General Constructions of Multi-Structured Designs

Ryoh Fuji-Hara
University of Tsukuba

Joint work with Ying Miao

1

Cyclotomic classes

$GF(q), q$ *a prime power* $q = ef + 1$

α : *a primitive element*

$$C_i = \{\alpha^i, \alpha^{i+e}, \alpha^{i+2e}, \cdots, \alpha^{i+(f-1)e}\}$$

$for\ i = 0, 1, ..., e-1$

2

Example

$GF(13), \quad 13 = 3 \cdot 4 + 1$

2 : *a primitive element*

$$C_0 = \{2^0, 2^3, 2^6, 2^9\}$$
$$C_1 = \{2^1, 2^4, 2^7, 2^{10}\}$$
$$C_2 = \{2^2, 2^5, 2^8, 2^{11}\}$$

3

(Internal) difference family

C_0= {1, 8, 12, 5},
C_1= {2, 3, 11, 10},
C_2= {4, 6, 9, 7}

$$\Delta_{13}(C_0) + \Delta_{13}(C_1) + \Delta_{13}(C_2)$$

= { 1, 1, 1, 2, 2, 2, 3, 3, 3, 4, 4, 5,
5, 5, 6, 6, 6, 7, 7, 7, 8, 8, 8, 9, 9,
9, 10, 10, 10, 11, 11, 11, 12, 12, 12 }

$= 3\ (GF(13) \setminus \{0\})$

4

Theorem

Let $C_0, C_1, ..., C_{e-1}$ cyclotomic classes
$q = ef + 1$ a prime

$$\sum \Delta_q(C_i) = \lambda(\mathbf{Z}_q \setminus \{0\})$$
$$\lambda = f - 1$$

=> An Optimal Frequency Hopping Sequence

5

A property on external differences

$$\vec{\mathbf{B}}_1 = (C_0, C_1, C_2)$$
$$\vec{\mathbf{B}}_2 = (C_1, C_2, C_0)$$

$$\Delta_{13}(C_0, C_1) + \Delta_{13}(C_1, C_2) + \Delta_{13}(C_2, C_0)$$

= {1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6,
6, 6, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, 10, 10, 10, 10, 11,
11, 11, 11, 12, 12, 12, 12}

$= 4\ (GF(13) \setminus \{0\})$

6

$$\vec{\mathbf{B}}_0 = (C_0, C_1, ..., C_{e-1})$$
$$\vec{\mathbf{B}}_1 = (C_1, C_2, ..., C_0)$$
$$\vdots$$
$$\vec{\mathbf{B}}_{e-1} = (C_{e-1}, C_0, ..., C_{e-2})$$

Theorem (Chu and Colbourn)

$q = ef + 1$ a prime

$$\sum_{i=0}^{e-1} \Delta_q(C_i, C_{i+k}) = f(\mathbf{Z}_q \setminus \{0\})$$ for any k

=> Optimal Frequency Hopping Sequences

if $f \geq 2$ and $e \geq 3f$

=> Cyclic Balanced Arrays

7

$q = 2ef + 1$ a prime

$D = \{\alpha^{2i} \mid 1 \leq i \leq (q-1)/2\}$ a subgroup of order ef a difference set

Theorem (Tonchev)

$C_i = \{\alpha^{2i}, \alpha^{2(i+e)}, \alpha^{2(i+2e)}, ..., \alpha^{2(i+(f-1)e)}\}$

$for\ i = 0, 1, ..., e-1$ subgroup and its cosets of D

$\tilde{\mathbf{B}} = \{C_0, C_1, ..., C_{e-1}\}$ DSS ρ = (q − 2f − 1)/4

regular and perfect

8

Example

v =31=2·5·3+1 ω=3 as a primitive element modulo 31

$C_0 = \{3^0 \equiv 1, 3^6 \equiv 16, 3^{12} \equiv 8, 3^{18} \equiv 4, 3^{24} \equiv 2\}$

$C_2 = \{9, 20, 10, 5, 18\} = C_0 3^2$

$C_4 = \{19, 25, 28, 14, 7\} = C_0 3^4$

$$\tilde{\mathbf{B}} = \{C_0, C_2, C_4\}$$

$\sum \Delta_{31}(C_i) = 2(\mathbf{Z}_{31} \setminus \{0\})$ difference family

$\Delta_{31}(C_0 \cup C_2 \cup C_4) = 7(\mathbf{Z}_{31} \setminus \{0\})$

the union is a difference set

$\sum_{i \neq j} \Delta_{31}(C_i, C_j) = 5(\mathbf{Z}_{31} \setminus \{0\})$

difference system of sets

9

On an Extension Field

$GF(3^2) : 9 = 2 \cdot 4 + 1 \quad (\alpha^2 = \alpha + 1)$

α : *a primitive element*

$$C_0 = \{\alpha^0, \alpha^2, \alpha^4, \alpha^6\}$$
$$C_1 = \{\alpha^1, \alpha^3, \alpha^6, \alpha^7\}$$

10

$$\Delta_{GF(9)}(C_0) + \Delta_{GF(9)}(C_1) = 3(GF(9) \setminus \{0\})$$

{C₀, C₁} is a difference family on the additive group of GF(9)

However

C_0	C_1	is not a cyclic design.
$C_0 + 1$	$C_1 + 1$	
$C_0 + 2$	$C_1 + 2$	
$\vdots$	$\vdots$	

11

Discrete Log $\log(\alpha^i) = i$

$GF(q), \quad q = ef + 1$ an extension field

Cyclotomic classes : $C_0, C_1, ..., C_{e-1}$

$for\ i \neq 0$

$$D_i = \log(C_i - 1) = \{\log(c-1) | c \in C_i\} \subset \mathbb{Z}_{q-1}$$

$for\ i = 0$

$$D_0 = \begin{cases} \{(q-1)/2\} \cup \log(C_0 - 1) \setminus \{\infty\} & \text{if } q \text{ is odd} \\ \{0\} \cup \log(C_0 - 1) \setminus \{\infty\} & \text{if } q \text{ is even} \end{cases}$$

replace ∞ by (q-1)/2 or 0

12

$$\mathcal{D} = \sum_j \Delta_{q-1}(D_j)$$

$\lambda_i(\mathcal{D})$: the number of the integer i which appears in $\mathcal{D}$

Theorem(Ding and Yin)

$$\lambda_i(\mathcal{D}) \leq f \quad for\ 1 \leq i < q-1$$

where $GF(q),\ \ q = ef + 1$

Example $GF(3^2) : 9 = \ 2 \cdot 4 + 1$

$$C_0 = \{\alpha^0, \alpha^2, \alpha^4, \alpha^6\}$$
$$C_1 = \{\alpha^1, \alpha^3, \alpha^5, \alpha^7\}$$

$$\begin{aligned} D_0' &= \log(C_0 - 1) \\ &= \log\{\alpha^0 - 1 = 0, \alpha^2 - 1 = \alpha, \alpha^4 - 1 = \alpha^0, \alpha^6 - 1 = \alpha^3\} \\ &= \{\infty, 1, 0, 3\} \end{aligned}$$

$$D_0 = \{4, 1, 0, 3\}$$
$$D_1 = \log(C_1 - 1) = \{7, 5, 6, 2\}$$

$\Delta_8(D_0) + \Delta_8(D_1) =$ { 1, 1, 1, 1, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 7, 7, 7, 7}

Example Even case

$$q = 2^4 = 3 \cdot 5 + 1 \quad (1 + \alpha = \alpha^4)$$

$$C_0 = \{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$$
$$C_1 = \{\alpha^1, \alpha^4, \alpha^7, \alpha^{10}, \alpha^{13}\}$$
$$C_2 = \{\alpha^2, \alpha^5, \alpha^8, \alpha^{11}, \alpha^{14}\}$$

$$D_0' = \log(C_0 - 1) = \{\infty, 14, 13, 7, 11\}$$

$$D_0 = \{0, 14, 13, 7, 11\}$$
$$D_1 = \log(C_1 - 1) = \{4, 1, 9, 5, 6\}$$
$$D_2 = \log(C_2 - 1) = \{8, 10, 2, 12, 3\}$$

$$\Delta_{15}(D_0) + \Delta_{15}(D_1) + \Delta_{15}(D_2)$$

= { 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 6, 7, 7, 7, 7, 7, 8, 8, 8, 8, 8, 9, 9, 9, 10, 10, 10, 10, 11, 11, 11, 11, 11, 12, 12, 12, 13, 13, 13, 13, 13, 14, 14, 14, 14, 14}

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
λ_i	5	5	3	5	4	3	5	5	3	4	5	3	5	5

where $q = 2^4 = 3 \cdot 5 + 1$

$q = ef + 1$

$$\vec{\mathbf{B}}_0 = (D_0, D_1, ..., D_{e-1})$$
$$\vec{\mathbf{B}}_1 = (D_1, D_2, ..., D_0)$$
$$\vec{\mathbf{B}}_{e-1} = (D_{e-1}, D_0, ..., D_{e-2})$$

$$\mathcal{F}_u = \sum_j \Delta_{q-1}(D_j, D_{j+u})$$

Theorem (Ding and Yin)

$$\lambda_i(\mathcal{F}_u) \leq f + 2$$
$$for\ 1 \leq i < q-1,\ 1 \leq u \leq e-1$$

=> FHS with e sequences

q=3・5+1

$$\Delta_{15}(D_0, D_1) + \Delta_{15}(D_1, D_2) + \Delta_{15}(D_2, D_0)$$

= {1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 8, 8, 8, 8, 8, 9, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 10, 10, 11, 11, 11, 11, 11, 12, 12, 12, 12, 12, 12, 13, 13, 13, 13, 13, 14, 14, 14, 14, 14}

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
λ_i	5	5	6	5	4	6	5	5	6	7	5	6	5	5

Note : $\frac{3 \cdot 25}{14} = 5.357$ (avarage of λ_i)

Geometrical Methods

Affine Geometry AG(n,q)

α : a primitive element of $GF(q^n)$

Points

$\alpha^\infty = 0,\ \alpha^0, \alpha^1, \alpha^2, ..., \alpha^{v-1}, \qquad v = q^n - 1$

$V = \{\infty, 0, 1, 2, .., v-1\}$

Line XY

$XY = \{\lambda X + (1-\lambda)Y \mid \lambda \in GF(q)\}$

19

The number of t-flats in AG(n,q)

Let $\begin{bmatrix} n \\ t \end{bmatrix}_q = \begin{cases} \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-t+1}-1)}{(q^t-1)(q^{t-1}-1)\cdots(q-1)}, & \text{if } 1 \le t \le n, \\ 1, & \text{if } t = 0. \end{cases}$

(Gaussian coefficient)

The number of t-flat in AG(n,q) containing ∞ : $\begin{bmatrix} n \\ t \end{bmatrix}_q$

The number of t-flat in AG(n,q) : $q^{n-t}\begin{bmatrix} n \\ t \end{bmatrix}_q$

20

Example: The lines of AG(3,3)

FHSS $\lambda_i \leq 2$ DSS $\beta_i \geq 10$

∞	0	13	1	9	3	2	21	12	4	18	7	6	11	10
∞	1	14	2	10	4	3	22	13	5	19	8	7	12	11
∞	2	15	3	11	5	4	23	14	6	20	9	8	13	12
∞	3	16	4	12	6	5	24	15	7	21	10	9	14	13
∞	4	17	5	13	7	6	25	16	8	22	11	10	15	14
∞	5	18	6	14	8	7	0	17	9	23	12	11	16	15
∞	6	19	7	15	9	8	1	18	10	24	13	12	17	16
∞	7	20	8	16	10	9	2	19	11	25	14	13	18	17
∞	8	21	9	17	11	10	3	20	12	0	15	14	19	18
∞	9	22	10	18	12	11	4	21	13	1	16	15	20	19
∞	10	23	11	19	13	12	5	22	14	2	17	16	21	20
∞	11	24	12	20	14	13	6	23	15	3	18	17	22	21
∞	12	25	13	21	15	14	7	24	16	4	19	18	23	22
			14	22	16	15	8	25	17	5	20	19	24	23
			15	23	17	16	9	0	18	6	21	20	25	24
			16	24	18	17	10	1	19	7	22	21	0	25
			17	25	19	18	11	2	20	8	23	22	1	0
			18	0	20	19	12	3	21	9	24	23	2	1
			19	1	21	20	13	4	22	10	25	24	3	2
			20	2	22	21	14	5	23	11	0	25	4	3
			21	3	23	22	15	6	24	12	1	0	5	4
			22	4	24	23	16	7	25	13	2	1	6	5
			23	5	25	24	17	8	0	14	3	2	7	6
			24	6	0	25	18	9	1	15	4	3	8	7
			25	7	1	0	19	10	2	16	5	4	9	8
						1	20	11	3	17	6	5	10	9

21

Example: Orthogonal Multi-Structured designs

∞	0	13	1	9	3	2	21	12	4	18	7	6	11	10
∞	1	14	2	10	4	3	22	13	5	19	8	7	12	11
∞	2	15	3	11	5	4	23	14	6	20	9	8	13	12
∞	3	16	4	12	6	5	24	15	7	21	10	9	14	13
∞	4	17	5	13	7	6	25	16	8	22	11	10	15	14
∞	5	18	6	14	8	7	0	17	9	23	12	11	16	15
∞	6	19	7	15	9	8	1	18	10	24	13	12	17	16
∞	7	20	8	16	10	9	2	19	11	25	14	13	18	17
∞	8	21	9	17	11	10	3	20	12	0	15	14	19	18
∞	9	22	10	18	12	11	4	21	13	1	16	15	20	19
∞	10	23	11	19	13	12	5	22	14	2	17	16	21	20
∞	11	24	12	20	14	13	6	23	15	3	18	17	22	21
∞	12	25	13	21	15	14	7	24	16	4	19	18	23	22
			14	22	16	15	8	25	17	5	20	19	24	23
			15	23	17	16	9	0	18	6	21	20	25	24
			16	24	18	17	10	1	19	7	22	21	0	25
			17	25	19	18	11	2	20	8	23	22	1	0
			18	0	20	19	12	3	21	9	24	23	2	1
			19	1	21	20	13	4	22	10	25	24	3	2
			20	2	22	21	14	5	23	11	0	25	4	3
			21	3	23	22	15	6	24	12	1	0	5	4
			22	4	24	23	16	7	25	13	2	1	6	5
			23	5	25	24	17	8	0	14	3	2	7	6
			24	6	0	25	18	9	1	15	4	3	8	7
			25	7	1	0	19	10	2	16	5	4	9	8
						1	20	11	3	17	6	5	10	9

22

From AG(n,q) $q = p^c$

Theorem

There exists an optimal FHS(p^{cn} -1, $p^{c(n-t)}$, p^{ct}–1) for any prime number p, $1 \le t < n$ and $1 \le c$.

Theorem

There exists a row and column design, v= q^n, block size qXq and the number of blocks $b = q^{n-2}\begin{bmatrix} n \\ 2 \end{bmatrix}_q$

23

Projective Geometry PG(n-1, q)

α : a primitive element of $GF(q^n)$

Points

$\alpha^0, \alpha^1, \alpha^2, ..., \alpha^{v-1}, \qquad v = \begin{bmatrix} n \\ 1 \end{bmatrix}_q = \dfrac{q^n-1}{q-1}$

$V = \{0, 1, 2, .., v-1\}$

Line XY

$XY = \{X + \lambda Y \mid \lambda \in GF(q)\} \cup \{Y\}$

The number of lines: $v = \begin{bmatrix} n \\ 2 \end{bmatrix}_q = \dfrac{(q^n-1)(q^{n-1}-1)}{(q-1)(q^2-1)}$

24

A t-spread is a set of t-flats in PG(n,q) which partition the points

There exists a t-spread if and only if $t+1 \mid n+1$

There is a special t-spread:

$S_i = \{0+i, m+i, 2m+i, ..., (k-1)m+i\}$

for $i = 0, 1, ..., m-1$

where $k = \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$ $m = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q / \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q$

$\sigma : x \mapsto x + m$

$\sigma(S_0) = S_0$

Let $W = \{F_0, F_1, ..., F_{u-1}\}$ $u = \begin{bmatrix} n-t \\ 1 \end{bmatrix}_q$

be the set of all $(t+1)$-flats containing S_0

Suppose $n = 2t+1$

Property

(1) $W = \{F_0, \sigma F_0, \sigma^2 F_0, ..., \sigma^{u-1} F_0\}$

(2) $\Delta_v F_i = \Delta_v F_j$ for any $F_i, F_j \in W$

Lemma

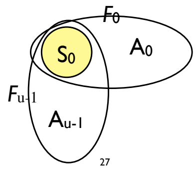
Let $A_i = F_i \setminus S$ be the affine part of the $(t+1)$-flat F_i

For $i = 0, 1, ..., u-1$, $S = S_0$

(1) $\Delta_v A_i = (q-1)(\mathbf{Z}_v \setminus S)$

(2) $\Delta_v(S, A_i) = \Delta_v(A_i, S) = \mathbf{Z}_v \setminus S$

(3) $\Delta_v F_i = (q+1)(\mathbf{Z}_v \setminus S) + k(S \setminus \{0\})$



Theorem

Let $n = 2t+1$ $u = (q^{t+1}-1)/(q-1)$

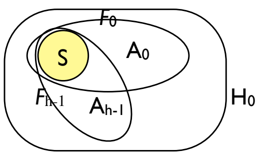
(1) Cyclic MSD $\{F_0, A_1, A_2, ..., A_{u-1}\}$ holds

$\lambda_i \le q^{t+1} + 1$ in $\Delta_v F_0 + \sum_{i=1}^{u-1} \Delta_v A_i$

(2) Cyclic MSD $\{S_0, A_0, A_1, ..., A_{u-1}\}$ holds

$\lambda_i \le q^{t+1} - 1$ in $\Delta_v S_0 + \sum_{i=0}^{u-1} \Delta_v A_i$

=> Optimal FHS



Let H_0 be a hyperplane of PG(2t+1,q) containing S

$\{F_0, F_1, ..., F_{h-1}\}$: the (t+1)-flats in H_0 containing S

$h = (q^t - 1)/(q-1)$

Theorem

(1) Cyclic MSD $\{F_0, A_1, A_2, ..., A_{h-1}\}$ holds

$\lambda_i \ge q^{2t-1} + q^{2t-2} + \cdots + q^{t+1}$

in $\sum_i \Delta_v(F_0, A_i) + \sum_{i \ne j} \Delta_v(A_i, A_j)$

(2) Cyclic MSD $\{S_0, A_{,0}, A_1, ..., A_{h-1}\}$ holds

$\lambda_i \ge q^{2t-1} + q^{2t-2} + \cdots + q^{t+1}$

in $\sum_i \Delta_v(S_0, A_i) + \sum_{i \ne j} \Delta_v(A_i, A_j)$

=> DSS

Example: DSS on PG(5,2)

$\rho = 8$

$F_0 = \{0, 1, 6, 8, 9, 14, 18, 27, 36, 38, 45, 48, 49, 52, 54\}$,

$A_1 = \{2, 12, 13, 16, 28, 33, 35, 41\}$,

$A_2 = \{3, 4, 7, 19, 24, 26, 32, 56\}$,

$\rho = 8$

$A_0 = \{1, 6, 8, 14, 38, 48, 49, 52\}$,

$A_1 = \{2, 12, 13, 16, 28, 33, 35, 41\}$,

$A_2 = \{3, 4, 7, 19, 24, 26, 32, 56\}$,

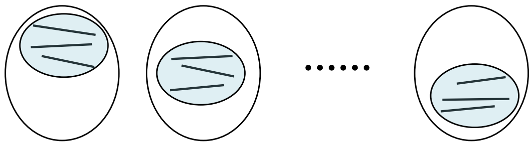
$S = \{0, 9, 18, 27, 36, 45, 54\}$.

31

Line Partition Problem

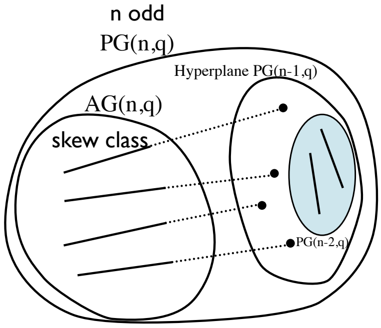
(t-partitioning, hyperplane line spread)

- A partition of the line set of PG(2n,q)
- Each class is a partition of the point set of distinct hyperplane



32

Affine skew resolution and PG Resolution



33

Theorem (Fuji-Hara and Vanstone 1988)

If there exist a hyper skew resolution in AG(2n+1,q) and a line partition in PG(2n,q), then there exists a resolution (parallelism) in PG(2n+1,q).

34

Example: PG(4,2) 31 points, 31X5 lines

Base lines of a cyclic line partition

$C_1 = \{1, 14, 15\}$,
$C_2 = \{2, 28, 30\}$,
$C_3 = \{4, 25, 29\}$,
$C_4 = \{8, 19, 27\}$,
$C_5 = \{16, 7, 23\}$

$\bigcup C_i$ is a hyperplane

(1) A disjoint difference family with $\lambda = 1$

(2) Their union is a difference set with $\lambda=7$

(3) Perfect Regular DSS $\sum_{i \neq j} \Delta_{31}(C_i, C_j) = 6(\mathbf{Z}_{31} \setminus \{0\})$

35

A cyclic line partition of PG(4,3) , v=121

$B_1 = \{28, 30, 74, 102\}$ $B_6 = \{46, 47, 51, 115\}$

$B_2 = \{69, 75, 86, 49\}$ $B_7 = \{2, 5, 17, 88\}$

$B_3 = \{71, 89, 1, 11\}$ $B_8 = \{112, 0, 36, 7\}$

$B_4 = \{77, 10, 109, 18\}$ $B_9 = \{79, 106, 93, 6\}$

$B_5 = \{95, 15, 70, 39\}$ $B_{10} = \{101, 61, 22, 3\}$

36

Known Line Partitions

Non Cyclic

PG(2^k-2,q) , q prime power,   k=2,3,...

Cyclic

PG(4,2)   PG(6,2)   PG(8,2)   PG(10,2)

PG(4,3)   PG(6,3)

PG(4,5)   PG(4,8)   PG(4,9)

37

The End

終

Thank You

38