UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE,
ZNANOST IN ŠPORT

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski socialni sklad

INTRODUCTION TO THE MINI COURSE

COMBINATORIAL DESIGNS

Mariusz Meszka
AGH University of Science and Technology, Kraków, Poland
meszka@agh.edu.pl

The roots of combinatorial design theory, date from the 18th and 19th centuries, may be found in statistical theory of experiments, geometry and recreational mathematics. Design theory rapidly developed in the second half of the twentieth century to an independent branch of combinatorics. It has deep interactions with graph theory, algebra, geometry and number theory, together with a wide range of applications in many other disciplines. Most of the problems are simple enough to explain even to non-mathematicians, yet the solutions usually involve innovative techniques as well as advanced tools and methods of other areas of mathematics. The most fundamental problems still remain unsolved.

Balanced incomplete block designs

A *design* (or *combinatorial design*, or *block design*) is a pair $(V, \mathcal{B})$ such that V is a finite set and $\mathcal{B}$ is a collection of nonempty subsets of V. Elements in V are called *points* while subsets in $\mathcal{B}$ are called *blocks*.

One of the most important classes of designs are balanced incomplete block designs.

Definition 1. A *balanced incomplete block design* (BIBD) is a pair $(V, \mathcal{B})$ where $|V| = v$ and $\mathcal{B}$ is a collection of b blocks, each of cardinality k, such that each element of V is contained in exactly r blocks and any 2-element subset of V is contained in exactly λ blocks. The numbers v, b, r, k an λ are *parameters* of the BIBD.

Since $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{\lambda v(v-1)}{k(k-1)}$ must be integers, the following are obvious arithmetic necessary conditions for the existence of a BIBD(v, b, r, k, λ):
(1) $\lambda(v-1) \equiv 0 \pmod{k-1}$,
(2) $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.
Parameter sets that satisfy (1) and (2) are called *admissible*.

The five parameters: v, b, r, k, λ are not independent; three of them: v, k and λ uniquely determine the remaining two as $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{vr}{k}$. Hence we often write (v, k, λ)-*design* (or $(v, k, \lambda) -$ BIBD) to denote a BIBD(v, b, r, k, λ).

Example 1. A $(7, 3, 1) -$ BIBD (the ”Fano plane”):
$V = \{0, 1, \ldots, 6\}$,
$\mathcal{B} = \{\{0, 1, 2\}, \{0, 3, 4\}, \{0, 5, 6\}, \{1, 3, 5\}, \{1, 3, 6\}, \{2, 3, 6\}, \{2, 4, 5\}\}$.

Example 2. A $(11, 5, 2) -$ BIBD:
$V = \{0, 1, \ldots, 10\}$,

$\mathcal{B} = \{\{0,1,2,6,9\}, \{0,1,5,8,10\}, \{0,2,3,4,8\}, \{0,3,5,6,7\}, \{0,4,7,9,10\}, \{1,2,3,7,10\}, \{1,3,4,5,9\}, \{1,4,6,7,8\}, \{2,4,5,6,10\}, \{2,5,7,8,9\}, \{3,6,8,9,10\}\}$.

A convenient way to represent a BIBD, other than a list of its blocks, is an incidence matrix. The *incidence matrix* of a $(v,k,\lambda)-\mathrm{BIBD}$ $(V,\mathcal{B})$, where $V = \{x_i : 1 \leq i \leq v\}$ and $\mathcal{B} = \{B_j : 1 \leq j \leq b\}$, is a $v \times b$ matrix $A = (a_{ij})$, in which $a_{ij} = 1$ when $x_i \in B_j$ and $a_{ij} = 0$ otherwise.

Theorem 1. *If A is an incidence matrix of a $(v,k,\lambda)-\mathrm{BIBD}$, then $AA^T = (r-\lambda)I + \lambda J$, where I is a $v \times v$ identity matrix and J is a $v \times v$ all ones matrix.*

Theorem 2 (Fisher's inequality)**.** *If a $(v,k,\lambda)-\mathrm{BIBD}$ exists with $2 \leq k < v$, then $b \geq v$.*

This result, for instance, shows that a $(21,6,1)-\mathrm{BIBD}$ cannot exist, since $b = 14 < 21 = v$, even though the above arithmetic necessary conditions are satisfied.

The *dual* of D is a design $D^* = (\mathcal{B}, V)$, where $\mathcal{B}$ corresponds to a set of elements and V to a set of blocks, such that $B \in \mathcal{B}$ is an element contained in $v \in V$ if and only if v is contained in B in D. Thus, if M is an incidence matrix of D, then M^T is an incidence matrix of D^*.

A BIBD is called *symmetric* if $v = b$ (and $r = k$).

The most fundamental necessary condition for the existence of symmetric designs is due to Bruck, Ryser and Chowla.

Theorem 3 (Bruck-Ryser-Chowla)**.** *Let v, k and λ be integers satisfying $\lambda(v-1) = k(k-1)$ and for which there exists a symmetric $(v,k,\lambda)-\mathrm{BIBD}$.*
(1) If v is even, then $n = k-\lambda$ is a square.
(2) If v is odd, then the equation $z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z not all zero.

Remark. *The dual of a* BIBD *is a* BIBD *if and only if the* BIBD *is symmetric.*

Also, the parameters of a symmetric design and its dual are the same, yet they are not necessarily isomorphic.

All necessary conditions specified above (taken together) are still not sufficient for the existence, for instance, of a symmetric $(111,111,11,11,1)-\mathrm{BIBD}$. One can easily check the set of parameters satisfies all conditions (including Fisher's inequality and Bruck-Ryser-Chowla theorem) but such design does not exist, what was proven by a detailed structural analysis combined with exhaustive computational search. The general existence question for BIBD's remains crucial open problem for infinitely many sets of parameters.

A *parallel class* in a design $(V,\mathcal{B})$ is a set of blocks that partition the set V. A *partial parallel class* is a set of blocks that contain no point of the design more than once.

Definition 2. A design $(V,\mathcal{B})$ is *resolvable* if all its blocks can be partitioned into parallel classes.

Example 3. A $(9,3,1)-\mathrm{BIBD}$ is resolvable; parallel classes are $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, $\mathcal{R}_4$:
$V = \{0,1,\ldots,9\}$,

$\mathcal{R}_1 = \{\{0,1,2\},\ \{3,4,5\},\ \{6,7,8\}\}$,
$\mathcal{R}_2 = \{\{0,3,6\},\ \{1,4,7\},\ \{2,5,8\}\}$,
$\mathcal{R}_3 = \{\{0,4,8\},\ \{1,5,6\},\ \{2,3,7\}\}$,
$\mathcal{R}_4 = \{\{0,5,7\},\ \{1,3,8\},\ \{2,4,6\}\}$.

Definition 3. Two designs, $(V_1, \mathcal{B}_1)$ and $(V_2, \mathcal{B}_2)$, are *isomorphic* if there exists a bijection $\alpha : V_1 \mapsto V_2$ such that for any $B_1 \in \mathcal{B}_1$ there exists $B_2 \in \mathcal{B}_2$, where $B_2 = \{\alpha(x_i) : x_i \in B_1\}$.

An *automorphism* is an isomorphism from a design to itself. The set of all automorphisms of a design forms a group called the *full automorphism group.* An *automorphism group* of a design is any subgroup of its full automorphism group.

Specifying an automorphism group allows sometimes to construct a design in much easier way. Then it is enough to select a set of *base* blocks which are representatives of each orbit of blocks under the prescribed automorphism group. All remaining blocks are obtained by action of the group on these base blocks.

For instance, a $(v, k, \lambda) -$ BIBD is *cyclic* if it admits a cyclic group of order v as its automorphism group.

Example 4. A cyclic $(13, 3, 1)-$BIBD has two base blocks $\{0, 1, 4\}$, $\{0, 2, 7\}$, where $V = \mathbb{Z}_{13}$ and a cyclic permutation $(0\,1\ldots 12)$ is an automorphism.

A *complement* of a design $(V, \mathcal{B})$ is a design $(V, \overline{\mathcal{B}})$, where $\overline{\mathcal{B}} = \{V \setminus B : B \in \mathcal{B}\}$. Thus a complement of a BIBD(v, b, r, k, λ) is a BIBD$(v, b, b - r, v - k, b - 2r + \lambda)$. A *supplement* of a BIBD(v, b, r, k, λ) is a BIBD obtained by taking all k-subsets which are not in $\mathcal{B}$ as blocks; in this way we get a BIBD$(v, \binom{v}{k} - b, \binom{v-1}{k-1} - r, k, \binom{v-2}{k-2} - \lambda)$.

A design $(V', \mathcal{B}')$ is a subdesign of $(V, \mathcal{B})$ if $V' \subset V$ and $\mathcal{B}' \subset \mathcal{B}$.

Given a design $D = (V, \mathcal{B})$, a *block intersection graph* $G(D)$ is a graph with the vertex set $\mathcal{B}$ and the edge set $\{\{B_i, B_j\} : B_i \cap B_j \neq \emptyset\}$. In particular, for a $(v, k, 1) -$ BIBD, $G(D)$ is strongly regular.

Exercise 1.

(1) Construct a $(6, 3, 2) -$ BIBD.

(2) Construct a $(13, 4, 1) -$ BIBD.

Exercise 2.

Find an isomorphism for the Fano plane given in Example 1 and its dual.

Exercise 3.

Prove that Fano plane is unique up to automorphism. Determine the order of its full automorphism group.

Exercise 4.

Construct a resolvable $(16, 4, 1) -$ BIBD.

Exercise 5.

Construct a cyclic $(19, 3, 1) -$ BIBD.

Exercise 6.

Given a BIBD$(v, b, r, k, 1)$, determine the parameters (i.e., order, size, degree, clique number, the number of common neighbors for each pair of adjacent vertices and for each pair of nonadjacent vertices) of its block intersection graph.

Latin squares

Definition 4. A *latin square* of *order n* (or *side n*) is an $n \times n$ array in which each cell contains a single symbol from an n-element set S, such that each symbol occurs exactly once in each row and exactly once in each column.

Definition 5. A *quasigroup* is an algebraic structure $(Q, \circ)$, where Q is a set and $\circ$ is a binary operation on Q such that the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions for every pair of elements a, b in Q. If Q is finite, then $|Q| = n$ is the *order* of the quasigroup.

A latin square can be viewed as a multiplication table of a quasigroup with the headline and sideline removed. Thus latin squares and quasigroups are equivalent combinatorial objects and we may use these two terms interchangeably.

Example 5. Latin square of order 4 and its corresponding quasigroup of order 4.

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

$\circ$	1	2	3	4
1	1	2	4	3
2	3	4	2	1
3	4	1	3	2
4	2	3	1	4

A latin square L of side n is *commutative* (or *symmetric*) if $L(i,j) = L(j,i)$ for all $1 \leq i, j \leq n$. L is *idempotent* if $L(i,i) = i$ for all $1 \leq i \leq n$. A latin square L' of even order $n = 2k$ is *half-idempotent* if $L'(i,i) = i$ and $L'(k+i, k+i) = i$ for all $1 \leq i \leq k$.

The existence of a latin square of order n is equivalent to the existence of a one-factorization of the complete bipartite graph $K_{n,n}$. Moreover, the existence of a commutative idempotent latin square of order n is equivalent to the existence of a one-factorization of the complete graph K_n.

Two latin squares, L and L', of order n are *isotopic* (or *equivalent*) if there are three bijections from the rows, columns and symbols of L to the rows, columns and symbols, respectively, of L', that map L to L'. Latin squares L and L' are *isomorphic* if there exists a bijection $\varphi : S \mapsto S$ such that $\varphi(L(i,j)) = L'(\varphi(i), \varphi(j))$ for every $i, j \in S$, where S is not only the set of symbols of each square but also the indexing set for the rows and columns of each square.

Two latin squares, L and L', of order n are *orthogonal* if the n^2 ordered pairs $(L(i,j), L'(i,j))$ are all distinct. A set of latin squares $L_1, L_2, \ldots, L_m$ is *mutually orthogonal* (or a set of MOLS(n)) if for every $1 \leq i < j \leq m$, L_i and L_j are orthogonal.

Example 6. A set of three MOLS(4):

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}$$

Let $N(n)$ denote the largest number of latin squares in a set of MOLS(n).

Remark. *For every n, $1 \leq N(n) \leq n-1$.*

Theorem 4. *If $q = p^k$ is a prime power, then $N(q) = q-1$.*

Theorem 5. *A pair of orthogonal latin squares of order n exists for all n other than 2 and 6 (for which no such pair exists).*

Construction of a pair of orthogonal latin squares of odd order n.
Let $S = \mathbb{Z}_n$. Then $L_1(i,j) = (i+j) \bmod n$ and $L_2(i,j) = (i-j) \bmod n$.

Construction of a set of n-1 MOLS of order $q = p^k$, where p is a prime.
Let $\mathbb{F}_q$ be a finite field of order q. Let $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ be elements of $\mathbb{F}_q$, where α_0 is a zero element. For each nonzero element α_r ($r \neq 0$) in $\mathbb{F}_q$, define a latin square $L_r(i,j) = \alpha_r \times \alpha_i + \alpha_j$.

Theorem 6. *The existence a set of $n-1$ MOLS(n) is equivalent to the existence of a BIBD($n^2+n+1, n^2+n+1, n+1, n+1, 1$) and a resolvable BIBD($n^2, n^2+n, n+1, n, 1$).*

Determining the value of $N(n)$ remains one of the most foremost problems in combinatorics.

Definition 6. A *partial latin square* of order n is an $n \times n$ array in which some cells are empty and some are filled with elements of S, such that each element of S appears in every row and every column at most once.

Theorem 7. *Any partial latin square of order n which has at most $n-1$ cells occupied can be completed to a latin square.*

Definition 7. A *latin rectangle* of size $m \times n$ ($m \leq n$) is an $m \times n$ array with entries from a set S of cardinality n such that every row is a permutation of S and every column contains no repetition.

Theorem 8. *If L is an $m \times n$ latin rectangle, then one can append $n-m$ further rows to L so that the resulting array in a latin square.*

Exercise 7.
(1) Find an idempotent commutative latin square of order 5.
(2) Find a half-idempotent commutative latin square of order 6.

Exercise 8.
Construct a set of two MOLS(3).

Steiner triple systems

The first class of intensively studied designs were BIBD's with block size 3 and $\lambda = 1$.

Definition 8. A *Steiner triple system*, STS(v), of order v is a $(v, 3, 1) -$ BIBD. Blocks of an STS(v) are often called *triples*.

The arithmetic necessary conditions for the existence of an STS(v) reduce to $v \equiv 1, 3 \pmod 6$. This is also a sufficient condition, what was proven in 1847 by Kirkman. One of the simplest known direct constructions is due to Bose and Skolem.

Bose construction (for STS(v) when $v \equiv 3 \pmod 6$).
Let $v = 6k + 3$ and let $(Q, \circ)$ be an idempotent commutative quasigroup of order $2k + 1$, where $Q = \{0, 1, \ldots, 2k\}$. Let $V = Q \times \{1, 2, 3\}$, and define $\mathcal{B}$ to contain the following two types of triples:
(1) for $0 \le i \le 2k$, $\{(i, 1), (i, 2), (i, 3)\} \in \mathcal{B}$
(2) for $0 \le i < j \le 2k$, $\{(i, 1), (j, 1), (i \circ j, 2)\} \in \mathcal{B}$, $\{(i, 2), (j, 2), (i \circ j, 3)\} \in \mathcal{B}$, $\{(i, 3), (j, 3), (i \circ j, 1)\} \in \mathcal{B}$.

Skolem construction (for STS(v) when $v \equiv 1 \pmod 6$).
Let $v = 6k + 1$ and let $(Q, \circ)$ be a half-idempotent commutative quasigroup of order $2k$, where $Q = \{0, 1, \ldots, 2k - 1\}$. Let $V = (Q \times \{1, 2, 3\}) \cup \{\infty\}$, and define $\mathcal{B}$ as follows:
(1) for $0 \le i \le k - 1$, $\{(i, 1), (i, 2), (i, 3)\} \in \mathcal{B}$
(1) for $0 \le i \le k - 1$, $\{\infty, (k + i, 1), (i, 2)\} \in \mathcal{B}$, $\{\infty, (k + i, 2), (i, 3)\} \in \mathcal{B}$, $\{\infty, (k + i, 3), (i, 1)\} \in \mathcal{B}$
(3) for $0 \le i < j \le 2k - 1$, $\{(i, 1), (j, 1), (i \circ j, 2)\} \in \mathcal{B}$, $\{(i, 2), (j, 2), (i \circ j, 3)\} \in \mathcal{B}$, $\{(i, 3), (j, 3), (i \circ j, 1)\} \in \mathcal{B}$.

An STS(v) is *cyclic* if it admits an automorphism which is a single cycle of length v. Then all triples may be represented by base triples, one for each orbit of triples under a cyclic automorphism. The existence of cyclic Steiner triple systems may be proved by solving two problems posed by Heffter in 1896. An ordered 3-element subset $\{a, b, c\}$ of the set $\{1, 2, \ldots, (v - 1)/2\}$ is called a *difference triple* if either $a + b = c$ or $a + b + c = v$.

Heffter's difference problems.
(1) Let $v = 6k + 1$. Is it possible to partition the set $\{1, 2, \ldots, 3k\}$ into k difference triples?
(2) Let $v = 6k + 3$. Is it possible to partition the set $\{1, 2, \ldots, 3k + 1\} \setminus \{2k + 1\}$ into k difference triples?

In 1939, Peltesohn solved both Heffter's difference problems in the affirmative except for $v = 9$ (for which no solution exists).

Example 7. A solution to the second Heffer's difference problem for $v = 27$ is:
$\{\{1, 2, 3\}, \{4, 10, 13\}, \{5, 6, 11\}, \{7, 8, 12\}\}$.
The base blocks corresponding to the difference triples are:
$\{0, 1, 3\}$, $\{0, 4, 14\}$,$\{0, 5, 11\}$,$\{0, 7, 15\}$.

Given a solution to the first Heffter's difference problem, i.e. the collection of k ordered triples, each triple $\{a, b, c\}$ forms the base triple $\{0, a_i, a_i + b_i\}$ of a cyclic STS$(6k + 1)$. Similarly, given a solution to the second Heffter's difference problem, each triple $\{a, b, c\}$ forms the base triple $\{0, a_i, a_i + b_i\}$ of a cyclic STS$(6k + 3)$; one more base triple (for *short orbit*) is $\{0, 2k + 1, 4k + 2\}$.

The number of pairwise nonisomorphic Steiner triple systems increases rapidly with v. While STS(7) and STS(9) are unique (up to isomorphism), there are two STS(13)'s, 80 STS(15)'s and $11{,}084{,}874{,}829$ STS(19)'s.

Definition 9. A *Kirkman triple system*, KTS(v), of order v is a resolvable STS(v) together with a resolution of its blocks.

Distinct resolutions of a given STS(v) may form nonisomorphic KTS's.

Example 8. KTS(15), $V = \{1, 2, \dots, 15\}$,
$\mathcal{R}_1 = \{\{1, 2, 3\}, \{4, 8, 12\}, \{5, 11, 14\}, \{6, 9, 15\}, \{7, 10, 13\}\}$,
$\mathcal{R}_2 = \{\{1, 4, 5\}, \{2, 12, 14\}, \{3, 9, 10\}, \{6, 11, 13\}, \{7, 8, 15\}\}$,
$\mathcal{R}_3 = \{\{1, 6, 7\}, \{2, 13, 15\}, \{3, 8, 11\}, \{4, 10, 14\}, \{5, 9, 12\}\}$,
$\mathcal{R}_4 = \{\{1, 8, 9\}, \{2, 4, 6\}, \{3, 13, 14\}, \{5, 10, 15\}, \{7, 11, 12\}\}$,
$\mathcal{R}_5 = \{\{1, 10, 11\}, \{2, 5, 7\}, \{3, 12, 15\}, \{4, 9, 13\}, \{6, 8, 14\}\}$,
$\mathcal{R}_6 = \{\{1, 12, 13\}, \{2, 8, 10\}, \{3, 5, 6\}, \{4, 11, 15\}, \{7, 9, 14\}\}$,
$\mathcal{R}_7 = \{\{1, 14, 15\}, \{2, 9, 11\}, \{3, 4, 7\}, \{5, 8, 13\}, \{6, 10, 12\}\}$.

The existence problem for Kirkman triple systems was completely solved by Ray-Chaudhuri and Wilson in 1971, more than 120 years after the problem was posed by Kirkman.

Theorem 9. *A Kirkman triple system of order v exists if and only if $v \equiv 3 \pmod 6$.*

Definition 10. A *Hanani triple system*, HTS(v), of order v is an STS(v) with a partition of its blocks into $(v - 1)/2$ almost parallel classes and a single partial parallel class with $(v - 1)/6$ triples.

Theorem 10. *A Hanani triple system of order v exists if and only if $v \equiv 1 \pmod 6$ and $v \notin \{7, 13\}$.*

A *partial triple system* PTS(v) is a pair $(V, \mathcal{B})$, where $|V| = v$ and $\mathcal{B}$ is a collection of 3-element subsets of V such that each unordered pair of elements of V occurs in at most one triple of $\mathcal{B}$. Let $(V, \mathcal{B})$ be a PTS(v) and $(W, \mathcal{D})$ be an STS(w) for which $V \subseteq W$ and $\mathcal{B} \subseteq \mathcal{D}$. Then $(W, \mathcal{D})$ is an *embedding* of $(V, \mathcal{B})$.

Theorem 11. *Any partial triple system* PTS(v) *can be embedded in an* STS(w) *if $w = 1, 3 \pmod 6$ and $w \geq 2v + 1$.*

Theorem 12 (Doyen-Wilson)**.** *Let $v, w \equiv 1, 3 \pmod 6$ and $v \geq 2w + 1$. Then there exists an* STS(v) *containing an* STS(w) *as a subsystem.*

Exercise 9.
Apply Skolem construction to get an STS(13).

Exercise 10.
Show that a cyclic STS(9) does not exist.

Exercise 11.
Find a solution to Heffer's difference problems when:
(1) v=19
(2) v=21.

Exercise 12.
Show that a HTS(7) does not exist.

Pairwise balanced designs and group divisible designs

Relaxing some of conditions in the definition of BIBD leads to other classes of designs. One of them considers the case when all blocks do not have to have the same size.

Definition 11. Let λ be a positive integer and K be a set of positive integers. A *pairwise balanced design*, PBD(v, K, λ), of order v with block sizes from K is a pair $(V, \mathcal{B})$ where V is a set of cardinality v and $\mathcal{B}$ is a collection of subsets of V called *blocks* such that each block $B \in \mathcal{B}$ has $|B| \in K$ and every pair of distinct elements of V occurs in exactly λ blocks.

Example 9. A PBD$(6, \{3, 4\}, 3)$:
$V = \{1, 2, 3, 4, 5, 6\}$,
$\mathcal{B} = \{\{1, 2, 3, 4\}, \{1, 3, 4, 5\}, \{1, 4, 5, 6\}, \{2, 3, 4, 6\}, \{2, 4, 5, 6\}, \{1, 2, 5\}, \{1, 2, 6\}, \{1, 3, 6\},$
$\{2, 3, 5\}, \{3, 5, 6\}\}$.

If a PBD(v, K, λ) has b_i blocks of size k_i for each $k_i \in K$, then $\lambda\binom{v}{2} = \sum_i b_i\binom{k_i}{2}$.

For a set of positive integers K, let $\alpha(K) = \gcd\{k - 1 : k \in K\}$ and $\beta(K) = \gcd\{k(k - 1) : k \in K\}$. Then the necessary consdistions for the existence of a PBD(v, K, λ) are:
(1) $\lambda(v - 1) \equiv 0 \pmod{\alpha(K)}$, and
(2) $\lambda v(v - 1) \equiv 0 \pmod{\beta(K)}$.

Remark. *Let $K \neq \{v\}$. If there exists a* PBD$(v, K, 1)$*, then $v \geq l(s - 1) + 1$, where l and s are the largest and the smallest sizes, respectively, of blocks in a* PBD*.*

Definition 12. Let K and G be sets of positive integers and λ be a positive integer. A *group divisible design* of order v and index λ, GDD(v, K, G, λ), is a triple $(V, \mathcal{B}, \mathcal{G})$ where V is a finite set of cardinality v, $\mathcal{G}$ is a partition of V into *groups* whose sizes belong to G, and $\mathcal{B}$ is a collection of subsets of V called *blocks* such that each $B \in \mathcal{B}$ has $|B| \in K$ and every pair of distinct elements of V is contained in exactly λ blocks or in one group, but not both. Moreover, $|\mathcal{G}| \geq 2$.

Given a GDD(v, K, G, λ) with a_i groups of size g_i, $i = 1, 2, \ldots, s$ (so that $\sum_{i=1}^{s} a_i g_i =$

v), we use exponential notation $g_1^{a_1}g_2^{a_2}\dots g_s^{a_s}$ for the *group type.* If $K=\{k\}$ and $\lambda=1$, then we write $k-\mathrm{GDD}$.

Example 10. A GDD$(10,\{3,4\},\{1,3\},1)$ of type 1^13^3:
$V=\{1,2,\dots,10\}$,
$\mathcal{G}=\{\{1,2,3\},\{4,5,6\},\{7,8,9\},\{10\}\}$,
$\mathcal{B}=\{\{1,4,7,10\},\{2,5,8,10\},\{3,6,9,10\},\{1,5,9\},\{2,6,7\},\{3,4,8\},\{1,6,8\},\{2,4,9\},$
$\{3,5,7\}\}$.

A GDD is *uniform* if $K=\{k\}$ and all its groups have the same size m, that is, if it is of type m^u for some positive integer u. The necessary conditions for the existence of a uniform GDD(v,k,m,λ) of type m^u are:
(1) $u\geq k$,
(2) $\lambda(u-1)m\equiv 0 \pmod{k-1}$,
(3) $\lambda u(u-1)m^2\equiv 0 \pmod{k(k-1)}$.

Definition 13. A *transversal design*, TD(k,m), is a uniform $k-\mathrm{GDD}$ of type m^k.

In other words, a GDD is a transversal design if and only if each block meets every group in exactly one point.

Theorem 13. *A transversal design* TD(k,m) *exists if and only if there exists a set of* $k-2$ MOLS(m)*. Moreover, a resolvable transversal design* TD(k,m) *exists if and only if there exists a set of* $k-1$ MOLS(m)*.*

A GDD(v,K,G,λ) may be viewed as a PBD$(v,K\cup G,\lambda)$ by considering all groups of the GDD to be blocks of the PBD, together with blocks of the GDD. Moreover, a GDD(v,K,G,λ) can be used to built a PBD$(v+1,K\cup\{g+1:\ g\in G\},\lambda)$ by adjoining a new point to each group to form new blocks. Conversely, a GDD may be obtained from a PBD by deleting a point.

Exercise 13.
(1) Construct a PBD$(10,\{3,4\},1)$.
(2) Construct a PBD$(12,\{3,4\},1)$.
(3) Construct a PBD$(11,\{3,5\},1)$.

Exercise 14.
Show that a PBD$(8,\{3,4\},1)$ does not exist.

Exercise 15.
(1) Construct a $3-\mathrm{GDD}$ of type 3^5.
(2) Construct a $4-\mathrm{GDD}$ of type 3^4.

Exercise 16.
Construct a resolvable TD$(5,7)$.

Room squares

Definition 14. Let S be a set of $n+1$ elements (*symbols*). A *Room square* of side n is an $n \times n$ array, R, that satisfies the following properties:
(1) every cell of R is either empty or contains an unordered pair of symbols from S,
(2) every symbol of S occurs exactly once in each row and exactly once in each column of R,
(3) every unordered pair of symbols occurs in precisely one cell in R.

Thus each row and each column of R contain $\frac{n-1}{2}$ empty cells.

Example 11. A room square of side 9:
$S = \{0, 1, \ldots, 9\}$,

01		49	37	28		56		
89	02				57	34		16
	58	03		69	24		17	
	36	78	04		19		25	
	79		12	05	38		46	
45					06	18	39	27
		26	59	13		07		48
67	14					29	08	35
23		15	68	47				09

Theorem 14. *A room square of side n exists if and only if n is odd and $n \notin \{3, 5\}$.*

For odd n, two 1-factorizations of the complete graph K_{n+1}, $\mathcal{F} = \{F_1, F_2, \ldots, F_n\}$ and $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ are *orthogonal* if $|F_i \cap G_i| \leq 1$ for all $1 \leq i, j \leq n$. The existence of a Room square of side n is equivalent to the existence of two orthogonal 1-factorizations of K_{n+1}.

Exercise 17.
Show that a Room square of side 5 does not exist.

Exercise 18.
Construct a Room square of side 7.

Hadamard matrices and designs

In 1893, Hadamard addressed the problem of the maximum absolute value of the determinant of an $n \times n$ complex matrix H with all its entries on a unit circle. That maximum value is $\sqrt{n^n}$. Among real matrices, this value is attained if and only if H has every entry either 1 or -1, and satisfies $HH^T = nI$. This condition means that any two distinct rows of $H(n)$ are orthogonal.

Definition 15. An $n \times n$ (± 1)-matrix $H(n)$ is a *Hadamard matrix* of side n if $HH^T = nI$.

Notice that we may multiply all entries in any row (and column) by -1 and the result is again a Hadamard matrix. By a sequence of such multiplications, a Hadamard matrix may be transformed into another Hadamard matrix, in which every entry in the first row or in the first column is 1. Such a Hadamard matrix is called *standardized*.

Example 12. $H(4)$:

$$\begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{bmatrix}$$

Necessary condition for the existence of an $H(n)$ is $n \equiv 0 \pmod 4$ or $n = 1, 2$. It is famous conjecture, stated by Hadamard in 1893, that the above condition is also sufficient. The smallest order for which the conjecture remains open is 428.

Definition 16. A *Hadamard design* is a symmetric $(4m-1, 2m-1, m-1) - \text{BIBD}$.

The existence of a Hadamard design of order $4m - 1$ is equivalent to the existence of a Hadamard matrix of side $4m$.

Example 13. $(7, 3, 1) - \text{BIBD}$ and its corresponding $H(8)$.

$$\begin{array}{|ccccccc|} \hline 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline \end{array} \qquad \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & - & + & - & - & - \\ + & - & + & + & - & + & - & - \\ + & - & - & + & + & - & + & - \\ + & - & - & - & + & + & - & + \\ + & + & - & - & - & + & + & - \\ + & - & + & - & - & - & + & + \\ + & + & - & + & - & - & - & + \end{bmatrix}$$

Exercise 19.
Construct a Hadamard matrix $H(12)$.

References

[1] C.J. Colbourn, J.H. Dinitz (eds.), *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/CRC, 2006.

[2] C.J. Colbourn, A. Rosa, *Triple Systems*, Clarendon Press, 1999.

[3] C.C. Lindner, C.A. Rodger, *Design Theory, Second Edition*, Chapman & Hall/CRC, 2009.

[4] D.R. Stinson, *Combinatorial Designs, Constructions and Analysis*, Springer, 2004.

[5] W.D. Wallis, *Introduction to Combinatorial Designs*, Chapman & Hall/CRC, 2007.