Cyclic Multi-Structured Designs and Sequences

Ryoh Fuji-Hara
University of Tsukuba

Joint work with Ying Miao

1

Sequence, Difference and Hamming Correlation

$V = \mathbf{Z}_v$ the cyclic group of order v

Automorphism $\sigma : V \to V$ $(V, \mathfrak{B})$

$\sigma : i \mapsto i+1 \pmod v$

For any block $\mathbf{B} \in \mathfrak{B}$,

$\sigma(\mathbf{B}) = \{\sigma(b) \mid b \in \mathbf{B}\}$

is also a block of $\mathfrak{B}$

2

Sequence

$X = (x_0, x_1, x_2, x_3, \cdots, x_{v-1})$

Block

$\tilde{\mathbf{B}} = \{C_1, C_2, ..., C_n\}$, $C_i \subseteq \mathbf{B}$

$C_0 = V \setminus \cup_{i=1}^{n} C_i$

Relation

$C_i = supp_X(i) = \{j \mid x_j = i,\ 0 \le j < v\}$

for $i = 0, 1, 2, ..., n$

3

Example

X_1=(1,1,0,0,1,0,0,0,0,0,0,0,0,0,0)
X_2=(1,0,1,0,0,0,0,0,1,0,0,0,0,0,0)

B_1={ {0,1,4} }

B_2={ {0,2,8} }

4

Binary Sequences

$X = (x_0, x_1, x_2, ..., x_{v-1}),$
$Y = (y_0, y_1, y_2, ..., y_{v-1}),\quad x_i, y_i \in \{0,1\}$

Hamming correlation

$$H^{(1)}_{X,Y}(t) = \sum_{i=0}^{v-1} h_1(x_i, y_{i+t (\text{mod } v)}),\ 0 \le t < v,$$

$$h_z(a,b) = \begin{cases} 1 & \text{if } a = b = z \\ 0 & \text{otherwise} \end{cases}$$

If X=Y , it is called auto-correlation,

5

Example

X_1=(1,1,0,0,1,0,0,0,0,0,0,0,0,0,0)

X_2=(1,0,1,0,0,0,0,0,1,0,0,0,0,0,0)

X_1=(1,1,0,0,1,0,0,0,0,0,0,0,0,0,0)
(0,0,0,1,1,0,0,1,0,0,0,0,0,0,0) $x_{i+12 \pmod{15}}$

$H_{X_1,X_1}(12) = 1$

6

Unordered Blocks with single sub-block

$$\tilde{\mathbf{B}}_1 = \{\ \{C_1\}\ \}\ ,\ C_1 \subseteq \mathbf{B}_1$$

$$\tilde{\mathbf{B}}_2 = \{\ \{C_2\}\ \}\ ,\ C_1 \subseteq \mathbf{B}_2$$

Internal Differences

$$\Delta_v(C_1) = \{x - y \pmod v \mid x, y \in C_1\}$$

External Differences

$$\Delta_v(C_1, C_2) = \{x - y \pmod v \mid x \in C_1, y \in C_2\}$$

7

Example

$$C_1 = \{0, 1, 4\}\ ,\ C_2 = \{0, 2, 8\}$$

Internal Differences

$$\Delta_{15}(C_1) = \{1, 3, 4, 14, 12, 11\},\ \Delta_{15}(C_2) = \{2, 6, 8, 13, 9, 7\}$$

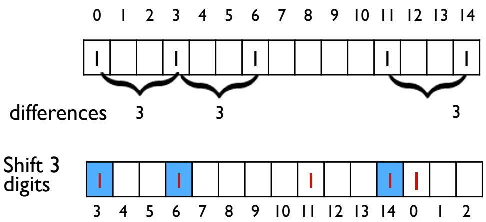
External Differences

$$\Delta_{15}(C_1, C_2) = \{0, 1, 4, 13, 14, 2, 8, 11\}$$

8

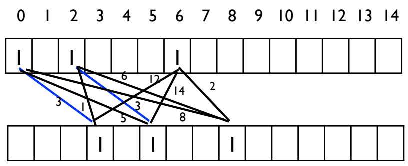
Differences and Correlation

Auto correlation



9

Cross correlation



$$\Delta_{15}(\{0, 2, 6\}, \{3, 5, 8\}) = \{1, 2, 3, 3, 5, 6, 8, 12, 14\}$$

$$\lambda_3(\{0, 2, 6\}, \{3, 5, 8\}) = 2$$

10

App. 5 **(Optical Orthogonal Code)**

$(v, k, \lambda_a, \lambda_c)$-OOC (Salehi 1989)

A set of {0,1}-sequences length v $X_1, X_2, \ldots, X_n$ with Hamming weight k satisfying

$$H^{(1)}_{X_i, X_i}(t) \leq \lambda_a \text{ for all } 1 \leq t < v$$

$$H^{(1)}_{X_i, X_j}(t) \leq \lambda_c \text{ for all } 0 \leq t < v$$

$$1 \leq i, j \leq n,\ i \neq j$$

11

$\lambda_t(C_1)$ and $\lambda_t(C_1, C_2)$ are the numbers of the integer t contained in $\Delta_v(C_1)$ and $\Delta_v(C_1, C_2)$, respectively

Property

$$\lambda_t(C_1) = H^{(1)}_{X_1, X_1}(t)$$

$$\lambda_t(C_1, C_2) = H^{(1)}_{X_1, X_2}(t)$$

12

Theorem (Bird and Keedwell)

If there exists a cyclic Steiner t-design S(t;k,v), then there exists an optimal (v,k,t-1)-OOC.

13

Related Code

Conflict-avoiding code (Levenshtein)

A code deleting the auto-correlation condition from OOC with

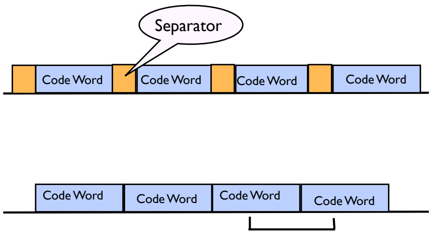
$$\lambda_c = 1$$

Condition

$$H^{(1)}_{X_i,X_j}(t) \le 1 \text{ for all } 0 \le t < v,\ 1 \le i,j \le n,\ i \ne j$$

14

App. 6 **(Comma Free Code)**



15

Structure of Codeword

Ordinal Codeword

Separator

Comma Free Codeword

Separator

16

Comma Free Code

```
2*2*121002*2*12100
          2X2X12100
```

Hamming Distance
(Ignore 'X' places)
0 4

17

Code Word

8	7	6	5	4	3	2	1	0
2	*	2	*	1	2	1	0	0

$X =$ `2 * 2 * 1 2 1 0 0`

$C_0 = \{0, 1\} = supp_X(0)$
$C_1 = \{2, 4\}$
$C_2 = \{3, 6, 8\}$

$$\sum_{i \ne j} \Delta_9(C_i, C_j) = \{4 \times \{1, 2, 3, ..., 8\}\}$$

18

If every element of $\mathbf{Z}_v \setminus \{0\}$ appears in $\sum_{i \neq j} \Delta_v(C_i, C_j)$ at least ρ times, then

$$\tilde{\mathbf{B}} = \{C_1, C_2, \ldots, C_n\}\ ,\ C_i \subseteq \mathbf{Z}_v$$
$$C_i \cap C_j = \emptyset$$

is called a DSS (Difference System of Sets), denoted by $DSS(v, n, \rho)$

regular : if $|C_i| = k$ for all $1 \leq i \leq n$

Theorem

$DSS(v, n, \rho)$ $\tilde{\mathbf{B}} = \{C_1, C_2, \ldots, C_n\}$ exists

if and only if

there exists an n- ary comma free code, where

length is v

length of separators is $s = \sum_{i=1}^{n} |C_i|$

minimum separation distance is ρ

App. 7 (Frequency Hopping Sequence)

Frequences $\mathcal{F} = \{0, 1, 2, \ldots, n\}$

Sequence $X = (x_0, x_1, \ldots., x_{v-1}),\ x_i \in \mathcal{F}$

an (n+1)-ary sequence

auto-correlation $H_{X,X}(t) = \sum_{k=0}^{n} H_{X,X}^{(k)}(t)$

cross-correlation $H_{X,Y}(t) = \sum_{k=0}^{n} H_{X,Y}^{(k)}(t)$

Correlations

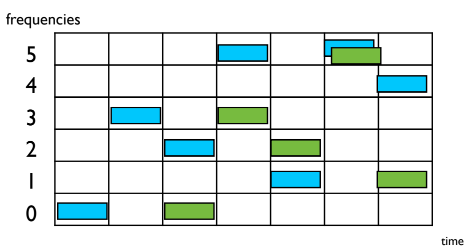
$$H(X) = \max_{1 \leq t < v} \{H_{X,X}(t)\}$$

$$H(X, Y) = \max_{0 \leq t < v} \{H_{X,Y}(t)\}$$

$$M(X, Y) = \max\{H(X), H(Y), H(X, Y)\}$$

Frequency Hopping Communication

X=(0,3,2,5,1,5,4....)



Bounds

Lempel and Greenberger(1974)
Fuji-Hara, Miao and Mishima(2004)

X : an m-ary sequence of length v $m = n + 1$ the number of frequences

$$H(X) \geq \lceil v/m \rceil \text{ when } v \neq m$$

Peng and Fan (2004)

$\mathcal{X}$: a set of m-ary sequences of length $v,\ |\mathcal{X}| = n$

$$M(\mathcal{X}) = \max\{\max_{X \in \mathcal{X}} H(X), \max_{X,Y \in \mathcal{X}, X \neq Y} H(X, Y)\}$$

$$M(\mathcal{X}) \geq \left\lceil \frac{(vn - m)v}{(vn - 1)m} \right\rceil$$

The set of sequences meeting the bound is called *optimal Frequency Hopping Sequences*

MSD and FH sequences

$$\vec{\mathbf{B}}_1 = (C_0, C_1, ..., C_n)\ ,\ C_i \subseteq \mathbf{Z}_v \qquad \cup C_i = \mathbf{Z}_v$$

$$\vec{\mathbf{B}}_2 = (D_0, D_1, ..., D_n)\ ,\ D_i \subseteq \mathbf{Z}_v \qquad \cup D_i = \mathbf{Z}_v$$

$$C_i = supp_X(i), \quad D_i = supp_Y(i)$$

Differences

$$\mathcal{B}_1 = \sum_{i=0}^{n} \Delta_v(C_i), \ \mathcal{B}_{12} = \sum_{i=0}^{n} \Delta_v(C_i, D_i)$$

Correlations

$$H(X) = \max_t \lambda_t(\mathcal{B}_1)$$

$$H(X,Y) = \max_t \lambda_t(\mathcal{B}_{12})$$

Example v=17, n+1=5

X=(4,0,0,2,1,0,1,3,3,2,2,3,3,1,0,1,2,0)
Y=(4,3,3,1,0,3,0,2,2,1,1,2,2,0,3,0,1,3)

C_0={1,13,16,4} D_0=C_3={10,11,7,6}
C_1={3,5,14,12} D_1=C_0={1,13,16,4}
C_2={9,15,8,2} D_2=C_1={3,5,14,12}
C_3={10,11,7,6} D_3=C_2={9,15,8,2}
C_4={0} D_4=C_4={0}

H(X)=3

H(X,Y)=4

Example *v=24, n+1=3*

X=(0, 1, 2, 1, 2, 2, 0, 2, 1, 2, 1, 1, 0, 2, 0, 2, 2, 1, 0, 0, 1, 1, 0, 0)
Y=(1, 2, 0, 2, 0, 0, 1, 0, 2, 0, 2, 2, 1, 0, 1, 0, 0, 2, 1, 1, 2, 2, 1, 1)

C0 ={0, 6, 12, 14, 18, 19, 22, 23},
C1 ={1, 3, 8, 10, 11, 17, 20, 21},
C2 ={2, 4, 5, 7, 9, 13, 15, 16}

H(X)=8

D0 ={2, 4, 5, 7, 9, 13, 15, 16},
D1 ={0, 6, 12, 14, 18, 19, 22, 23},
D2 ={1, 3, 8, 10, 11, 17, 20, 21}

H(Y)=8

H(X,Y)=10

Related Code

Cyclic Code and FHS

$\mathcal{X}$: a set of FH sequences of m symbols and length v, $|\mathcal{X}| = n$
$M(\mathcal{X}) = h$

$\Updownarrow$

m-ary Cyclic Code
code length: v
the number of codewords: nv
minimum distance: $v - h$

Related Code

Constant-Composition Code (CCC)

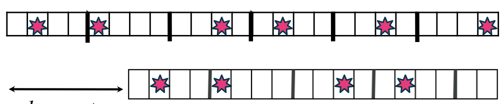
in every code word, symbol i appears exactly w_i times,

1. A cyclic CCC is a set of FH sequences

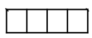
2. Actually, the most of known CCCs are cyclic.

App. 8 **Ultra Wide Band (UWB)**

Time hopping sequence X=(1,0,2,1,2,3, ...)



l=sm+t
$0 \le s < v,\ 0 \le t < m$

 frame (*m* slots)

 time slot

UWB correlation

Time hopping sequence $X=(x_0,x_1,x_2,...,x_{v-1})$
(m-ary sequence)

Binary sequence $A=(a_0,a_1.a_2,...,a_{mv-1})$

$$a_i=\begin{cases}1 & \text{if there is an integer } j \text{ such that } i=jm+x_j\\ 0 & \text{other wise.}\end{cases}$$

$$H_{XX}(l)=\sum_{k=0}^{mv-1} a_k a_{k+l}$$

see Chu and Colbourn 2004

UWB correlation (by differences)

$\vec{\mathbf{B}}_X=(C_0,C_1,...,C_{m-1}),\ C_i=supp_X(i)$
$\vec{\mathbf{B}}_Y=(D_0,D_1,...,D_{m-1}),\ D_i=supp_Y(i)$

Lemma

Let $\mathcal{B}_{XY}(t)=\sum_{i=0}^{m-1}\Delta_v(C_i,D_i')$, *where*

$$D_i'=\begin{cases}D_{m-t+i}+1 \pmod v & \text{for } 0\le i\le t-1\\ D_{i-t} & \text{for } t\le i\le m-1\end{cases}$$

then UWB correlation is

$$M_{X,Y}(l)=\lambda_s(\mathcal{B}_{XY}(t)),\ \text{where } l=sm+t$$

Maximum correlation $M(X,Y)=\max_{s,t}\lambda_s(\mathcal{B}_{XY}(t))$

Note: D_i' , $i=0,1,2...m-1,$ are not mutually disjoint

When X=Y

$$\begin{array}{ll}\Delta(C_0\ , & C_{m-t}+1)\\ \Delta(C_1\ , & C_{m-t+1}+1)\\ \vdots & \vdots\\ \Delta(C_{t-1}\ , & C_{m-1}+1)\\ \Delta(C_t\ , & C_0)\\ \vdots & \vdots\\ \Delta(C_{m-1}\ , & C_{m-t-1})\end{array}$$

t

m-t

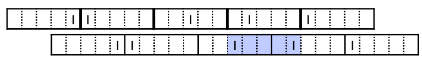
$l = s\,m + t$

Example

$v=ef+1=4\cdot4+1$

X=

4	0	2	1	0	1	3	3	2	2	3	3	1	0	1	2	0



t=3

$C_0=\{1,13,16,4\}$
$C_1=\{3,5,14,12\}$
$C_2=\{9,15,8,2\}$
$C_3=\{10,11,7,6\}$
$C_4=\{0\}$

$D'_0=C_2+1=\{10,16,9,3\}$
$D'_1=C_3+1=\{11,12,8,7\}$
$D'_2=C_4+1=\{1\}$
$D'_3=C_0=\{1,13,16,4\}$
$D'_4=C_1=\{3,5,14,12\}$

M(X,X)=5

Theorem

If there exists a partition of V

$$C_0,C_1,...,C_{m-1}$$

such that external difference of every pair of distinct subsets is perfect

$$\Delta_v(C_i,C_j)=\lambda(\mathbf{Z}_v\setminus\{0\})$$

then auto-correlation of the UWB sequence is minimum.

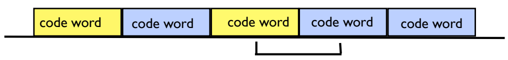
Open problem: Is there a such sets ?

New Problem

App. 9

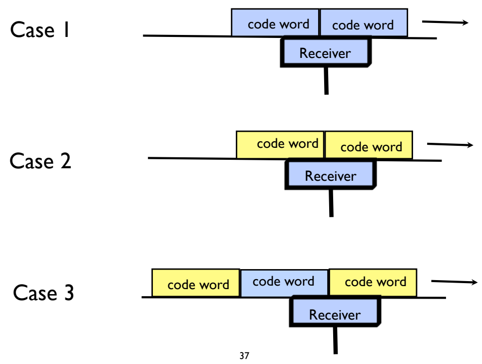
(Multi-access Comma Free Code)

Two or more codes are used on a channel



Neither of code words

3 Cases



Separator of [blue] $\mathcal{A} = (A_0, A_1, ..., A_{m-1})$

Separator of [yellow] $\mathcal{B} = (B_0, B_1, ..., B_{m-1})$

Condition 1

$\mathcal{A}$ is a $DSS(v, m, \rho_a)$

$\mathcal{B}$ is a $DSS(v, m, \rho_b)$

Condition 2

In $\sum_{i \neq j} \Delta_v(A_i, B_j)$, every element of $\mathbb{Z}_v$

appears at least $\mu (\geq 1)$ times.

($(\mathcal{A}, \mathcal{B})$ is called Mutual Difference System of Sets,

MDSS(v, m, μ))

Note: $(\mathcal{A}, \mathcal{B})$ is a MDSS(v,m,μ) <=> $(\mathcal{B}, \mathcal{A})$ is a MDSS (v,m,μ)

Let $C_i = A_i \cup (B_i + v)$

$\mathcal{C} = (C_i \mid i = 0, 1, ..., m-1)$

Condition 3

In $\sum_{i \neq j} \Delta_{2v}(C_i, A_j)$ and $\sum_{i \neq j} \Delta_{2v}(C_i, B_j)$,

every element of $\mathbb{Z}_{2v}$ appears at least σ (≥ 1) times.

($(\mathcal{C}, \mathcal{A})$ and $(\mathcal{C}, \mathcal{B})$ are MDSS($2v$, m, σ))

Example, From a Line Partition of PG(4,2)

$\mathcal{A}$ ({1, 14, 15}, {2, 28, 30}, {4, 25, 29}, {8, 19, 27}, {16, 7, 23})

$\mathcal{B}$ ({4, 25, 29}, {8, 19, 27}, {16, 7, 23}, {1, 14, 15}, {2, 28, 30})

$\mathcal{C}$ ({1, 14, 15, 35, 56, 60}, {2, 28, 30, 39, 50, 58},
{4, 25, 29, 47, 38, 54}, {8, 19, 27, 32, 45, 46},
{16, 7, 23, 33, 59, 61})

Cond. 1: $\mathcal{A}$ and $\mathcal{B}$ are DSS(31,5,6)

Cond. 2: $(\mathcal{A}, \mathcal{B})$ is an MDSS(31,5,5)

Cond. 3: $(\mathcal{C}, \mathcal{A})$ is an MDSS(62,5,4)

$(\mathcal{C}, \mathcal{B})$ is an MDSS(62,5,4)

Hints

$$\begin{aligned}
\Delta_{2v}(C_i, A_j) &= \Delta_{2v}(A_i + (B_i + v), A_j) \\
&= \Delta_{2v}(A_i, A_j) + \Delta_{2v}((B_i + v), A_j) \\
&= \Delta_{2v}(A_i, A_j) + (\Delta_{2v}(B_i, A_j) + v) \\
&= Mod(\Delta(A_i, A_j), 2v) + (\Delta(B_i, A_j) + v)
\end{aligned}$$

Δ : integer differences

Perfect difference Family: $B_1, B_2, .., B_m$

$\Delta(B_i)$: the correction of positive integer differences

If every integer from 1 to v/2 appear exactly λ times in $\sum_i \Delta(B_i)$, it is called a PDF .

(1) (13, 4, 1)-PDF:
$\{0, 1, 4, 6\} \Longrightarrow 1, 4, 3, 6, 5, 2$

(2) (49, 4, 1)-PDF:
$\{0, 5, 22, 24\} \Longrightarrow 5, 22, 17, 24, 19, 2$
$\{0, 7, 13, 23\} \Longrightarrow 7, 13, 6, 23, 16, 10$
$\{0, 3, 14, 18\} \Longrightarrow 3, 14, 11, 18, 15, 4$
$\{0, 1, 9, 21\} \Longrightarrow 1, 9, 8, 21, 20, 12$

43

Open Problem

Is there a (near) perfect difference family

$A_1 , A_2 , ..., A_m$

such that

- mutually disjoint
- their union is also a (near)PDF

44

The Intermission

休憩

45