A Big Data problem arising in Design Theory

Cyclic $(v; k_1, k_2, k_3; \lambda)$ Difference Families with Three Base Blocks

Ilias S. Kotsireas

CARGO Lab
Wilfrid Laurier University
Waterloo, ON, Canada

March 09, 2022

Summary

Introduction

Design Theory

- fundamental objects: designs
- strong interactions with other fundamental DM objects:
  codes, graphs
- applications:
  cryptography, quantum computing, telecommunications, radar
- Hadamard matrices, Hadamard conjecture
- Cyclic Difference Families
- Unsurprisingly: Big Data enters the picture!

The SDS formalism

SDS

SDS == supplementary difference sets

Consider the ring $\mathbf{Z}_v = \{0, 1, \ldots, v-1\}$ of integers modulo a positive integer v. Let $k_1, \ldots, k_t$ be positive integers and λ an integer such that

$$\lambda(v-1) = \sum_{i=1}^{t} k_i(k_i - 1), \tag{1}$$

and let $X_1, \ldots, X_t$ be subsets of $\mathbf{Z}_v$ such that $|X_i| = k_i, \quad i \in \{1, \ldots, t\}$. We say that $X_1, \ldots, X_t$ are *supplementary difference sets* (SDS) with parameters $(v; k_1, \ldots, k_t; \lambda)$, if the multiset of the union of the differences of $X_1, \cdots, X_t$ is equal to λ copies of $\{1, 2, \cdots, u-1\}$.

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v=7, k_1=k_2=k_3=3, \lambda=1, t=3$
$(7;2,2,2;1)$
$X_1=\{0,1\}, X_2=\{0,2\}, X_3=\{0,3\}$
$\{1,6\}\bigcup\{2,5\}\bigcup\{3,4\} \rightsquigarrow$
1 copy of $\{1,\ldots,6\}$

- SDSs with $t=1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t=2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t=3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v=19, \lambda=8, t=3$
$k_1=9, k_2=7, k_3=6,$
$(19;9,7,6;8)$
$X_1=\{0,1,2,3,5,7,12,13,16\}$
$X_2=\{0,1,2,4,5,10,13\}$
$X_3=\{0,1,4,6,8,13\}$
$\rightsquigarrow$
8 copies of $\{1,\ldots,18\}$

OPEN PROBLEMS:

$(167;83,76,73;107)$
$(167;79,76,74;104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

$\boxed{\text{OPEN PROBLEMS:}}$

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

SDS examples

$v = 7, k_1 = k_2 = k_3 = 3, \lambda = 1, t = 3$
$(7; 2, 2, 2; 1)$
$X_1 = \{0, 1\}, X_2 = \{0, 2\}, X_3 = \{0, 3\}$
$\{1, 6\} \bigcup \{2, 5\} \bigcup \{3, 4\} \rightsquigarrow$
1 copy of $\{1, \ldots, 6\}$

- SDSs with $t = 1$ are called cyclic difference sets, (Baumert 1971)
- SDSs with $t = 2$ are called difference families with two base blocks, (Djokovic 2011)
- SDSs with $t = 3$ are called difference families with three base blocks. v prime $p \equiv 3 \pmod 4$, (Djokovic,Kotsireas, 2016)

$v = 19, \lambda = 8, t = 3$
$k_1 = 9, k_2 = 7, k_3 = 6,$
$(19; 9, 7, 6; 8)$
$X_1 = \{0, 1, 2, 3, 5, 7, 12, 13, 16\}$
$X_2 = \{0, 1, 2, 4, 5, 10, 13\}$
$X_3 = \{0, 1, 4, 6, 8, 13\}$
$\rightsquigarrow$
8 copies of $\{1, \ldots, 18\}$

OPEN PROBLEMS:

$(167; 83, 76, 73; 107)$
$(167; 79, 76, 74; 104)$

PAF & PSD invariants

- PAF == Periodic Autocorrelation Function
- PSD == Power Spectral Density (DFT)
- For SDS $(v; k1; k2; k3; \lambda)$ with three base blocks, denote a new parameter as: $n = k_1 + k_2 + k_3 - \lambda$.
- Denote the $\{\pm 1\}$-sequences (of lengths v) associated to X_1, X_2, X_3 by A, B, C
- $$PSD(A, i) + PSD(B, i) + PSD(C, i) = 4n, i = 1, \ldots, v - 1$$
- $$PAF(A, i) + PAF(B, i) + PAF(C, i) = 3v - 4n = 1, i = 1.., v - 1$$

Computational Results

Computational Results

- D. Z. Djokovic, I. S. Kotsireas
  A class of cyclic $(v; k_1, k_2, k_3; \lambda)$ difference families with $v \equiv 3 \pmod 4$ a prime. Special Matrices 4 (2016), pp. 317-–325

- skew Hadamard matrices of orders $4 \cdot 239 = 956$ and $4 \cdot 331 = 1324$

- SDS $(v; k_1, k_2, k_3; \lambda)$ for all parameters sets with prime $v \leq 131$, $v \equiv 3 \pmod 4$.

Computational Results

how about SDS with 3 blocks for prime = 3 mod 4? say for v=23.

look for SDS(23;11,10,7;11),

n = 11+10+7-11 = 17

3 {-1/+1} sequences having

PAF = tv-4n = 3*23-4*17 = 1

and

PSD = 4n = 4*17 = 68

(23-2*11)^2 + (23-2*10)^2 + (23-2*7)^2 = a^2 +b ^2 +c ^2 = 91

and it turns out that the equation a^2 +b ^2 +c ^2 = 91

has only one solution (up to sign): 1, 3, 9

Figure: take-home toy problem

The End