代数的手法による組合せデザインの構成法について

盧 暁南 (岐阜大学)

大阪組合せ論セミナー
2025 年 10 月 31 日

自己紹介 (専門分野)

組合せデザイン理論 (本日に紹介する内容に限らず) に関して

- 組合せ論 (代数的，数論的，幾何的，...)
- 応用 (符号，暗号，統計，その他の情報学，...)
- 計算機探索

およびその周辺について，
なんでもやる，工学部に所属している数学の人間です．

「構成的」(数学的もアルゴリズム的も) アプローチが好きです．

「組合せデザイン」とは (私見)

応用の観点から

- すべての組合せを公平に登場させたい (e.g., 統計的実験計画法，暗号における認証符号)
- 最小限の回数で必要な組合せをカバーしたい (e.g., ソフトウェのテストケース生成)

数学の観点から

- 幾何学から：有限幾何学の組合せ論的一般化
- 極値集合論から：極値集合族 (e.g., Turán number 達成する hypergraph)
- グラフ理論から：完全グラフの clique 分解
- 群論から：(特殊な) 置換群の軌道
- 統計学から：準ランダムサンプリング (i.e., shadow が一様分布)

「代数的手法」について

A combinatorial object without symmetries doesn't exist – by definition.

by Gian-Carlo Rota

1. Introduction via finite geometry
2. Design of experiments and BIB designs
3. Difference sets, difference families, and cyclotomy
4. Designs with high symmetry
5. 3-designs with point-regular automorphisms

Finite affine planes

Finite projective planes (axioms)

Let P be a finite set of points and L be a finite set of lines.
The incidence structure $(P, L, \in)$ is called a finite projective plane, if the following hold:

1. Any two distinct points are joined by exactly one line.
2. Any two distinct lines meet in exactly one point.
3. There exist at least four points, no three of which are collinear.

- Each line contains $q+1$ points.
- Each point lies on $q+1$ lines.

Finite affine planes

Finite affine planes (axioms)

Let P be a finite set of points and L be a finite set of lines.
The incidence structure $(P, L, \in)$ is called a finite affine plane, if the following hold:

1. Any two distinct points are joined by exactly one line.
2. For any line and any point not on that line, there exists exactly one line passing through the point and parallel to the given line.
3. There exist at least three points, no three of which are collinear.

- Each line contains q points.
- Each point lies on $q + 1$ lines.

Generalization to Steiner systems

Steiner systems

1. Let $\mathcal{B}$ be a collection of subsets (called blocks) of a v-element set V, where each block has size k.
2. Every t-subset of V is contained in exactly one block.

The incidence structure $(V, \mathcal{B})$ is called a Steiner system $S(t, k, v)$ or a t-$(v, k, 1)$ design.

2. Equivalently, $\bigcup_{B \in \mathcal{B}} \binom{B}{t} = \binom{V}{t}$ (as multisets).

Analogy with finite geometry

- Any t (especially for $t = 2$) points uniquely determine a block.
- Each block contains the same number of points.
- Each point is contained in the same number of blocks.

Divisibility conditions for Steiner systems

Necessary (divisibility) conditions for the existence of $S(t,k,v)$

If a Steiner system $S(t,k,v)$ exists, then

$$\binom{k-i}{t-i} \,\Big|\, \binom{v-i}{t-i} \quad \text{for all } i \in \{0,1,\ldots,t-1\}.$$

- These divisibility conditions ensure that the number of blocks containing a given i-subset of points is an integer.
- The total number of blocks is $b = \dfrac{\binom{v}{t}}{\binom{k}{t}}$.
- The number of blocks incident with each point is $r = \dfrac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$.

Results on existence of Steiner systems

- $t = 2$, $k = 3$ (Steiner triple systems): divisibility conditions are sufficient. [Kirkman, 1847]
- $t = 2$, $k \in \{4, 5\}$: divisibility conditions are sufficient. [Hanani, 1961]
- $t = 2$, $6 \le k \le 10$: divisibility conditions are sufficient except for a few small values of v. [1970s–2000s]
- $t = 2$, general k, divisibility conditions are asymptotically sufficient. [Wilson, 1972–1975] (based on number-theoretic and recursive combinatorial constructions)
- $t = 3$, $k = 4$ (Steiner quadruple systems): divisibility conditions are sufficient. [Hanani, 1960]
- General (t, k), divisibility conditions are asymptotically sufficient. [Keevash, 2014+ (v1), 2024+ (v4)] (based on probabilistic methods)
- $t \ge 4$: only finitely many explicit examples are known;
  $t \ge 6$: no explicit examples are known.

Research problems in combinatorial design theory

$$\text{PG \& AG} \xrightarrow{\text{generalization}} S_1(t,k,v) \xrightarrow{\text{generalization}} S_\lambda(t,k,v) \text{ (i.e., a } t\text{-}(v,k,\lambda) \text{ design)}$$

$$\xrightarrow{\text{+ various conditions}} \text{various types of designs}$$

Main research questions:

- Existence: Under what conditions does a particular design exist (or not exist)?
- Construction: How can such designs be explicitly constructed?
- (Algebraic) properties: What kind of properties (e.g., symmetries) do they have? Existence and construction of designs with desired properties.

Construction of finite projective planes

Finite projective plane (Axioms)

1. Any two distinct points are joined by exactly one line.
2. Any two distinct lines meet in exactly one point.
3. There exist at least four points, no three of which are collinear.

1. Consider the 3-dimensional vector space $V = \mathbb{F}_q^3$ over a finite field $\mathbb{F}_q$.
2. A point corresponds to a 1-dimensional subspace of V.
   - The total number of points is $\frac{q^3-1}{q-1} = q^2 + q + 1$.
3. A line corresponds to a 2-dimensional subspace of V.
   - Each line contains $q + 1$ points.
4. This gives a finite projective plane of order q, i.e., $S(2, q+1, q^2+q+1)$ with $q^2 + q + 1$ blocks.

Construction of finite affine planes

Finite affine plane (Axioms)

1. Any two distinct points are joined by exactly one line.
2. For any line and any point not on that line, there exists exactly one line passing through the point and parallel to the given line.
3. There exist at least three points, no three of which are collinear.

1. Set of points: $\mathbb{F}_q^2 = \{(x, y) \mid x, y \in \mathbb{F}_q\}$
2. Set of lines:

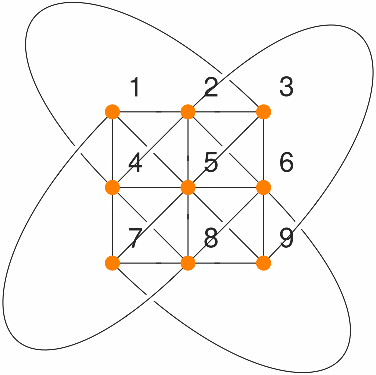
$$\begin{aligned} L_{m,b} &= \{(x, y) \in \mathbb{F}_q^2 \mid y = mx + b\} && \text{for } (m, b) \in \mathbb{F}_q^2, \\ L_a &= \{(x, y) \in \mathbb{F}_q^2 \mid x = a\} && \text{for } a \in \mathbb{F}_q. \end{aligned}$$

3. This gives a finite affine plane of order q, i.e., $S(2, q, q^2)$ with $q^2 + q$ blocks.

affine plane AG$(2, 3)$

Example: affine plane AG$(2, 3)$, i.e., $S(2, 3, 9)$

$$V = \{1, 2, \dots, 9\}, \quad \mathcal{B} = \{123, 456, 789, 147, 258, 369, 168, 249, 357, 159, 267, 348\}$$



From projective planes to affine planes

By removing the “points at infinity” and the lines containing them from the finite projective plane $\mathrm{PG}(2, q)$, we obtain the finite affine plane $\mathrm{AG}(2, q)$.

- The projective plane has $q^2 + q + 1$ points.
- Remove the $q + 1$ points at infinity (one corresponding to each class of parallel lines).
- The remaining q^2 points form the point set of the affine plane.
- Removing the $q + 1$ lines containing those points leaves $q^2 + q$ lines in total.

Existence of finite projective planes

- For every prime power q, a projective plane of order q exists.
- Bruck–Ryser Theorem (1949): If a projective plane of order n exists and $n \equiv 1, 2 \pmod 4$, then n must be a sum of two squares. (Rules out $n = 6, 14, 21, 22, \ldots$)
- $n = 10$: Nonexistence (Lam–Thiel–Swiercz, 1989; heavy computer-aided proof)
- Other non-prime-power orders: open.

Conjecture

A finite projective plane of order n exists only when n is a prime power.

Equivalently, $\exists$? $S(2, n+1, n^2+n+1)$ or $S(2, n, n^2)$ for non-prime-power $n \geq 12$?

Table: Number of finite projective planes of order n

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
#	1	1	1	1	0	1	1	4	0	≥ 1	??	≥ 1	0	??	≥ 22	≥ 1	??	≥ 1	??

1 Introduction via finite geometry

2 Design of experiments and BIB designs

3 Difference sets, difference families, and cyclotomy

4 Designs with high symmetry

5 3-designs with point-regular automorphisms

Spring balance weighing designs: Model 1

Consider a weighing problem using a spring balance (バネばかりの秤量計画)

- 7 objects

- Estimator $=$ weighing $=$ true weight $+$ error

$$\hat{x}_i = y_i = x_i + \varepsilon_i$$

for $0 \le i \le 6$.

- 7 weighings

Spring balance weighing designs: Model 2

- Three objects in each weighing

$$
\begin{aligned}
y_0 &= x_0 + x_1 + x_3 + \varepsilon_0 \\
y_1 &= x_1 + x_2 + x_4 + \varepsilon_1 \\
y_2 &= x_2 + x_3 + x_5 + \varepsilon_2 \\
y_3 &= x_3 + x_4 + x_6 + \varepsilon_3 \\
y_4 &= x_4 + x_5 + x_0 + \varepsilon_4 \\
y_5 &= x_5 + x_6 + x_1 + \varepsilon_5 \\
y_6 &= x_6 + x_0 + x_2 + \varepsilon_6
\end{aligned}
$$

- 7 weighings

Design matrices for spring balance weighing designs

- $\boldsymbol{y} = [y_0, y_1, \ldots, y_6]^\top$, $\boldsymbol{x} = [x_0, x_1, \ldots, x_6]^\top$, $\boldsymbol{\varepsilon} = [\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_6]^\top$.

- Model 1: $\boldsymbol{y} = D_1 \boldsymbol{x} + \boldsymbol{\varepsilon}$

$$D_1 = I_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Model 2: $\boldsymbol{y} = D_2 \boldsymbol{x} + \boldsymbol{\varepsilon}$

$$D_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- D_1 (resp., D_2) is called the design matrix (計画行列) of Model 1 (resp., Model 2).

Least-squares estimation for spring balance weighing

- Model 2: $\boldsymbol{y} = D_2\boldsymbol{x} + \boldsymbol{\varepsilon}$
  $\iff \quad D_2^\top \boldsymbol{y} = M_2\boldsymbol{x} + D_2^\top\boldsymbol{\varepsilon} \quad \iff \quad M_2^{-1}D_2^\top\boldsymbol{y} = \boldsymbol{x} + M_2^{-1}D_2^\top\boldsymbol{\varepsilon}$

$$M_2 = D_2^\top D_2 = \begin{bmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{bmatrix}, \quad M_2^{-1} = \frac{1}{18}\begin{bmatrix} 8 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 8 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 8 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 8 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 8 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 8 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 8 \end{bmatrix}$$

- M_2 is called the information matrix (情報行列) of D_2

Estimate and variance for spring balance weighing

- Model 2:

$$\hat{\boldsymbol{x}} = M_2^{-1} D_2^{\top} \boldsymbol{y} = \frac{1}{6} \begin{bmatrix} 2 & -1 & -1 & -1 & 2 & -1 & 2 \\ 2 & 2 & -1 & -1 & -1 & 2 & -1 \\ -1 & 2 & 2 & -1 & -1 & -1 & 2 \\ 2 & -1 & 2 & 2 & -1 & -1 & -1 \\ -1 & 2 & -1 & 2 & 2 & -1 & -1 \\ -1 & -1 & 2 & -1 & 2 & 2 & -1 \\ -1 & -1 & -1 & 2 & -1 & 2 & 2 \end{bmatrix} \boldsymbol{y}$$

- $\varepsilon_i \sim N(0, \sigma^2)$ i.i.d. for $0 \le i \le 6$.
- Model 2: $\mathrm{V}(\hat{x}_i) = \frac{4}{9}\sigma^2$
- Model 1: $\mathrm{V}(\hat{x}_i) = \sigma^2$
- Model 2 is better than Model 1
  (because Model 2 has a smaller variance of estimation error).

Set system representation of design matrix

- Index the columns (for seven objects) of D_2 by $0, 1, \ldots, 6$

$$D_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Rows (for seven weighings) of D_2 can be represented by subsets of $\{0, 1, \ldots, 6\}$

$$B_0 = \{0, 1, 3\}, B_1 = \{1, 2, 4\}, B_2 = \{2, 3, 5\},$$
$$B_3 = \{3, 4, 6\}, B_4 = \{4, 5, 0\}, B_5 = \{5, 6, 1\}, B_6 = \{6, 0, 2\}.$$

BIB designs

Balanced Incomplete Block Design

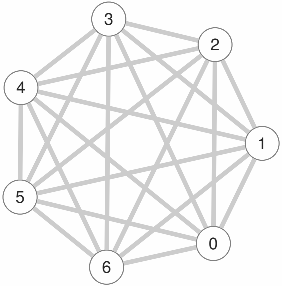
Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{B})$ is a (v, k, λ) balanced incomplete block design (釣合い型不完備ブロックデザイン; BIBD) or a 2-(v, k, λ) design, if the following hold:

1. $|V| = v$,
2. For any $B \in \mathcal{B}$, $|B| = k$.
3. For any pair of points $\{x, y\} \subseteq V$, there are exactly λ blocks $B \in \mathcal{B}$ containing $\{x, y\}$.

- v: number of elements or number of points
- k: block size
- λ: index

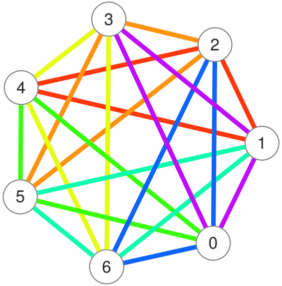
BIB designs and graph decomposition

- K_v: complete graph of order v
- $(v, k, \lambda = 1)$ BIBD $\iff$ decomposition of K_v into K_k's.
- $(v, k = 3, \lambda = 1)$ BIBD $\iff$ decomposition of K_v into triangles.



BIB designs and graph decomposition

- K_v: complete graph of order v
- $(v, k, \lambda = 1)$ BIBD $\iff$ decomposition of K_v into K_k's.
- $(v, k = 3, \lambda = 1)$ BIBD $\iff$ decomposition of K_v into triangles.



$$\{0,1,3\},\ \{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{4,5,0\},\ \{5,6,1\},\ \{6,0,2\}.$$

Fisher's inequality

Theorem (Fisher's inequality)

For a (v, k, λ) BIBD with $v > k$, the number of blocks $b \geq v$, where $b = \lambda \cdot \frac{v(v-1)}{k(k-1)}$

Symmetric BIBD

A (v, k, λ) BIBD with $b = v$ is called a symmetric design.

A projective plane of order q is a symmetric $(q^2 + q + 1, q + 1, 1)$ BIBD.

Bruck–Ryser–Chowla Theorem

Theorem (Bruck–Ryser–Chowla Theorem, 1949–1950)

If a symmetric (v, k, λ) BIBD exists, then

1. *for v even, $k - \lambda$ must be a square.*
2. *for v odd, there exists integers x, y, z with $(x, y, z) \neq (0, 0, 0)$ such that*

$$z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2.$$

BRC Theorem is a generalization of Bruck–Ryser theorem for finite projective planes.

Examples by Bruck–Ryser–Chowla theorem

$(22, 7, 2)$ SBIBD does not exist

- $r = \lambda(v-1)/(k-1) = 2 \times 21/6 = 7 \in \mathbb{Z}$, $\quad b = vr/k = 22 \times 7/7 = 22 \in \mathbb{Z}$.
- By BRC theorem, since $k - \lambda = 7 - 2 = 5$ is not a square, nonexistence.

$(43, 7, 1)$ SBIBD does not exist

- $r = \lambda(v-1)/(k-1) = 1 \times 42/6 = 7 \in \mathbb{Z}$, $\quad b = vr/k = 43 \times 7/7 = 43 \in \mathbb{Z}$.
- By BRC theorem, consider the equation $z^2 = 6x^2 - y^2$.
- By modulo 3,

$$z^2 \equiv -y^2 \equiv 2y^2 \pmod 3 \iff 2 \equiv (y^{-1}z)^2 \pmod 3 \iff \left(\frac{2}{3}\right) = 1,$$

where $(\frac{2}{3})$ is the Legendre symbol. However, 2 is not a square mod 3.

New designs from the old designs

Theorem (sum of BIBD)

If there exists a (v, k, λ_1) BIBD and a (v, k, λ_2) BIBD, then a $(v, k, \lambda_1 + \lambda_2)$ BIBD exists.

- $(V, \mathcal{B}_1)$, $(V, \mathcal{B}_2) \rightsquigarrow (V, \mathcal{B}_1 \cup \mathcal{B}_2)$

Theorem (complementation design)

A (v, b, r, k, λ) BIBD ($n \geq k + 2$) exists iff a $(v, b, b - r, v - k, b - 2r + \lambda)$ BIBD exists.

- $(V, \mathcal{B}) \rightsquigarrow (V, \overline{\mathcal{B}})$ with $\overline{\mathcal{B}} := \{V \setminus B \mid B \in \mathcal{B}\}$

Steiner triple systems

Steiner triple system; STS

A $(v, 3, 1)$ BIBD is called a Steiner triple system (STS), denoted by STS(v).

- If there exits an STS(v), then $v \equiv 1, 3 \pmod 6$.
- Bose construction (for $v \equiv 3 \pmod 6$) and Skolem construction (for $v \equiv 1 \pmod 6$) are well-known direct constructions for STS(v).

Theorem

An STS(v) exists if and only if $v \equiv 1, 3 \pmod 6$.

Cyclotomic construction for STS

Cyclotomy $\approx$ multiplicative subgroups and their cosets in $\mathbb{F}_q^*$

Theorem (Anstice, 1852–1853)

For prime $p = 6t + 1$, let α be a primitive element in $\mathbb{F}_p$ and $\omega := \alpha^{2t}$. (Then, ω is a primitive cubic root of unity in $\mathbb{F}_p^*$.) Let

$$D_i = \alpha^i \cdot \{1, \omega, \omega^2\} = \{\alpha^i, \alpha^{2t+i}, \alpha^{4t+i}\} \quad \text{and}$$
$$\mathcal{B} = \{D_i + j : 0 \le i \le t-1, j \in \mathbb{F}_p\}.$$

Then $(\mathbb{F}_p, \mathcal{B})$ is an STS(p).

Example (STS(7))

Let $p = 6t + 1 = 7$ where $t = 1$. Take $\alpha = 3$, then $D = \{1, \alpha^2, \alpha^4\} = \{1, 2, 4\}$ in $\mathbb{F}_7$.
Let $\mathcal{B} = \{D + j : j \in \mathbb{F}_7\}$. Then $(\mathbb{F}_7, \mathcal{B})$ is an STS(7).

Heffter's difference problem

difference triple

Let v be an odd integer. The triple $\{x, y, z\} \subset \{1, 2, \ldots, \frac{v-1}{2}\}$ is a difference triple if

- $x + y = z$ $(x < y < z)$, or
- $x + y + z \equiv 0 \pmod{v}$.

Moreover, $B(T) := \{0, x, x + y\}$ is called the associated base block of T.

Heffter's difference problem

For $v \equiv 1, 3 \pmod{6}$, let $t = \left\lfloor \frac{v}{6} \right\rfloor$. Let $\mathcal{T} = \{T_1, T_2, \ldots, T_t\}$ be a collection of difference triples. Then $\mathcal{T}$ is said to be a solution of Heffter's Difference Problem (HDP), denoted by HDP(v), if

- if $v \equiv 1 \pmod{6}$, $\bigcup_{i=1}^{t} T_i = [1, \frac{v-1}{2}]$;
- if $v \equiv 3 \pmod{6}$, $\bigcup_{i=1}^{t} T_i = [1, \frac{v-1}{2}] \setminus \{\frac{v}{3}\}$.

Heffter's Difference Problem $\Longleftrightarrow$ Cyclic STS

Theorem

For any $v \equiv 1, 3 \pmod 6$, *there exists a cyclic STS*(v) *iff there exists an HDP*(v).

Theorem (Pelteson, 1939)

For any $v \equiv 1, 3 \pmod 6$ *with* $v \geq 7$, $v \neq 9$, *there exists an HDP*(v).

Theorem

For any $v \equiv 1, 3 \pmod 6$ *with* $v \geq 7$, $v \neq 9$, *there exists a cyclic STS*(v).

Pairwise balanced design

Pairwise balanced design

Let K be a finite set of positive integers. Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{B})$ is a (v, K, λ) pairwise balanced design (PBD) if the all the following conditions hold.

1. $|V| = v$,
2. For any $B \in \mathcal{B}$, $|B| \in K$, where $v \geq \max K$.
3. For any pair of points $\{x, y\} \subseteq V$, there are exactly λ blocks $B \in \mathcal{B}$ containing $\{x, y\}$.

- When $K = \{k\}$, a (v, K, λ) PBD is just a (v, k, λ) BIBD.
- E.g. $(v, \{3, 5\}, 1)$ PBD $\iff$ decomposition of K_v into K_3 and K_5.

Group divisible design

Group divisible design

Let K and G be finite sets of positive integers. Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{G}, \mathcal{B})$ is a (v, G, K, λ) group divisible design (GDD) if

1. $|V| = v$,
2. $\mathcal{G} = \{V_1, V_2, \ldots, V_m\}$ $(m \geq 2)$ is a partition of V, i.e., $V_i \cap V_j = \emptyset$ and $\bigcup_{i=1}^{m} V_i = V$. The subsets V_i are called groups.
3. For any $V_i \in \mathcal{G}$, $|V_i| \in G$ where $v > \max G$.
4. For any $B \in \mathcal{B}$, $|B| \in K$, where $v \geq \max K$.
5. For any pair of points x, y from different groups, there are exactly λ blocks $B \in \mathcal{B}$ containing $\{x, y\}$.
6. For any pair of points x, y from the same group, no block contains $\{x, y\}$.

GDD and Transversal Designs

- When $G = \{1\}$, a (v, G, K, λ) GDD is just a (v, K, λ) PBD.
- When $G = \{g\}$, where $g \geq 2$, the GDD is said to be of type $g^{v/g}$.
- When $G = \{g\}$, $K = \{k\}$, a (v, G, K, λ) GDD of type g^k is a transversal design, denoted by $\mathrm{TD}(g, k, \lambda)$.

Theorem

The following are equivalent.

1. *TD$(g, k, 1)$,*
2. *OA$(N = g^2, k, g, 2)$ $(\lambda = 1)$,*
3. *$k - 2$ MOLS(g).*

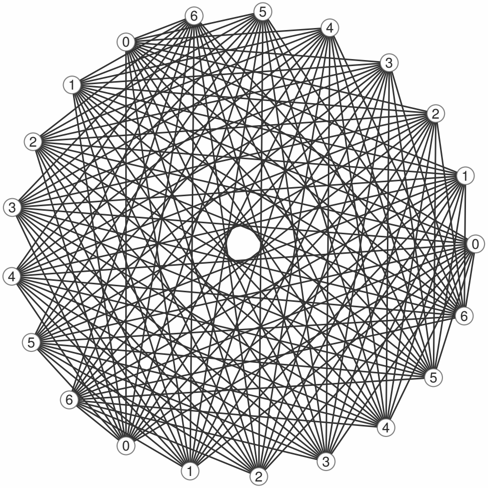
Latin square of order $n \iff$ TD$(3, n, 1)$

- $n = 7$
- $X = (x_{r,c}) =$

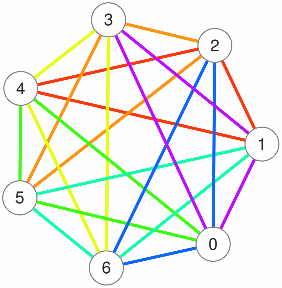
0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

- $G_{\text{row}} = \{r_1 := (r, 1) \mid 0 \le r \le n-1\}$,
  $G_{\text{col}} = \{c_2 := (c, 2) \mid 0 \le c \le n-1\}$,
  $G_{\text{ele}} = \{e_3 := (e, 3) \mid 0 \le e \le n-1\}$,
- $V = G_{\text{row}} \cup G_{\text{col}} \cup G_{\text{ele}} = \{0, 1, \dots, n-1\} \times \{1, 2, 3\}$
- $\mathcal{G} = \{G_{\text{row}}, G_{\text{col}}, G_{\text{ele}}\}$
- $\mathcal{B} = \Big\{\{r_1, c_2, e_3\} \mid 0 \le r, c \le n-1, x_{r,c} = e\Big\}$
- $(V, \mathcal{G}, \mathcal{B})$ is a TD$(3, n, 1)$.

Construct new BIBD using GDD



Complete 3-partite graph $K_{7,7,7}$



Complete graph K_7

1. Introduction via finite geometry
2. Design of experiments and BIB designs
3. Difference sets, difference families, and cyclotomy
4. Designs with high symmetry
5. 3-designs with point-regular automorphisms

Difference sets (DS)

Definition

Let $(G, +)$ be a finite abelian group of order v. A subset $D \subseteq G$ with $|D| = k$ is called a (v, k, λ) difference set if every nonzero $g \in G$ can be expressed in exactly λ ordered pairs $(x, y) \in D \times D$ such that $x - y = g$, i.e.,

$$\#\Big\{(x, y) \in D \times D : \ x - y = g\Big\} = \lambda \quad \text{for all } g \in G^*.$$

- $k(k-1) = \lambda(v-1)$.
- The family $\{D + g : \ g \in G\}$ forms a symmetric 2-(v, k, λ) design.

Definition using group-ring expression

Identify D with $D = \sum_{x \in D} x$ in $\mathbb{Z}[G]$. Then, D is a (v, k, λ) difference set iff

$$DD^{(-1)} = k \cdot 1_G + \lambda \sum_{g \in G \setminus \{0\}} g.$$

Character-sum criterion for difference sets

- $\widehat{G} = \{\chi : G \to \mathbb{C}^{\times} : \ \chi \text{ is a homomorphism}\}$.

Character-sum criterion (Turyn, 1965)

$D \subseteq G$ is a difference set in G iff, for every nontrivial character $\chi \in \widehat{G} \setminus \{1_{\mathrm{G}}\}$,

$$\left| \sum_{x \in D} \chi(x) \right|^2 = k - \lambda.$$

Paley difference sets

Paley difference sets (1933)

Let $q \equiv 3 \pmod 4$. Let $D = C_0^{(2)}$ be the set of nonzero quadratic residues in $\mathbb{F}_q^\times$.
Then, D is a $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ difference set in $G = (\mathbb{F}_q, +)$

Sketch of proof: Using the quadratic character η and the canonical additive character ψ, the sums $\sum_{x \in D} \psi(ax)$ can be expressed by $G(\eta)$ and $\eta(a)$. Since $|G(\eta)| = \sqrt{q}$ and $q \equiv 3 \pmod 4$, the character-sum criterion is satisfied.

Cyclotomy in finite fields

Cyclotomic classes

Let q be a prime power and fix a primitive element $\alpha \in \mathbb{F}_q^\times$. For $e \mid (q-1)$, define

$$C_0^{(e)} = \langle \alpha^e \rangle, \qquad C_i^{(e)} = \alpha^i C_0^{(e)} \ (i = 1, \ldots, e-1).$$

Here, $C_i^{(e)}$ is called the *i-th cyclotomic class* of index e.

- $C_0^{(2)}$ is a (Paley) DS.

Question

For which e, does the cyclotomic class $C_0^{(e)}$ form a difference set in $(\mathbb{F}_q, +)$?

Cyclotomic difference sets: known cases

Theorem (Lehmer, 1953)

Let $q = p^\ell$, where p is an odd prime. Let $e \geq 2$ be an even divisor of $q - 1$.

- $e = 2$: $C_0^{(2)}$ is a difference set iff $q \equiv 3 \pmod 4$.
- $e = 4$: $C_0^{(4)}$ is a difference set iff $q = p = 1 + 4t^2$ for some odd integer t.
- $e = 6$: $C_0^{(6)}$ is never a difference set.
- $e = 8$: $C_0^{(8)}$ is a difference set iff $q = p = 1 + 8u^2 = 9 + 64v^2$ for some odd integers u, v.

Theorem (Xia, 2018)

If $e \leq 22$ and $e \notin \{2, 4, 8\}$, then $C_0^{(e)}$ is never a difference set in $(\mathbb{F}_q, +)$.

Conjecture

$C_0^{(e)}$ is a difference set in $(\mathbb{F}_q, +)$ only when $e \notin \{2, 4, 8\}$.

Union of cyclotomic classes (1)

Difference sets from cyclotomic classes of index 6 (Hall, 1956)

Let q be an odd prime power of the form $q = 4x^2 + 27$ for some integer x.
Then $C_0^{(6)} \cup C_1^{(6)} \cup C_3^{(6)}$ is a $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ difference set in $(\mathbb{F}_q, +)$ with parameters.

Remark: There are only finitely many proper prime powers of the form $q = 4x^2 + 27$.

Union of cyclotomic classes (2)

Theorem (Feng, Xiang, 2012)

Let $p_1 \equiv 7 \pmod 8$ be a prime, $e = 2p_1^m$, and let p be a prime such that $f := \mathrm{ord}_e(p) = \frac{\varphi(e)}{2}$. Let s be an odd integer, and put $q = p^{fs}$. Let I be any subset of $\mathbb{Z}/e\mathbb{Z}$ satisfying

$$\{\, i \bmod p_1^m : \ i \in I \,\} = \mathbb{Z}/p_1^m\mathbb{Z}.$$

Define

$$D = \bigcup_{i \in I} C_i^{(e)} \subseteq \mathbb{F}_q^{\times}.$$

Then D is a skew Hadamard difference set in $(\mathbb{F}_q, +)$ whenever $p \equiv 3 \pmod 4$.

Union of cyclotomic classes (3)

Theorem (Feng, Momihara, Xiang, 2015)

Let $p_1 \equiv 3 \pmod 8$ be a prime with $p_1 \neq 3$, and let $e = 2p_1^m$. Let $p \equiv 3 \pmod 4$ be a prime such that $f := \mathrm{ord}_e(p) = \frac{\varphi(e)}{2}$. Put $q = p^f$, and define

$$J = \langle p \rangle \cup 2\langle p \rangle \cup \{0\} \pmod{2p_1},$$

and

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in J} C^{(e)}_{2i+p_1^{m-1}j}.$$

Assume that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$.
Then D is a skew Hadamard difference set in $(\mathbb{F}_q, +)$.

Character sums in cyclotomic constructions

- Additive character: $\psi_a(x) = \exp\left(\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)\right)$.
- Multiplicative character: $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$.
- Gauss sum: $G(\chi) = \sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi_1(x)$.
- Jacobi sum: $J(\chi_1,\chi_2) = \sum_{x\in\mathbb{F}_q} \chi_1(x)\chi_2(1-x)$.

Character sums over D can be expressed as linear combinations of $G(\chi)$ and $J(\chi_1,\chi_2)$. Known evaluations such as $|G(\chi)| = \sqrt{q}$ allow verifying the constant-modulus condition required for a difference set.

Singer difference sets (via finite projective geometry)

From planes to (Singer) difference sets

If a projective plane of order n admits a point-regular automorphism group G of order $v = n^2 + n + 1$ (e.g., the Desarguesian plane $\mathrm{PG}(2, q)$ via a Singer cycle), then choosing one line L and taking

$$D = \{g \in G : \ 0^g \in L\} \subseteq G$$

gives an $(n^2 + n + 1, \ n + 1, \ 1)$ difference set in G (a *Singer difference set*).

Generally, points and hyperplanes of the projective space $\mathrm{PG}(n - 1, q)$ give rise to a cyclic group $G \simeq \mathbb{Z}_{(q^n-1)/(q-1)}$, and furthermore $\left(\frac{q^n-1}{q-1}, \ \frac{q^{n-1}-1}{q-1}, \ \frac{q^{n-2}-1}{q-1}\right)$ Singer difference sets.

Difference families (DF)

Definition

Let G be a finite abelian group of order v. A collection $\mathcal{F} = \{D_1, \ldots, D_m\}$ with $D_i \subseteq G$ and $|D_i| = k$ is a (v, k, λ) difference family if

$$\sum_{i=1}^{m} \#\Big\{(x, y) \in D_i \times D_i : \ x - y = g\Big\} = \lambda \qquad \text{for all } g \in G^*.$$

- $mk(k-1) = \lambda(v-1)$.
- The family $\{D_i + g : \ 1 \le i \le m, \ g \in G\}$ forms a 2-(v, k, λ) design.

Radical difference families (via cyclotomy)

Definition

Let $q \equiv 1 \pmod{k(k-1)}$ be a prime power. A $(q, k, 1)$ difference family in $(\mathbb{F}_q, +)$ is called a radical difference family if the base blocks satisfy:

- If k is odd, each base block is a coset of the group of k-th roots of unity in $\mathbb{F}_q^\times$.
- If k is even, each base block is the union of a coset of the $(k-1)$-th roots of unity together with 0.

For odd k, let $e = (q-1)/k$. The group of k-th roots of unity is $C_0^{(e)}$.

Hence, a radical difference family can be viewed as collections of cyclotomic classes $C_i^{(e)}$.

- $k = 3$: Anstice's STS (1852, 1853)
- $k = 4, 5$: Bose (1939)

Existence for radical difference families

Radical difference families with $k = 4, 5$ (Buratti, 1995)

- Let $p = 12t + 1$ be a prime, with 2^e the largest power of 2 dividing t.
  Then a $(p, 4, 1)$ radical DF exists if and only if -3 is not a 2^{e+2}-th power in $\mathbb{F}_p$.
- Let $p = 20t + 1$ be a prime, with 2^e the largest power of 2 dividing t.
  Then a $(p, 5, 1)$ radical DF exists if and only if $\frac{11+5\sqrt{5}}{2}$ is not a 2^{e+1}-th power in $\mathbb{F}_p$.

Existence for difference families

DFs with $k = 4, 5, 6$ and prime power q (Buratti, 1995; Chen, Zhu, 1998–1999)

- A $(q, 4, 1)$ DF exists for all prime powers $q \equiv 1 \pmod{12}$.
- A $(q, 5, 1)$ DF exists for all prime powers $q \equiv 1 \pmod{20}$.
- A $(q, 6, 1)$ DF exists for all prime powers $q \equiv 1 \pmod{30}$, except for $q = 61$.

Sketch:

1. For $q > q_0(k)$, show asymptotical existence using Weil's estimation on multiplicative character sums (under complicated combinatorial conditions).
2. For $q \leq q_0(k)$, do hard works (with aid of computers).

Efforts on improving the bound q_0 (1)

A "combinatorially user-friendly" encapsulation of Weil's estimation:

Theorem (Buratti, Pasotti, 2009)

Let $q \equiv 1 \pmod{e}$ be a prime power. Let $\{b_1, b_2, \ldots, b_t\}$ be an arbitrary t-subset in $\mathbb{F}_q$. Let $(j_1, j_2, \ldots, j_t)$ be an arbitrary t-tuple of $\mathbb{Z}_e$. Set

$$X = \left\{ x \in \mathbb{F}_q : \ x - b_i \in C_{j_i}^{(e)} \text{ for each } 1 \le i \le t \right\}.$$

Then, $|X| > n$ whenever $q > Q(e, t, n)$, where

$$Q(e,t,n) = \left(\frac{U + \sqrt{U^2 + 4e^{t-1}(t+en)}}{2} \right)^2 \quad \text{and} \quad U = \sum_{h=1}^{t} \binom{t}{h} (e-1)^h (h-1).$$

In particular, X is not empty if $q > Q(e,t) := Q(e,t,0)$.

Efforts on improving the bound q_0 (2)

Improvement on Buratti–Pasotti theorem, giving better bounds of q_0 for DF with specific k.

Theorem (L., 2017)

Let $q \equiv 1 \pmod{e}$ be a prime power. Suppose $a_j, b_j \in \mathbb{F}_q^*$ and $c_j \in \mathbb{Z}_e$ for $1 \le j \le t-1$ such that $\{a_j^{-1} b_j \mid 1 \le j \le t-1\} \cup \{0\}$ is a t-subset of $\mathbb{F}_q$. Let $X = \{x \in \mathbb{F}_q \mid x$ satisfies (i) and (ii)$\}$.

1. $x \in C_i^{(e)}$ *for* $i \in \mathbb{Z}_e^\times$;
2. $a_j x + b_j \in C_{c_j i}^{(e)}$ *for* $1 \le j \le t-1$ *and* $i \in \mathbb{Z}_e^\times$.

Then $|X| > n$ whenever $q > L(e,t,n)$ ...

$$q > L(e,t,n) := \left(\frac{c_1 + \sqrt{c_1^2 + 4\varphi(e) c_0}}{2\varphi(e)} \right)^2 \quad \text{with } c_0 := (en + t - 1)e^{t-1} + e - 1 \text{ and } c_1 := \left(e - w^* + \sum_{w \mid e, \mu(\frac{e}{w}) \neq 0} (e - w) \right) \Psi,$$

where w^* is the largest divisor of e with $\mu(\frac{e}{w}) = -1$ and $\Psi := \sum_{\ell=1}^{t-1} \binom{t-1}{\ell} (e-1)^\ell \ell$.

In particular, X is not empty if $q > L(e,t) := L(e,t,0)$.

Efforts on improving the bound q_0 (3)

Table: Improved existence bounds $q_0(k)$ for $(q, k, 1)$-DFs with $3 \mid k$

k	t	e	L. (2017)	Buratti–Pasotti (2009)	Chen–Zhu (1998, 1999)
6	4	5	3.60×10^5	1.89×10^6	=L
9	7	12	1.51×10^{16}	3.76×10^{16}	4.78×10^{20}
12	10	22	4.26×10^{27}	5.15×10^{28}	4.17×10^{31}

1. Introduction via finite geometry
2. Design of experiments and BIB designs
3. Difference sets, difference families, and cyclotomy
4. Designs with high symmetry
5. 3-designs with point-regular automorphisms

Automorphisms of designs

Let G be a permutation group on a finite set V.

- G is t-transitive if it acts transitively on ordered t-subsets of V.
- G is t-homogeneous if it acts transitively on unordered t-subsets of V.

Designs from group actions (t-homogeneous $\Longrightarrow$ t−*design*)

If G acts t-homogeneously on a set V of size v, and $\mathcal{B}$ is the orbit of some k-subset under G, then $(V, \mathcal{B})$ is a t-(v, k, λ) design for some λ.

Example (Mathieu groups $\Longrightarrow$ t-designs with $t \geq 3$)

- $M_{22} \Longrightarrow$ 3-$(22, 6, 1)$ design
- M_{11} (resp., M_{23}) $\Longrightarrow$ 4-$(11, 5, 1)$ design (resp., 4-$(23, 7, 1)$ design)
- M_{12} (resp., M_{24}) $\Longrightarrow$ 5-$(12, 6, 1)$ design (resp., 5-$(24, 8, 1)$ design)

Automorphisms of designs

Let $\mathscr{D} = (V, \mathcal{B})$ be a design.

Automorphism

A bijection $g : V \to V$ is an automorphism of $\mathscr{D}$ if for every $B \in \mathcal{B}$,

$$g(B) := \left\{g(x) : x \in B\right\} \in \mathcal{B}.$$

All automorphisms form a group $\mathrm{Aut}(\mathscr{D})$ under composition.

Flags

A flag is an incident pair (x, B) with $x \in X$, $B \in \mathcal{B}$, and $x \in B$.

Transitivity

Let $G \leq \mathrm{Aut}(\mathscr{D})$.

Point-transitive

For any points $x, y \in V$, there exists $g \in G$ with $g(x) = y$.

Block-transitive

For any blocks $B_1, B_2 \in \mathcal{B}$, there exists $g \in G$ with $g(B_1) = B_2$.

Flag-transitive

For any flags (x_1, B_1) and (x_2, B_2), there exists $g \in G$ with $g(x_1) = x_2$ and $g(B_1) = B_2$.

- Flag-transitive $\Rightarrow$ point-transitive and block-transitive.
- For non-trivial 2-designs, block-transitive $\Rightarrow$ point-transitive (Block, 1965).

Automorphism groups of affine planes

Example (Affine Plane $\mathrm{AG}(2,3)$)

- Point set: $V = \mathbb{F}_3^2$
- Block set: all affine lines
- Parameters: 2-$(9,3,1)$.
- $\mathrm{Aut} \cong \mathrm{AGL}(2,3)$ of order $3^2 \cdot 48 = 432$.
  - $\mathrm{GL}(2,3) = \{A \in M_2(\mathbb{F}_3) : \det A \neq 0\}$ of order $(3^2-1)(3^2-3) = 8 \cdot 6 = 48$.
  - $\mathrm{AGL}(2,3) = V \rtimes \mathrm{GL}(2,3)$ by $x \mapsto Ax + b$ with $A \in \mathrm{GL}(2,3), b \in V$.
- Point-, block-, and flag-transitive.

Affine Planes $\mathrm{AG}(2,q)$, $q \geq 3$

- Parameters: 2-$(q^2, q, 1)$.
- $\mathrm{Aut} \cong \mathrm{A\Gamma L}(2,q)$ acts transitively on points, lines, and flags.

Automorphism groups of projective planes

Example (Fano Plane $\mathrm{PG}(2,2)$)

- Point set: 1-dimensional subspaces of $\mathbb{F}_2^3$
- Block set: 2-dimensional subspaces of $\mathbb{F}_2^3$
- Parameters: 2-$(7,3,1)$.
- $\mathrm{Aut} \cong \mathrm{PGL}(3,2)$ of order 168.
  - $\mathrm{GL}(3,2) = \{A \in M_3(\mathbb{F}_2) : \det A \neq 0\}$, $Z = \{\lambda I_3 : \lambda \in \mathbb{F}_2^\times\}$.
  - $\mathrm{PGL}(3,2) = \mathrm{GL}(3,2)/Z \cong \mathrm{GL}(3,2)$ of order $(2^3-1)(2^3-2)(2^3-2^2) = 7 \cdot 6 \cdot 4 = 168$.
- Point-, block-, and flag-transitive.

Projective Planes $\mathrm{PG}(2,q)$, $q \geq 3$

- Parameters: 2-$(q^2+q+1, q+1, 1)$.
- $\mathrm{P\Gamma L}(3,q)$ acts transitively on points, lines, and flags.

Flag-transitive t-$(v,k,1)$ designs: Classification complete

Flag-transitive 2-$(v,k,1)$ designs (BDDKLS ’90; Liebeck ’98; Saxl ’02, etc.):

- PG, AG, unitals, 1-d. affine types.

Flag-transitive 3-$(v,k,1)$ designs (Huber ’05, ’09):

- $\mathrm{AG}_2(d,2)$, 3-$(q+1,4,1)$ with $\mathrm{Aut} \cong \mathrm{PSL}(2,q)$
- 3-$(q^e+1,q+1,1)$ $(\mathrm{PGL}(2,q^e) \curvearrowright \mathbb{P}^1(\mathbb{F}_q))$
- 3-$(22,6,1)$ with $\mathrm{Aut} \cong M_{22}$ (Witt-type).

Flag-transitive t-$(v,k,1)$ designs with $t \in \{4,5\}$ (Huber ’09): only Witt designs

- 4-$(11,5,1)$ with $\mathrm{Aut} \cong M_{11}$, 4-$(23,7,1)$ with $\mathrm{Aut} \cong M_{23}$
- 5-$(12,6,1)$ with $\mathrm{Aut} \cong M_{12}$, 5-$(24,8,1)$ with $\mathrm{Aut} \cong M_{24}$

Flag-transitive 6-$(v,k,1)$ designs (Huber ’09): non-existence

Block-transitive t-$(v, k, 1)$ designs

Block-transitive t-$(v, k, 1)$ designs with $t \geq 8$ (Cameron, Praeger '93): non-existence

Block-transitive 7-$(v, k, 1)$ designs (Huber '10): non-existence

Block-transitive 6-$(v, k, 1)$ designs (Huber '08, '10): non-existence except possibly in a specific small class

Block-transitive t-$(v, k, 1)$ designs with $t \in \{4, 5\}$ (Huber '09): only Witt designs.

Block-transitive 3-$(v, k, 1)$ designs: not fully classified

Block-transitive 2-$(v, k, 1)$ designs: too many

1. Introduction via finite geometry
2. Design of experiments and BIB designs
3. Difference sets, difference families, and cyclotomy
4. Designs with high symmetry
5. 3-designs with point-regular automorphisms

Point-regular designs

Let $G \leq \mathrm{Aut}(\mathscr{D})$.

Point-regular

G is point-regular if it acts regularly (i.e., sharply transitively) on V, i.e., for any $x, y \in X$ there is a unique $g \in G$ with $g(x) = y$.

With a point-regular G, we can identify X with G

Example: Boolean Steiner Quadruple Systems

Steiner quadruple system

A 3-$(v, 4, 1)$ design is also called a Steiner quadruple system $\mathrm{SQS}(v)$.

Boolean Steiner Quadruple Systems:

- For $m \geq 3$, take $V = \mathbb{F}_2^m$.
- Let $\mathcal{B}$ be the affine 2-flats of $\mathrm{AG}(m, 2)$ (each has 4 points).
- Then $(V, \mathcal{B})$ is a 3-$(2^m, 4, 1)$ design, i.e., SQS(2^m).
- The additive group $(\mathbb{F}_2^m, +)$ is point-regular on points, so these SQSs are G-invariant with a point-regular automorphism group.

Cyclic SQS

Cyclic design

Let $V = \mathbb{Z}_v$. A design $(V, \mathcal{B})$ is cyclic if $x \mapsto x + 1 \pmod{v}$ is an automorphism, i.e. $\mathbb{Z}_v$ acts regularly by translations on points and preserves $\mathcal{B}$.

A cyclic SQS is strictly cyclic if no nontrivial translation fixes a block setwise.

- Each block orbit has full length v. Hence b is a multiple of v.
- In terms of stabilizers, $|\mathrm{Stab}_{\mathbb{Z}_v}(B)| = 1$ for all base blocks.

A cyclic SQS on $\mathbb{Z}_v$ is symmetric cyclic (aka. reversible) if inversion $x \mapsto -x$ is also an automorphism. Equivalently, the design is invariant under the dihedral group $D_{2v} = \langle x \mapsto x + 1,\ x \mapsto -x \rangle$.

Affine-invariant SQS

Affine-invariant design

Let $V = \mathbb{Z}_v$. An SQS on V is affine-invariant if

$$\mathbb{Z}_v \rtimes \mathbb{Z}_v^\times \cong \{x \mapsto ax + b : a \in \mathbb{Z}_v^\times,\ b \in \mathbb{Z}_v\}$$

acts by automorphisms.

- An affine-invariant SQS is strictly cyclic if, in addition, there exists a regular cyclic subgroup $\langle \tau \rangle \leq \mathrm{Aut}$ acting as a v-cycle on points and fixing no block setwise.
- An affine-invariant strictly cyclic SQS(v) exists only when $v \equiv 2, 10 \pmod{24}$.

Example: affine-invariant SQS(10)

Example: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$$
\begin{array}{lll}
\{0,1,5,9\}, & \{0,2,5,8\}, & \{0,1,3,4\}, \\
\{1,2,6,0\}, & \{1,3,6,9\}, & \{1,2,4,5\}, \\
\{2,3,7,1\}, & \{2,4,7,0\}, & \{2,3,5,6\}, \\
\{3,4,8,2\}, & \{3,5,8,1\}, & \{3,4,6,7\}, \\
\{4,5,9,3\}, & \{4,6,9,2\}, & \{4,5,7,8\}, \\
\{5,6,0,4\}, & \{5,7,0,3\}, & \{5,6,8,9\}, \\
\{6,7,1,5\}, & \{6,8,1,4\}, & \{6,7,9,0\}, \\
\{7,8,2,6\}, & \{7,9,2,5\}, & \{7,8,0,1\}, \\
\{8,9,3,7\}, & \{8,0,3,6\}, & \{8,9,1,2\}, \\
\{9,0,4,8\}, & \{9,1,4,7\}, & \{9,0,2,3\}.
\end{array}
$$

Example: affine-invariant SQS(10)

Example: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$+5$

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

A (strictly) cyclic SQS

Cyclic orbits

$B + c \in \mathcal{O}_{\text{cyclic}}$

Example: affine-invariant SQS(10)

Example: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

A (strictly) cyclic SQS

$\xrightarrow{+5}$

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

Cyclic orbits $\quad B + c \in \mathcal{O}_{\text{cyclic}}$

Base blocks of cyclic orbits

Example: affine-invariant SQS(10)

Example: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

+5

×3

A (strictly) cyclic SQS

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

Base blocks of cyclic orbits

An affine-invariant SQS

Affine orbits $aB + c \in \mathcal{O}_{\text{affine}}$

Example: affine-invariant SQS(10)

Example: SQS(10), $V = \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

$+5$ $\times 3$

$\{0,1,5,9\}$,	$\{0,2,5,8\}$,	$\{0,1,3,4\}$,
$\{1,2,6,0\}$,	$\{1,3,6,9\}$,	$\{1,2,4,5\}$,
$\{2,3,7,1\}$,	$\{2,4,7,0\}$,	$\{2,3,5,6\}$,
$\{3,4,8,2\}$,	$\{3,5,8,1\}$,	$\{3,4,6,7\}$,
$\{4,5,9,3\}$,	$\{4,6,9,2\}$,	$\{4,5,7,8\}$,
$\{5,6,0,4\}$,	$\{5,7,0,3\}$,	$\{5,6,8,9\}$,
$\{6,7,1,5\}$,	$\{6,8,1,4\}$,	$\{6,7,9,0\}$,
$\{7,8,2,6\}$,	$\{7,9,2,5\}$,	$\{7,8,0,1\}$,
$\{8,9,3,7\}$,	$\{8,0,3,6\}$,	$\{8,9,1,2\}$,
$\{9,0,4,8\}$,	$\{9,1,4,7\}$,	$\{9,0,2,3\}$.

A (strictly) cyclic SQS

Cyclic orbits $B + c \in \mathcal{O}_{\text{cyclic}}$

Base blocks of cyclic orbits

An affine-invariant SQS

Affine orbits $aB + c \in \mathcal{O}_{\text{affine}}$

Base blocks of affine orbits

Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathbb{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over $\mathbb{F}_p$.

Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathbb{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^{\sigma}, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Consider the following involutions on $\mathbb{P}(\mathbb{F}_p)$:

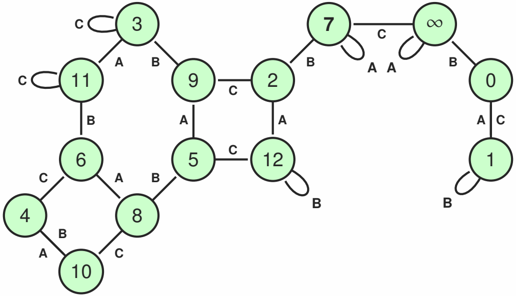
$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$

$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$

$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}.$$

For $p \equiv 1 \pmod 4$, $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

Example: $\mathrm{LG}(\mathbb{P}(\mathbb{F}_{13}))$



Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathbb{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over $\mathbb{F}_p$.

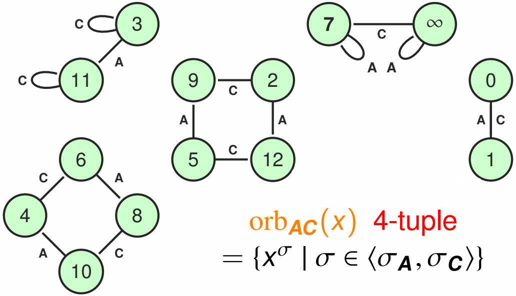
Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathbb{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^{\sigma}, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Consider the following involutions on $\mathbb{P}(\mathbb{F}_p)$:

$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$
$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$
$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}.$$

For $p \equiv 1 \pmod 4$, $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

Example: $\mathrm{LG}(\mathbb{P}(\mathbb{F}_{13}))$



$\mathrm{orb}_{\boldsymbol{AC}}(x)$ 4-tuple
$= \{x^{\sigma} \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{C}} \rangle\}$

Projective lines and graphs $\mathrm{LG}(V_p)$

$\mathbb{P}(\mathbb{F}_p) := \mathbb{F}_p \cup \{\infty\}$: the projective line over $\mathbb{F}_p$.

Let $\mathrm{LG}(V_p)$ be a graph whose vertex set is $V_p \subseteq \mathbb{P}(\mathbb{F}_p)$ and edge set is $\{\{x, y\} \mid x = y^\sigma, \sigma \in \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}\}$.

Consider the following involutions on $\mathbb{P}(\mathbb{F}_p)$:

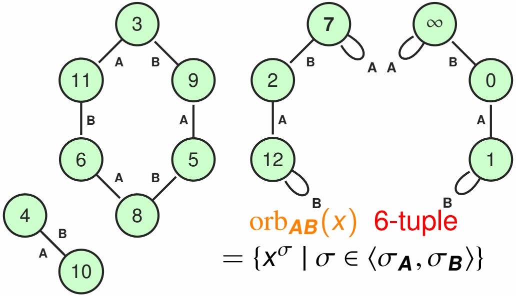
$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x,$$

$$\sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x},$$

$$\sigma_{\boldsymbol{C}} : x \mapsto \frac{x-1}{2x-1}.$$

For $p \equiv 1 \pmod 4$, $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}} \rangle = \mathrm{PSL}(2, p)$.

Example: $\mathrm{LG}(\mathbb{P}(\mathbb{F}_{13}))$

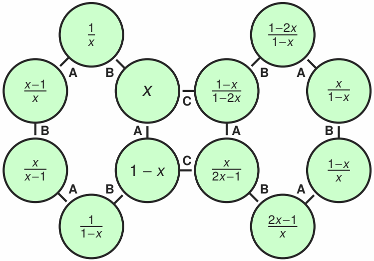


$\mathrm{orb}_{\boldsymbol{AB}}(x)$ 6-tuple

$= \{x^\sigma \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}} \rangle\}$

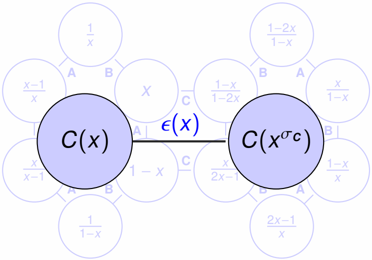
Cross-ratio classes and and graphs $\mathrm{CG}(V_p)$

- $\mathrm{orb}_{\boldsymbol{AB}}(x) = \left\{x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x\right\} =: C(x)$, a cross-ratio class.
- $\left|C(x)\right| = \begin{cases} 3 & \text{if } x \in C(0) \cup C(2) \\ 2 & \text{if } x \in C(\xi_p) \\ 6 & \text{otherwise} \end{cases}$, where ξ_p is a root of $x^2 - x + 1 = 0$.



Cross-ratio classes and and graphs $\mathrm{CG}(V_p)$

- $\mathrm{orb}_{\boldsymbol{AB}}(x) = \left\{x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x\right\} =: C(x)$, a cross-ratio class.
- $\left|C(x)\right| = \begin{cases} 3 & \text{if } x \in C(0) \cup C(2) \\ 2 & \text{if } x \in C(\xi_p) \\ 6 & \text{otherwise} \end{cases}$, where ξ_p is a root of $x^2 - x + 1 = 0$.



Let $\mathrm{CG}(V_p)$ be a graph with vertex set consisting of cross-ratio classes $\{C(x) \mid x \in V_p \subseteq \mathbb{P}(\mathbb{F}_p)\}$. Each pair of $\boldsymbol{C}$-edges in $\mathrm{LG}(V_p)$ corresponds to an edge in $\mathrm{CG}(V_p)$.

- $\Omega_p = \mathbb{P}(\mathbb{F}_p) \setminus (C(0) \cup C(2)) = \mathbb{F}_p \setminus \{0, 1, -1, 2, 2^{-1}\}$.

Existence of graph 1-factors $\Longrightarrow$ existence of SQSs

Theorem (L., Jimbo, 2017)

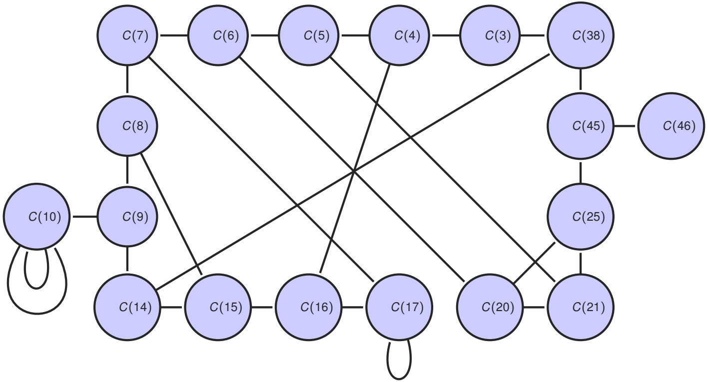
Let $q \equiv 1 \pmod 4$ be a prime. If there exists a 1-factor (perfect matching) in $\mathrm{CG}(\Omega_p)$, then there exists an affine-invariant SQS$(2p)$.

- Existence verified for all primes $p < 10^5$ with $p \equiv 1 \pmod 4$.

Theorem (L., Jimbo, 2017)

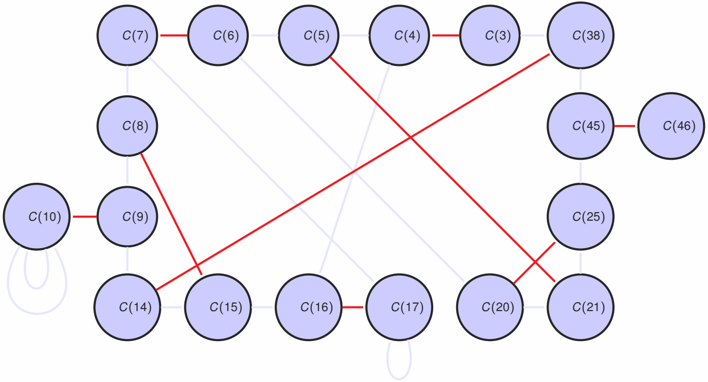
Let $q \equiv 5 \pmod{12}$ be a prime. If there exists a 1-factor (perfect matching) in $\mathrm{CG}(\Omega_p)$, then there exists an affine-invariant SQS$(2p^m)$ for all $m \geq 1$.

Example: 1-factors of $\mathrm{CG}(\Omega_p)$ with $p = 109$



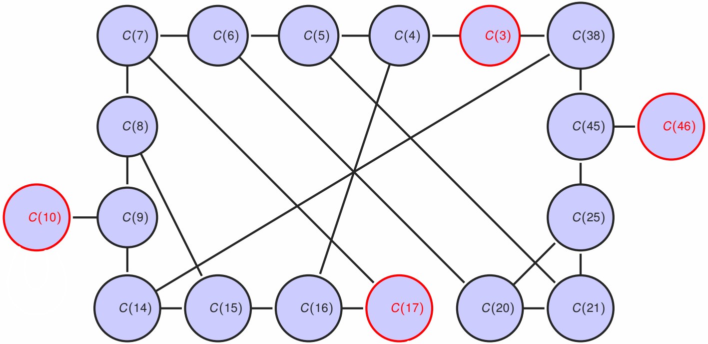
The CG graphs are essentially isomorphic to Köhler's orbit graphs (1978).

Example: 1-factors of $\mathrm{CG}(\Omega_p)$ with $p = 109$



The CG graphs are essentially isomorphic to Köhler's orbit graphs (1978).

Example: 1-factors of $\mathrm{CG}(\Omega_p)$ with $p = 109$



The CG graphs are essentially isomorphic to Köhler's orbit graphs (1978).

Abelian group-invariant SQSs (1)

Symmetric K-invariant SQS

Let K be an abelian group of order v. A Steiner quadruple system of order v (SQS(v)) $(K, \mathcal{B})$ is called symmetric K-invariant if for each $B \in \mathcal{B}$, it holds that $B + x \in \mathcal{B}$ for each $x \in K$ and $B = -B + y$ for some $y \in K$.

Theorem (Munemasa, Sawa, 2012)

Let K be an abelian group of order $v \equiv 2$ or $4 \pmod 6$. For a subset $\mathcal{B}$ of $\binom{K}{4}$ containing $\mathcal{B}_0$, the incidence structure $(K, \mathcal{B})$ is a symmetric K-invariant SQS(v) if and only if $\mathcal{B} = \mathcal{B}_0 \cup \{B \in \binom{K}{4} \colon \mathrm{orb}_{\hat{K}}(B) \in \mathcal{F}\}$ for some one-factor $\mathcal{F}$ of the Köhler graph of K.

Abelian group-invariant SQSs (2)

Theorem (Ji, L., 2021)

A symmetric K-invariant SQS(v) exists if and only if $v \equiv 2, 4 \pmod{6}$, the order of each element of K is not divisible by 8 and there exists a symmetric cyclic SQS$(2p)$ for any odd prime divisor p of v.

Proof contains:
Careful group theoretical discussions
+ Very careful discussions on the graph structures (defined on quadruple orbits)
+ Super complicated combinatorial recursive arguments
+ Some analytic number theoretical stuff for a special case...

One of the hardest part in our proof ...

Theorem (Ji, L., 2021)

Let H be a multiplicative subgroup of $\mathbb{Z}_p^*$ such that $|H| = h = (p-1)/k$ with k an absolute constant. Let $H_\omega = \omega H$ be a coset of H such that $\omega^2 \in H$. Let $I = \{a, a+b, \ldots, a+(\ell-1)b\}$ be an arithmetic progression in $\mathbb{Z}_p$ with $|I| = \ell = O(p)$. Then,

$$N := \#\{x \in \mathbb{Z}_p^* : x, x^{-1} \in H_\omega \cap I\} = \frac{\ell^2 h}{p^2} + O(\sqrt{p}\log^2 p).$$

In particular, $N > 0$ if

$$\frac{\ell^2(p+1)}{kp^2} > 2\sqrt{p}(1-\log 2+\log p)^2 + \frac{2\ell(k-1)\sqrt{p}(1-\log 2+\log p)}{kp}.$$

Summary & Insights

- A group G + a set of base blocks $\mathcal{D}$ (a relatively small collection of subsets) $\Longrightarrow$ designs.
- When group G is "strong", it becomes relatively easier to find the base blocks.
  In this case, most results heavily rely on group theory (e.g., the classification of finite simple groups).
- When the base blocks are highly structured (e.g., cyclotomy), the group tends to be a simpler one.
  In this case, the approach is more closely related to number theory.
- Finding a good balance between G and $\mathcal{D}$ is interesting but challenging.
- These methods can be applied to many problems arising from information theory and statistics.
- However, classical open problems (such as the existence of projective planes of non-prime order or cyclotomic difference sets) may require entirely new mathematical ideas.