Algebraic Geometry Codes In a Pure Gröbner Basis Theoretical Setting

O. Geil

Aalborg University

KIAS-RIMS joint workshop on Computer Algebra,
Kyoto July 31-August 4 - 2006

Outline

Model

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

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

$P_i(e_i = 0) = p$ 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

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

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

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

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

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

Minimum distance decoding

Decoding procedure:
When we receive $\vec{r}$ we investigate if there exist a code word $\vec{c}$ with

$$\mathrm{dist}_H(\vec{c}, \vec{r}) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

If positive we decode to $\vec{c}$.

Minimum distance decoding corrects errors with high probability.

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 Codes

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

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

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

$C(s) = \varphi(R_s) = \{(F(P_1), \ldots, F(P_n)) \mid \deg F \leq s\}, \quad s \in \{0, \ldots, n-1\}$

One possible generator matrix is $G = \begin{bmatrix} \varphi(1) \\ \varphi(X) \\ \vdots \\ \varphi(X^s) \end{bmatrix}$

The parameters of RS codes

A polynomial of degree less than $s+1$ can have at most s zeros. Hence, $d \geq n-s$ (Singleton bound gives equality).

$[n, k, d] = [q, s+1, n-s]$.

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

The parameters of RS codes

A polynomial of degree less than $s+1$ can have at most s zeros. Hence, $d \geq n-s$ (Singleton bound gives equality).

$[n, k, d] = [q, s+1, n-s]$.

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

The parameters of RS codes

A polynomial of degree less than $s+1$ can have at most s zeros. Hence, $d \geq n-s$ (Singleton bound gives equality).

$[n,k,d] = [q, s+1, n-s]$.

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

Dual description

$C^\perp$ the dual space of C (may often have more elements in common).

A parity check matrix H for C is a generator matrix for $C^\perp$.

$C = \{\vec{c} \mid H\vec{c} = \vec{0}\}$.

For Reed-Solomon codes simple correspondence:
$C(s) = (C(n-s-2))^\perp$.

Generalizing Reed-Solomon Codes

Some nice algebraic structure R and map φ.

$C = \varphi(R')$ or $C = (\varphi(R'))^{\perp}$ for some $R' \subseteq R$.

If being set up cleverly, information on R reveals information on C.

Strategies

- Well-established theory
  - (Generalized) Reed-Muller codes (G or H)
  - Geometric Goppa codes through algebraic geometry or/and function field theory (G or H)
- More recent approaches
  - Codes from order domains (G or H).
    - (Generalized) Reed-Muller codes
    - One-point geometric Goppa codes and their duals
    - Codes from surfaces
    - Improved constructions of all the above codes

This talk: Order domain codes (G) from pure Gröbner basis theoretical point of view

Strategies

- Well-established theory
  - (Generalized) Reed-Muller codes (G or H)
  - Geometric Goppa codes through algebraic geometry or/and function field theory (G or H)
- More recent approaches
  - Codes from order domains (G or H).
    - (Generalized) Reed-Muller codes
    - One-point geometric Goppa codes and their duals
    - Codes from surfaces
    - Improved constructions of all the above codes

This talk: Order domain codes (G) from pure Gröbner basis theoretical point of view

Gröbner basis tools

Footprint (Δ-set):

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

$\#\mathbb{V}_{\bar{\mathbb{F}}}(J) \leq \#\Delta_{\prec}(J)$.

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

The map φ

Assume $\mathbb{V}_{\bar{\mathbb{F}}_q}(J)$ **is finite** and write $\{P_1, \ldots, P_n\} = \#\Delta_{\prec}(J)$

$$\varphi : \begin{cases} \mathbb{F}[X_1, \ldots, X_m]/J & \rightarrow & \mathbb{F}^n \\ F + J & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

φ is surjective homomorphism of vectorspaces.

Assume further that J **is radical.**
Then $\#\mathbb{V}_{\bar{\mathbb{F}}}(J) = \#\Delta_{\prec}(J)$.

Hence, φ is injective as well. φ is a vectorspace isomorphism.

Main observations

Main observation 1:
$w_H(\varphi(F+J)) \geq n - \#\Delta_{\prec}(\langle F\rangle + J)$

Main observation 2: (assuming J is radical and $\Delta_{\prec}(J)$ is finite)
If $R' \subseteq \mathbb{F}[X_1,\ldots,X_m]/J$ is of dimension k then $\varphi(R')$ is of dimension k.

If $\mathbb{F} = \mathbb{F}_q$ we can "make" J radical by assuming $X_1^q - X_1, \ldots, X_m^q - X_m \in J$.

To be explored in this talk...

Question:
How do we estimate $\#\Delta_{\prec}(\langle F\rangle + J)$?

Answer:
By choosing clever J and proper $\prec$ accordingly. This is the core of order domain theory.

Reed-Solomon codes revisited

$J = \langle X^q - X \rangle$. $\{P_1, \ldots, P_q\} = \mathbb{F}_q(J)$.
$\Delta_<(J) = \{1, X, \ldots, X^{q-1}\}$.

$$\{M(P_1), M(P_2), \ldots, M(P_q)) \mid M \in \{1, X, \ldots, X^{q-1}\}\}$$

is a basis for $\mathbb{F}_q^q$.

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

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

Hence,

$$w_H((F(P_1), F(P_2), \ldots, F(P_q))) \geq q - i.$$

$$\begin{array}{ccccc} & & \Delta_<(\langle X^q - X \rangle) & & \\ 1 & X & X^2 & \cdots & X^{q-2} & X^{q-1} \end{array} \qquad \begin{array}{cccccc} & & & \#\Delta_<(\langle X^i, X^q \rangle) & & \\ 0 & 1 & 2 & \cdots & q-2 & q-1 \end{array}$$

$\dim(C(s)) = s + 1$ and $d(C(s)) \geq q - s$ follows.

Generalized Reed-Muller codes and hyperbolic codes

$J = \langle X^5 - X, Y^5 - Y \rangle$. $\mathbb{V}_{\mathbb{F}_5}(J) = \{P_1, \ldots, P_{25}\}$.
$\varphi(F + J) = (F(P_1) \ldots, F(P_{25}))$.
Let $\prec$ ANY monomial ordering.

$w_H(\varphi(F + J)) = 25 - \#\Delta_\prec(\langle F \rangle + J)$
$\geq 25 - \#\Delta_\prec(\langle \mathrm{Im}(F) \rangle + J) = 25 - \#\Delta_\prec(\langle \mathrm{Im}(F), X^5, Y^5 \rangle)$

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

$F(X, Y) = XY + aX^2 + bY + cX + d$. Choose $\prec$ with $X^2 \prec XY$.
$w_H(\varphi(F + J)) \geq 16$

Generalized Reed-Muller codes

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

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

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

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

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

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

Hyperbolic codes

Choose $X^i Y^j$'s with $\#\Delta(\langle X^5, Y^5, X^i Y^j \rangle)$ 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	$*$

$J = \langle X^8 - X, Y^8 - Y \rangle$, $\mathbb{V}_{\mathbb{F}_8}(I) = \{P_1, \ldots, P_{64}\}$

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

$J = \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$.
$\mathbb{V}_{\mathbb{F}_q}(J) = \{P_1, \ldots, P_{q^m}\}$.

For $X_1^{i_1} \cdots X_m^{i_m} \in \mathrm{Span}_{\mathbb{F}_q}\{M \in \Delta_\prec(J)\}$ define

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

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.

Generalized Reed-Muller codes and hyperbolic codes

For any s, $0 \leq s \leq (q-1)m$ we have

$$\begin{aligned} \mathrm{RM}_q(s,m) &= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(X^{i_1}\cdots X^{i_m}+J) \mid i_1,\ldots,i_m < q \\ &\qquad \text{and } \ i_1+\cdots+i_m \leq s\} \end{aligned}$$

$$\begin{aligned} d\left(\mathrm{RM}_q(s,m)\right) &= \min\{q^m - D(X_1^{i_1}\cdots X_m^{i_m}) \mid i_1,\ldots,i_m < q \\ &\qquad \text{and } \ i_1+\cdots+i_m \leq s\} \end{aligned}$$

And for any $s \in D(\Delta_{\prec}(J))$ we have

$$\begin{aligned} \mathrm{Hyp}_q(s,m) &= \mathrm{Span}_{\mathbb{F}_q}\{\varphi(X^{i_1}\cdots X^{i_m}+J) \mid i_1,\ldots,i_m < q \\ &\qquad \text{and } \ D(X_1^{i_1}\cdots X_m^{i_m}) \leq s\}. \end{aligned}$$

$$d\left(\mathrm{Hyp}_q(s,m)\right) = n - s$$

Corresponding dimensions easily found by simple counting.

Codes from Hermitian curve

$J = \langle X^{q+1} - Y^q - Y, X^{q^2} - X, Y^{q^2} - Y \rangle$.
$\mathbb{V}_{\mathbb{F}_{q^2}}(J) = \{P_1, \ldots, P_{q^3}\}$.

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 $w_H(\varphi(F+J))$ we consider

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

We next show that last expression is at most equal to

$$\# \left(\Delta_{\prec_w}(\langle X^{q+1} - Y^q, \mathrm{Im}(F(X,Y))\rangle) \cap \Delta_{\prec_w}(J)\right)$$

Run 1:
Apply Buchberger's algorithm to $\{X^{q+1} - Y^q, \mathrm{Im}(F)\}$ with respect to $\prec_w$.
By induction any polynomial produced in any step of the algorithm is either 0 or is a monomial.

Run 2:
Apply **simultaneously and in a similar manner** Buchberger's algorithm to $\{X^{q+1} - Y^q - Y, F(X,Y)\}$.
Every time a monomial N is produced in "Run 1" a polynomial having N as unique monomial of highest weight is produced in "Run 2".
This is due to the fact that F has a unique monomial of highest weight and that $X^{q+1} - Y^q - Y$ has exactly two monomials of highest weight.
"Run 2" may continue after termination of "Run 1".

$D(X^iY^j)$

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 $w_H(\varphi(F)) \geq n - D(\mathrm{Im}(F))$.

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

$\mathbb{V}_{\mathbb{F}_4}(J) = \{P_1, \ldots, P_8\}$.

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

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

$$\begin{array}{cccc|cccc|cccc}
\multicolumn{4}{c}{\Delta_{\prec_w}(J)} & \multicolumn{4}{c}{w(X^iY^j)} & \multicolumn{4}{c}{n-D(X^iY^j)} \\
Y & XY & X^2Y & X^3Y & 3 & 5 & 7 & 9 & 5 & 3 & 2 & 1 \\
1 & X & X^2 & X^3 & 0 & 2 & 4 & 6 & 8 & 6 & 4 & 2
\end{array}$$

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

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

$E(0)$ 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 $[8,5,3]$, $\tilde{E}(6)$ is $[8,7,2]$, ...

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

Observation 1:

$$\begin{array}{cccc} \multicolumn{4}{c}{w(X^iY^j)} \\ 3 & 5 & 7 & 9 \\ 0 & 2 & 4 & 6 \end{array} \qquad \begin{array}{cccc} \multicolumn{4}{c}{D(X^iY^j)} \\ 3 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 \end{array}$$

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

Observation 2:

$$\begin{array}{cccc} \multicolumn{4}{c}{w(X^iY^j)} \\ 3 & 5 & 7 & 9 \\ 0 & 2 & 4 & 6 \end{array} \qquad \begin{array}{cccc} \multicolumn{4}{c}{8 - D(X^iY^j)} \\ 5 & 3 & 2 & 1 \\ 8 & 6 & 4 & 2 \end{array}$$

$n - D(X^iY^j)$ 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.
$w(X) = 3, w(Y) = 4$

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

$n - D(X^4Y^2) =$
$\#\{20 + 0, 20 + 3, 20 + 4, 20 + 6, 20 + 8, 20 + 9, 20 + 12\} = 7$

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

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

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

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

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

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

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

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

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

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

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

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

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 $M_1 \prec_{\mathcal{M}} M_2$.

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

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.

More defining polynomials

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.

Weights in $\mathbb{N}_0^2$

$$H_1 = X^q + YZ^q - Y^qZ - X, H_2 = U^q - Z^{q+1} + aX^q - aY^qZ + bY^{q+1} + U$$

where $a, b \in \mathbb{F}_q$. $\quad I = \langle H_1, H_2 \rangle \subseteq \mathbb{F}_{q^2}[X, Y, Z, U]$.

Definition of $\prec_w$:
$w(X) = (q, 1), w(Y) = (0, q), w(Z) = (q, 0), w(U) = (q+1, 0) \in \mathbb{N}_0^2$
$\prec_{\mathbb{N}_0^2}$ any fixed monomial ordering on $\mathbb{N}_0^2$ with
$(q^2 + q, 0) \succ_{\mathbb{N}_0^2} (q^2, q), (q, q^2), (0, q^2 + q)$.
$\prec_{\mathcal{M}}$ any fixed monomial ordering on $\mathcal{M}(X, Y, Z, U)$ with
$X^q \succ_{\mathcal{M}} YZ^q$ and $U^q \succ_{\mathcal{M}} Z^{q+1}$.

H_1: $\quad w(X^q) = (q^2, q)$, $w(YZ^q) = (q^2, q)$, $w(Y^qZ) = (q, q^2)$, $w(X) = (q, 1)$
H_2: $\quad w(U^q) = (q^2 + q, 0)$, $w(Z^{q+1}) = (q^2 + q, 0)$, $w(X^q) = (q^2, q)$, $w(Y^qZ) = (q, q^2)$, $w(Y^{q+1}) = (0, q^2 + q)$, $w(U) = (q + 1, 0)$.

Weights in $\mathbb{N}_0^2$ - continued

$\mathrm{Im}(H_1) = X^q$ and $\mathrm{Im}(H_2) = U^q$ are relatively prime. Hence, $\{H_1(X,Y,Z,U), H_2(X,Y,Z,U)\}$ is a Gröbner basis.
H_1 and H_2 have exactly two polynomials of highest weight.
No two monomials in footprint are of same weight.

The order domain assumption is satisfied.

Putting $X_1^q - X_1, \ldots, X_m^q - X_m$ back in place

Assume $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ satisfy the order domain assumption.

Let $J = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$

$\mathbb{V}_{\mathbb{F}_q}(J) = \{P_1, \ldots, P_n\}$

$$\varphi : \begin{cases} \mathbb{F}_q[X_1, \ldots, X_m]/J & \rightarrow & \mathbb{F}_q^n \\ F + J & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

is an isomorphism

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

Assume

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

satisfy the order domain assumption.

Let $B_1, \ldots, B_s$ 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

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

Define

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

We have

$$w_H(\varphi(F + J)) \geq n - D(N).$$

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

For weights being numerical:

For any $s \in \mathbb{N}_0$ we have

$$E(s) = \mathrm{Span}_{\mathbb{F}_q}\{\varphi(M+J) \mid M \in \Delta_{\prec_w}(J) \text{ and } w(M) \leq s\}$$

$$d(E(s)) \geq \min\{n - D(M) \mid M \in \Delta_{\prec_w}(J) \text{ and } w(M) \leq s\}$$

For weights being numerical or not:

For any $s \in D(\Delta_{\prec}(J))$ we have

$$\tilde{E}(S) = \mathrm{Span}_{\mathbb{F}_q}\{\varphi(m+J) \mid m \in \Delta_{\prec_w}(J) \text{ and } n - D(M) \geq s\}.$$

$$d(E(s)) \geq s$$

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.

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.

Open question:
Are the two classes of codes the same when $\Delta_{\prec_w}(J)$ has the shape of a box?

$I = \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z$ revisited

$J = \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z, X^{16} - X, Y^{16} - Y, Z^{16} - Z \rangle \subseteq \mathbb{F}_{16}[X, Y, Z]$ has Gröbner basis $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z, X^{16} - X, Y^{16} - Y, Z^{16} - Z\}$ with respect to $\prec_w$.

Footprint has the shape of box.

Codes will be of length $n = \#\Delta_{\prec_w}(J) = 256$.

$I = \langle H_1, H_2 \rangle$ revisited

$$J = \langle H_1, H_2, X^{q^2} - X, Y^{q^2} - Y, Z^{q^2} - Z, U^{q^2} - U \rangle \subseteq \mathbb{F}_{q^2}[X, Y, Z, U]$$

has Gröbner basis

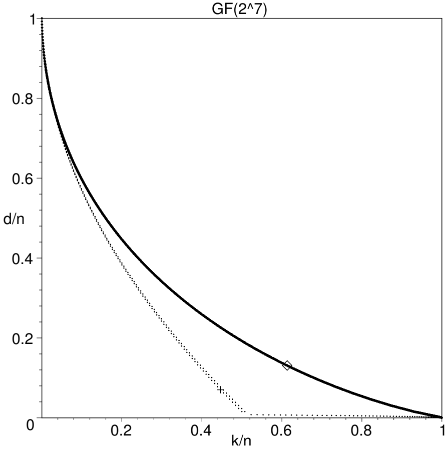
$$\{H_1, H_2, X^{q^2} - X, Y^{q^2} - Y, Z^{q^2} - Z, U^{q^2} - U\}$$

with respect to $\prec_w$.

Footprint is a box.

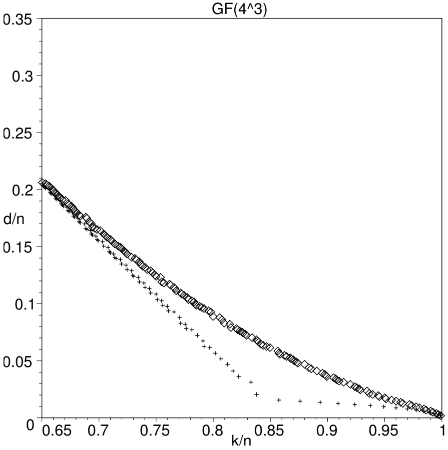
Codes will be of length $n = \#\Delta_{\prec_w}(J) = q^6$

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



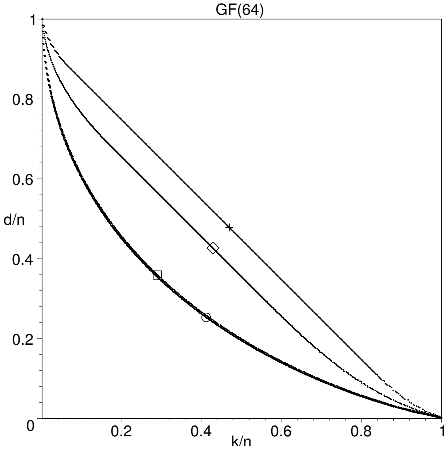
Alphabet=$\mathbb{F}_{q^r} = \mathbb{F}_{2^7}$, $n = 2^{13}$ Improved versus non-improved.

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



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

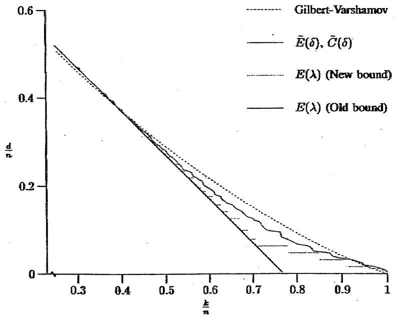
$$I = \langle X^{(q^r-1)/(q-1)} - Y^{q^{r-1}} - Y^{q^{r-2}} - \cdots - Y \rangle \subseteq \mathbb{F}_{q^r}[X, Y]$$



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 $n = 2^{12}$

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

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

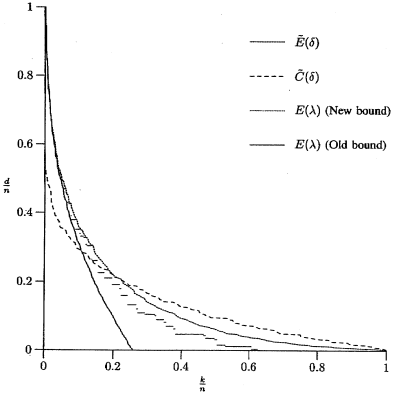


alphabet $= \mathbb{F}_{16}$, $n = 256$

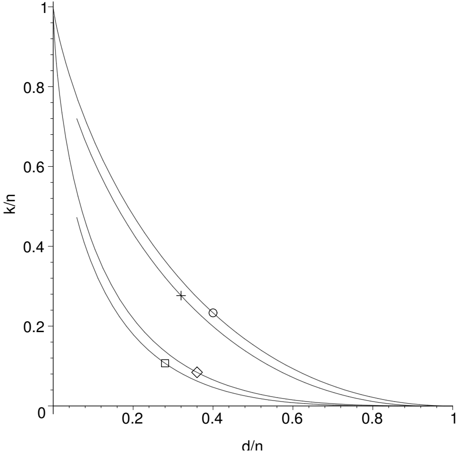
$I = \langle X^5 - Y^4 - Y, Y^5 - Z^4 - Z, Z^5 - U^4 - U^2 \rangle \subseteq \mathbb{F}_{16}[X, Y, Z, U]$

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

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



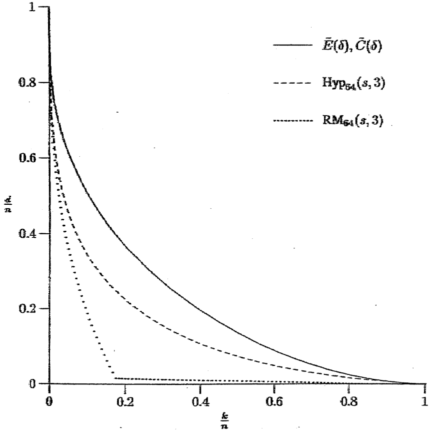
Tensor product of m Hermitian order domains involves weights in $\mathbb{N}_0^m$.



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

Invitation

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?

Invitation 2: Only a few have looked at surfaces. More examples would be desirable

Invitation

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?

Invitation 2: Only a few have looked at surfaces. More examples would be desirable

Invitation

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?

Invitation 2: Only a few have looked at surfaces. More examples would be desirable

Invitation

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?

Invitation 2: Only a few have looked at surfaces. More examples would be desirable

Invitation

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?

Invitation 2: Only a few have looked at surfaces. More examples would be desirable

- 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.