corresponding to the lexicographic ordering) is

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

Hence,

$$\{(M(P_1), M(P_2), \ldots, M(P_7)) \mid M \in \{1, X, X^2, Y, XY, Y^2, XY^2\}\}$$

is a basis for $\mathbb{F}_3^7$.

Reed-Solomon codes revisited

$P_1, P_2, \ldots, P_{16}$ the zeros of $X^{16} - X$ (the elements of $\mathbb{F}_{16}$).
Footprint: $\Delta_<(\langle X^{16} - X\rangle) = \{1, X, X^2, \ldots, X^{15}\}$. Hence,

$$\{M(P_1), M(P_2), \ldots, M(P_{16})) \mid M \in \Delta_<(\langle X^{16} - X\rangle)\}$$

constitutes a basis for $\mathbb{F}_{16}^{16}$.

$\Delta_<(\langle X^{16} - X\rangle)$						$\#\Delta_<(\langle X^i, X^{16}\rangle)$					
1	X	X^2	$\cdots$	X^{14}	X^{15}	0	1	2	$\cdots$	14	15

For F with $\mathrm{lm}(F) = X^i$ we have

$$\Delta_<(\langle F, X^{16} - X\rangle) \subseteq \Delta_<(\langle X^i, X^{16}\rangle).$$

By Key observation 1,

$$w_H((F(P_1), F(P_2), \ldots, F(P_1))) = 16 - \#\Delta_<(\langle F, X^{16} - X\rangle) \geq 16 - i.$$

We have shown $\dim(\mathrm{RS}_{16}(k)) = k$ for $k < 16$ and
$d(\mathrm{RS}_{16}(k)) \geq 16 - (k-1) = 16 - k + 1$.

Generalized Reed-Muller codes and hyperbolic codes

Let $P_1, P_2, \ldots, P_{25}$ be the common zeros of $X^5 - X, Y^5 - Y$.
We consider words of the form $(F(P_1), F(P_2), \ldots, F(P_{25}))$.
Let $\prec$ be any monomial ordering.

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

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

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

$$\#\Delta_\prec(\langle X^5 - X, Y^5 - Y, G(X, Y) \rangle) \le \#\Delta_\prec(\langle X^5, Y^5, XY \rangle \le 9$$

$$w_H(G(P_1), G(P_2), \ldots, G(P_{25})) \ge 25 - 9 = 16$$

Generalized Reed-Muller codes

New notation: $\varphi(G) = (G(P_1), G(P_2), \ldots, G(P_{25}))$.
$\mathrm{RM}_5(4,2) = \mathrm{Span}_{\mathbb{F}_5}\{\varphi(X^iY^j) \mid i+j \leq 4\}$

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

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

Worst case 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	$*$

$P_1, P_2, \ldots, P_{64}$ the common zeros of $X^8 - X, Y^8 - Y$

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 $[64, 37, 14 = 64 - 50]$

Generalized Reed-Muller codes and Hyperbolic codes

$\{P_1, \ldots, P_{q^m}\}$ the common zeros of $X_1^q - X_1, \ldots, X_m^q - X_m$.

If $G(X_1, \ldots, X_m)$ has leading monomial $X_1^{i_1} \cdots X_m^{i_m}$ then

$$\begin{aligned} w_H\left(G(P_1), \ldots, G(P_{q^m})\right) &= q^m - \#\Delta_\prec(\langle G, X_1^q - X_1, \ldots, X_m^q - X_m\rangle) \\ &\geq q^m - \#\Big(\Delta_\prec(\langle X_1^{i_1} \cdots X^{i_m}\rangle) \cap \\ &\qquad \Delta_{\prec_\prec}(\langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle)\Big) \end{aligned}$$

For $X_1^{i_1} \cdots X_m^{i_m} \in \Delta_\prec(\langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle)$ define

$$\begin{aligned} D(X_1^{i_1} \cdots X_m^{i_m}) &= \#\Delta_\prec(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q\rangle) \\ &= \#\Big(\Delta_\prec(\langle X_1^{i_1} \cdots X_m^{i_m}\rangle) \cap \Delta_\prec(I)\Big) \\ &= q^m - \prod_{s=1}^{m}(q - i_s) \end{aligned}$$

Generalized Reed-Muller codes and hyperbolic codes

If $\mathrm{lm}(F(X_1, \ldots, X_m)) = X_1^{i_1} \cdots X_m^{i_m}$ then

$$w_H(\varphi(F)) \geq q^m - D(X_1^{i_1} \cdots X_m^{i_m}) = \prod_{s=1}^{m} (q - i_s)$$

The polynomial $\prod_{t=1}^{m} \prod_{s=1}^{i_t} (X_t - P_s)$ has leading monomial equal to $X_1^{i_1} \cdots X_m^{i_m}$ (for ANY ordering) and has $D(X_1^{i_1} \cdots X_m^{i_m})$ zeros.

General constructions of generalized Reed-Muller codes and hyperbolic codes along the lines in above examples.

Codes from Hermitian curve

$J = \langle X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle$. Common zeros are $\{P_1, \ldots, P_{q^3}\}$.

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

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

To estimate $w_H\left((F(P_1), \ldots, F(P_{q^3})\right)$ we consider

$$\begin{aligned} & \#(\Delta_{\prec_w}(\langle F(X,Y), X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle)) \\ \leq \; & \#\left(\Delta_{\prec_w}(\langle X^{q+1} - Y^q - Y, F(X,Y)\rangle) \cap \Delta_{\prec_w}(J)\right) \end{aligned}$$

Codes from hermitian curve

We can show:

$$\begin{aligned} & \#\Big(\Delta_{\prec_w}(\langle X^{q+1}-Y^q-Y, F(X,Y)\rangle)\cap\Delta_{\prec_w}(J)\Big) \\ \leq\ & \#\Big(\Delta_{\prec_w}(\langle X^{q+1}-Y^q, \mathrm{lm}(F(X,Y))\rangle)\cap\Delta_{\prec_w}(J)\Big) \end{aligned}$$

Proof relies on the fact that $X^{q+1}-Y^q-Y$ has precisely two monomials of highest weight and that $F\in\mathrm{Span}_{\mathbb{F}_{q^2}}(J)$ has no two monomials of same weight.

(Run Buchberger's algorithm simultaneously for $\{X^{q+1}-Y^q, \mathrm{lm}(F(X,Y))\}$ and $\{X^{q+1}-Y^q-Y, F(X,Y)\}$.)

$D(X^iY^j)$

For $X^iY^j \in \Delta_{\prec_w}(J)$ define

$$D(X_1^{i_1}\cdots X_m^{i_m}) = \#\left(\Delta_{\prec_w}(\langle X^{q+1}-Y^q, \mathrm{Im}(F(X,Y))\rangle) \cap \Delta_{\prec_w}(J)\right)$$

We have shown $w_H(\varphi(F)) \geq n - D(\mathrm{Im}(F))$, where $\varphi(F) = (F(P_1),\ldots,F(P_{q^3}))$.

$J = \langle X^3 - Y^2 - Y, X^4 - X, Y^4 - Y \rangle$

The zeros are $\{P_1, \ldots, P_8\}$.

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

Let $F(X, Y) = Y + aX + b$ then $w_H(\varphi(F)) \geq 8 - 3 = 5$.

$\Delta_{\prec_w}(J)$				$w(X^iY^j)$				$n-D(X^iY^j)$			
Y	XY	X^2Y	X^3Y	3	5	7	9	5	3	2	1
1	X	X^2	X^3	0	2	4	6	8	6	4	2

$$\begin{aligned} E(s) &= \mathrm{Span}_{\mathbb{F}_4}\{\varphi(X^iY^j) \mid w(X^iY^j) \le s, X^iY^j \in \Delta_{\prec_w}(J)\} \\ &= \mathrm{Span}_{\mathbb{F}_4}\{\varphi(X^iY^j) \mid w(X^iY^j) \le s\} \end{aligned}$$

$$\tilde{E}(s) = \mathrm{Span}_{\mathbb{F}_4}\{\varphi(X^iY^j) \mid n-D(X^iY^j) \ge s, X^iY^j \in \Delta_{\prec_w}(J)\}$$

$E(0)$ 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 $[8,3,5]$, $\tilde{E}(2)$ is $[8,7,2]$, ...

Some observations on $D(X^iY^j)$

Observation 1:

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

$w(X^iY^j) \geq D(X^iY^j)$

Observation 2:

$w(X^iY^j)$				$8 - D(X^iY^j)$			
3	5	7	9	5	3	2	1
0	2	4	6	8	6	4	2

$n - D(X^iY^j)$ counts what $w(X^iY^j)$ can hit. Meaning that:

$8 - D(Y) = 5$ as $3 + 0 = 3$, $3 + 2 = 5$, $3 + 3 = 6$, $3 + 4 = 7$ and $3 + 6 = 9$

$8 - D(XY) = 3$ as $5 + 0 = 0$, $5 + 2 = 7$ and $5 + 4 = 9$

Some observations on $D(X^iY^j)$ - continued

Observation 1:
$w(X^iY^j) \geq D(X^iY^j)$

Observation 2:
$n - D(X^iY^j)$ counts what $w(X^iY^j)$ can hit.

These observations can be shown to hold for general $I = \langle X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle$ as a consequence of the following facts:

Fact 1:
The polynomial $\{X^{q+1} - Y^q - Y\}$ has precisely two monomials of highest weight.

Fact 2: In $\Delta_{\prec_w}(\langle X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle)$ there are no two monomials of the same weight.

$J = \langle X^9 - X, Y^9 - Y, X^4 - Y^3 - Y \rangle$ has 27 common points.
$w(X) = 3, w(Y) = 4$

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

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

Hermitian codes

Our method gives true minimum distance for all codes $E(s)$ and all codes $\tilde{E}(s)$ coming from the Hermitian curve.

The estimations are even tight in general case of norm-trace curves.

Generalized RM codes and hyperbolic 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

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

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

$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	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

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

Generalized RM codes and hyperbolic 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

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

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

$J = \langle X^q - X, Y^q - Y \rangle$ and $I = \langle \ \rangle$

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

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

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

$J = \langle X^3 - Y^2 - Y, X^q - X, Y^q - Y \rangle$ and

$I = \langle X^3 - Y^2 - Y \rangle$

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

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

Forgetting about the $X_1^q - X_1, \ldots, X_m^q - X_m$

- $\emptyset$ is a Gröbner basis for $\langle 0 \rangle$ and $\{X^{q+1} - Y^q - Y\}$ is a Gröbner basis for $\langle X^{q+1} - Y^q - Y \rangle$. Both with respect to some weighted degree monomial ordering.
- In examples so far 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.
- $\mathbb{F}_q[X, Y]$ 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 $M_1 \prec_{\mathcal{M}} M_2$.

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

Order domain assumptions:
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.

Another example

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

Definition of $\prec_w$: $w(X) = 16, w(Y) = 20, w(Z) = 25 \in \mathbb{N}_0$.
$\prec_{\mathbb{N}_0} = <$ (the usual (and unique) monomial ordering on $\mathbb{N}_0$).
$\prec_{\mathcal{M}}$ the lexicographic ordering with $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z$.

$\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z\}$ is a Gröbner basis w.r.t. $\prec_w$.
Every defining monomial has precisely two monomials of highest weight.
Monomials in footprint $\Delta_{\prec}(I) = \{X^i Y^j Z^l \mid j < 4, l < 4\}$ is of different weights.

The order domain assumption is satisfied.

$D(X_1^{i_1} \cdots X_m^{i_m})$

Assume

$$I = \langle F_1, \dots, F_s \rangle \subseteq \mathbb{F}_q[X_1, \dots, X_m]$$

satisfy the order domain assumption and define

$$J = \langle F_1, \dots, F_s, X_1^q - X_1, \dots, X_m^q - X_m \rangle$$

Let $B_1, \dots, B_s$ be binomials, B_i being the difference of the two monomials of highest weight in F_s

Given $F \in \mathrm{Span}\{M \mid M \in \Delta_{\prec_w}(J)\}$ with $\mathrm{lm}(F) = N$ we have

$$\Delta_{\prec_w}(\langle N, B_1, \dots, B_s \rangle) \supseteq \Delta_{\prec_w}(\langle F, F_1, \dots, F_s \rangle)$$

Define

$$D(N) = \#\left(\Delta_{\prec_w}(\langle N, B_1, \dots, B_s \rangle) \cap \Delta_{\prec_w}(J)\right).$$

We conclude

$$w_H\left((F(P_1), \dots, F(P_n))\right) \geq n - D(N).$$

Some nice results

Result 1:

$$n - D(X_1^{i_1} \cdots X_m^{i_m}) \quad = \quad \#\{s \in w(\Delta_{\prec_w}(J)) \mid \\ s - w(X_1^{i_1} \cdots X_m^{i_m}) \in w(\Delta_{\prec_w}(J))\}$$

(we count what can be “hit”)

Result 2:
If weights are **numerical**, then

$$D(X_1^{i_1} \cdots X_m^{i_m}) \leq w(X_1^{i_1} \cdots X_m^{i_m}).$$

Code constructions

$E(s)$ and $\tilde{E}(s)$ codes along the lines of above examples.

Time does not permit to go in deeper detail here.

Some features of the theory

- Works for any one-point geometric Goppa code
- Gives improved one-point geometric Goppa codes
- Generalizations of one-point geometric Goppa codes to surfaces
- Easily extended to deal with generalized Hamming weights
- Connects nicely to Shibuya and Sakaniwa's nice theory
- Theory can be reformulated directly in "code-domain". Doing this allows for even more codes to be treated.
- Strong connection to Feng-Rao theory

Feng-Rao theory

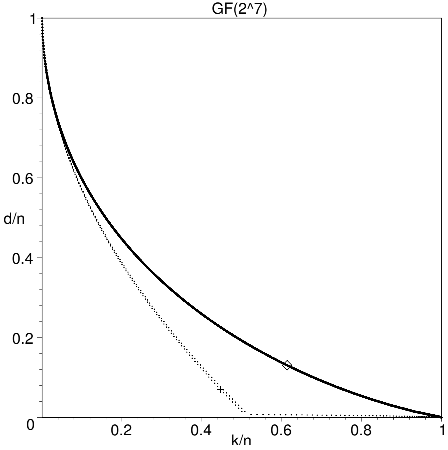
Are concerned with H instead of G (dual description).

Feng-Rao counts what can hit the weight under consideration.
We count what the weight under consideration can hit.
Feng-Rao investigate weights not used in code construction
We investigate weights used in code construction

When $\Delta_{\prec_w}(J)$ has the shape of a box (in some dimension) the two methods produce same estimates for the two classes of codes under consideration.

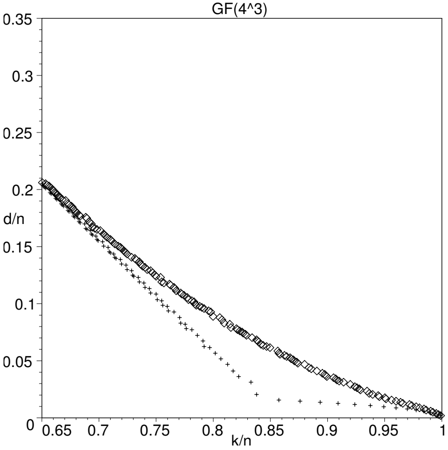
When not form of a box we get typically not similar estimates as Feng-Rao.

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



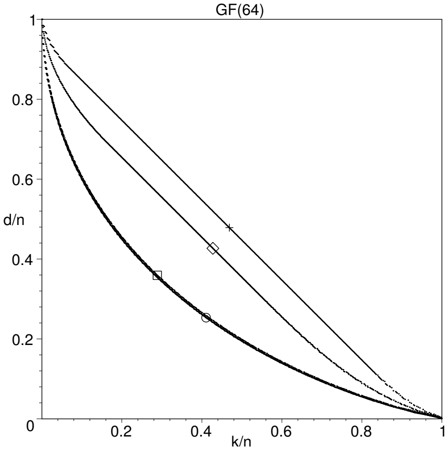
Alphabet=$\mathbb{F}_{q^r} = \mathbb{F}_{2^7}$, $n = 2^{13}$ Improved versus non-improved.

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



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

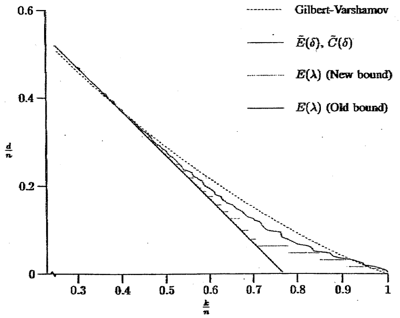
$$I = \langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y \rangle \subseteq \mathbb{F}_{q^r}[X,Y]$$



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

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

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

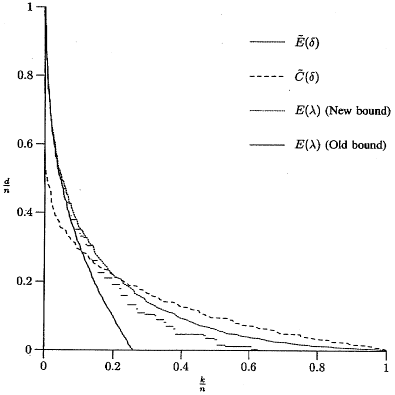


alphabet $= \mathbb{F}_{16}$, $n = 256$

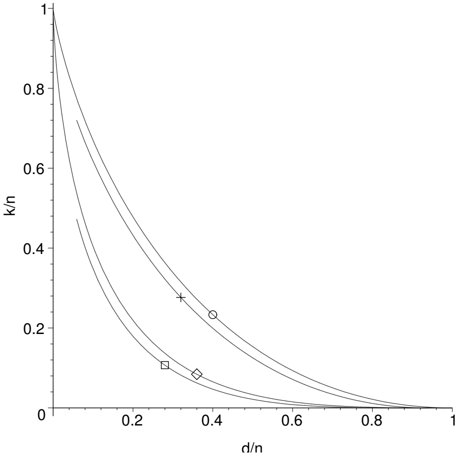
$I = \langle X^5 - Y^4 - Y,\ Y^5 - Z^4 - Z,\ Z^5 - U^4 - U^2 \rangle \subseteq \mathbb{F}_{16}[X, Y, Z, U]$

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

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



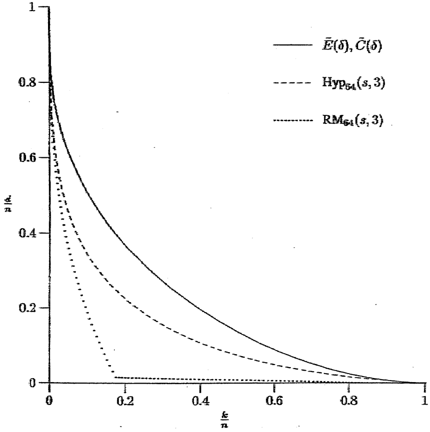
Tensor product of m Hermitian order domains involves weights in $\mathbb{N}_0^m$.



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 $n = 68719476736$.

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

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



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

- H. E. Andersen, O. Geil, The Missing Evaluation Codes from Order Domain Theory, (2004), submitted.
- O. Geil, On Codes From Norm-Trace Curves, *Finite Fields and their Applications*, **9**, (2003), 351-371.
- O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci. 2227*, (S. Bozta, I. Sphparlinski, Eds.), Springer, Berlin, 2001, 159-171.
- 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.

- S. Miura, Ph.D. thesis, Univ. Tokyo, May 1997.
- S. Miura, Linear Codes on Affine Algebraic Varieties, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1386-1397.
- S. Miura, Linear Codes on Affine Algebraic Curves, *Trans. IEICE*, **J81-A**, no. 10 (1998), 1398-1421.
- T. Shibuya and K. Sakaniwa, A Dual of Well-Behaving Type Designed Minimum Distance, *IEICE Trans. Fund.*, **E84-A**, (2001), 647-652.