LECTURE NOTES

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 $(v, k, \lambda) - \text{BIBD}$) to denote a BIBD$(v, b, r, k, \lambda)$.

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

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

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

The necessary conditions are also sufficient for the existence of a (v,k,1)-BIBD with small k:
when $k = 2$, $v \geq 2$,
when $k = 3$, $v \equiv 1, 3 \pmod 6$,
when $k = 4$, $v \equiv 1, 4 \pmod{12}$,
when $k = 5$, $v \equiv 1, 5 \pmod{20}$.
For $k = 6$, a $(v, 6, 1)-$BIBD exists if $v \equiv 1, 6 \pmod{15}$ and $v \neq 16, 21, 36, 46;\ 51, 61, 81, 166, 226, 231, 256, 261, 286, 316, 321, 346, 351, 376, 406, 411, 436, 441, 471, 501, 561, 591, 616, 646, 651, 676, 771, 796, 801$. In the case of the orders $v = 16, 21, 36, 46$ it is proven that a $(v, 6, 1)-$BIBD does not exists, in the case of remaining 29 orders the existence problem is still unsettled.

A convenient way to represent a BIBD, other than a list of its blocks, is an incidence matrix. The *incidence matrix* of a $(v, k, \lambda) - \text{BIBD}$ $(V, \mathcal{B})$, 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.

Lemma 1. *If A is an incidence matrix of a $(v, k, \lambda) - \text{BIBD}$, 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 $(v, k, \lambda) - \text{BIBD}$ exists with $2 \leq k < v$, then $b \geq v$.*

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

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 $(v, k, \lambda) - \text{BIBD}$.*
(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.

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^*.

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 $(111, 111, 11, 11, 1) - \text{BIBD}$. 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 together with an exhaustive computational search. The general existence question for BIBD's remains crucial open problem for infinitely many sets of parameters.

Definition 2. 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. In particular, a $(v, k, \lambda) - \text{BIBD}$ is *cyclic* if it admits a cyclic group of order v as its 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.

Let G be a group of order v. A k-element subset D of G is a (v, k, λ)-*difference set* if every non-zero element of G has exactly λ representations as a difference $d - d'$ of elements d and d' from D.

Theorem 4. *A set $D = \{d_1, d_2, \ldots, d_k\}$ of k residues modulo v is a (v, k, λ)-difference set if and only if the sets $B_i = \{d_1 + i, d_2 + i, \ldots, d_k + i\} \bmod v$, $i = 0, 1, \ldots, v - 1$ form blocks of a cyclic $(v, k, \lambda) - \text{BIBD}$.*

Example 3. $\{0, 1, 3, 9\}$ is a $(13, 4, 1)$-difference set in the group $\mathbb{Z}_{13}$.
Thus $\{0, 1, 3, 9\}$ is the base block of a cyclic $(13, 4, 1) - \text{BIBD}$.

The concept of a difference set may be extended to a larger number of sets. Let G be a group of order v. A collection $\mathcal{D} = \{D_1, D_2, \ldots D_s\}$ of k-element subsets of G, where $D_i = \{d_1^i, d_2^i, \ldots d_k^i\}$, $i = 1, 2, \ldots s$, forms a (v, k, λ)-*difference family* if every non-zero element of G occurs exactly λ times as a difference $d_i^p - d_j^p$.

Theorem 5. *If a set $\mathcal{D} = \{D_1, D_2, \ldots, D_s\}$ is a (v, k, λ)-difference family over the cyclic group G, then $Orb_G(D_1) \cup Orb_G(D_2) \cup \ldots \cup Orb_G(D_s)$ is the collection of blocks of a cyclic $(v, k, \lambda) - \text{BIBD}$.*

Example 4. $\{\{0, 2, 10, 15, 19, 20\}, \{0, 3, 7, 9, 10, 16\}\}$ is a $(21, 6, 3)$-difference family in the group $\mathbb{Z}_{21}$.

Let G be a group of order $v-1$. A collection $\mathcal{D} = \{D_1, D_2, \ldots D_s\}$ of k-element subsets of $G \cup \{\infty\}$, is a *1-rotational* (v, k, λ)-*difference family* if every element of $G \setminus \{0\} \cup \{\infty, -\infty\}$ occurs exactly λ times as a difference $d_i^p - d_j^p$.

Theorem 6. *If a set $\mathcal{D} = \{D_1, D_2, \ldots, D_s\}$ is a 1-rotational (v, k, λ)-difference family over the group G, then $Orb_G(D_1) \cup Orb_G(D_2) \cup \ldots \cup Orb_G(D_s)$ is the collection of blocks of a $(v, k, \lambda) - \text{BIBD}$ admitting an automorphism group fixing one point and acting sharply transitively on the other points.*

Example 5. $\{\{0,1,3\}, \{0,1,5\}, \{0,2,5\}, \{0,4,\infty\}\}$ is a 1-rotational $(12,3,2)$-difference family.

The concept of a difference family has been generalized by Bose to form a basis of a method that is called the *method of pure and mixed differences*. Let G be an additive abelian group and let T be a t-element set. Consider the set $V = G \times T$. For any two elements $(x,i) \neq (y,j)$ of V, the differences arising from this pair may be of two kinds:
(1) if $i = j$ then $\pm(x-y)$ is a *pure* difference of class i
(2) if $i \neq j$ then $\pm(x-y)$ is a *mixed* difference of class $i\,j$.
A pure difference of any class may equal to any nonzero element of G while a mixed difference may equal to any element of G.

Suppose that there exists a collection of k-element sets $\mathcal{D} = \{D_1, D_2, \ldots, D_s\}$ such that every nonzero element of G occurs exactly λ times as a pure difference of class i for each $i \in T$, and moreover every element of G occurs exactly λ times as a mixed difference of class $i\,j$ for all $i,j \in T$, $i \neq j$. Then the sets in $\mathcal{D}$ form a *basis* of a $(v,k,\lambda) - \mathrm{BIBD}$ $(V,\mathcal{B})$, where $\mathcal{B} = \{D_i + g :\ g \in G,\ i = 1,2,\ldots s\}$.

Example 6. Let $G = \mathbb{Z}_5$ and $T = \{1,2\}$.
$\mathcal{D} = \{\{0_1, 2_1, 3_1, 3_2\}, \{0_1, 2_2, 3_2, 4_2\}, \{0_1, 1_1, 0_2, 2_2\}\}$ is a basis for a $(10,4,2) - \mathrm{BIBD}$.

Example 7. Let $G = \mathbb{Z}_3$ and $T = \{1,2,3\}$.
$\mathcal{D} = \{\{0_1, 1_1, 0_2\}, \{0_2, 1_2, 0_3\}, \{0_1, 0_3, 1_3\}, \{0_1, 1_2, 2_3\}\}$ is a basis for a $(9,3,1) - \mathrm{BIBD}$.

The above construction may be extended by adding one fixed point.

Example 8. Let $V = (\mathbb{Z}_7 \times \{1,2\}) \cup \{\infty\}$.
$\mathcal{D} = \{\{0_1, 1_1, 3_1\}, \{0_1, 0_2, 1_2\}, \{0_1, 2_2, 4_2\}, \{0_1, 3_2, 6_2\}, \{0_1, 4_2, \infty\}\}$ is a basis for a $(15,3,1)-$ BIBD.

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 $\mathrm{BIBD}(v,b,r,k,\lambda)$ is a $\mathrm{BIBD}(v,b,b-r,v-k,b-2r+\lambda)$. A *supplement* of a $\mathrm{BIBD}(v,b,r,k,\lambda)$ is a BIBD obtained by taking all k-subsets which are not in $\mathcal{B}$ as blocks; in this way we get a $\mathrm{BIBD}(v, \binom{v}{k} - b, \binom{v-1}{k-1} - r, k, \binom{v-2}{k-2} - \lambda)$.

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 $(v,k,1) - \mathrm{BIBD}$, $G(D)$ is strongly regular.

Exercise 1.
(1) Construct a $(6,3,2) - \mathrm{BIBD}$.
(2) Construct a $(13,4,1) - \mathrm{BIBD}$.
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.
Find a $(41, 5, 1)$-difference family in the group $\mathbb{Z}_{41}$.

Exercise 5.
Construct a cyclic $(21, 3, 1) - \text{BIBD}$.

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 3. 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.

The nature of symbols in S is of no importance so usually we take $S := \{1, 2, \ldots, n\}$.

Definition 4. 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 9. 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+1}.

A latin square is *reduced* (or in *standard form*) if both its first column and first row contain consecutive symbols in an increasing order.

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.

Latin squares are completely enumerated for small orders.

n	number of non-isotopic latin squares	number of reduced latin squares
2	1	1
3	1	1
4	2	4
5	2	56
6	22	9,408
7	564	16,942,080
8	1,676,267	535,281,401,856
9	115,618,721,533	377,597,570,964,258,816
10	7,580,721,483,160,132,811,489,280	
11	5,363,937,773,277,371,298,119,673,540,771,840	

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 10. A set of three MOLS(4):

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

In any latin square belonging to some set of MOLS(n), relabeling symbols does not affect to the orthogonality.

Theorem 7. *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 $L_2(i,j) = (i-j) \bmod n$.

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

Construction of a set of $q-1$ 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 $L_r(i,j) = \alpha_r \times \alpha_i + \alpha_j$.

Determining the value of $N(n)$ remains one of the most foremost problems in combinatorics. For instance, it is known that $N(n) \geq 3$ for all $n \neq 2, 3, 6$ and possibly 10.

Definition 5. 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 9. *Any partial latin square of order n which has at most $n-1$ cells occupied can be completed to a latin square.*

Deciding whether a partial latin square can be completed is an NP-complete problem, even if there are no more than 3 unfilled cells in any row or column.

Definition 6. 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 10. *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.*

Definition 7. Let a, b and n be positive integers with $a \times b = n$. Let an $n \times n$ array be partitioned into disjoint $a \times b$ *regions*. An (a,b)-*Sudoku latin square* is a latin square on the set $\{1, 2, \ldots, n\}$ where each region contains all of the symbols. An (a,b)-*Sudoku critical set* of size k is a partial latin square P with k nonempty cells that may be completed in exactly one way to an (a,b)-Sudoku latin square, but removal of any of the filled cells from P destroys the uniqueness of a completion.

Example 11. A $(3,3)$-Sudoku critical set of size 17:

4 2		1
8 1	5 9	4 7 3
3 5	4 1 8 6	2

(3,3)-Sudoku critical sets are known for all sizes from 17 to 35. For instance, the existence of a (3,3)-Sudoku critical set is still unsettled for the size 16. The number of distinct (n,n)-Sudoku latin squares for $n = 1$, 2 and 3 is 1, 288 and $6,670,903,752,021,072,936,960$, respectively. The number of inequivalent (n,n)-Sudoku latin squares for $n = 1$, 2 and 3 is 1, 2 and $5,472,730,538$, respectively.

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).

Exercise 9.
Complete a Sudoku critical set from the Example 11.

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 concerns the case when all blocks do not have to have the same size.

Definition 8. 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 size $|B| \in K$ and every pair of distinct elements of V occurs in exactly λ blocks.

Example 12. 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 conditions 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 9. 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 $g_1^{a_1} g_2^{a_2} \ldots g_s^{a_s}$ for the *group type*. If $K = \{k\}$ and $\lambda = 1$, then we write $k -$ GDD.

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

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 10. A *transversal design*, TD(k, m), is a uniform $k-$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 11. *A transversal design* TD(k, m) *exists if and only if there exists a set of* $k-2$ MOLS(m).

A GDD$(v, K, G, 1)$ may be viewed as a PBD$(v, K \cup G, 1)$ by considering all groups of the GDD to be blocks of the PBD, together with blocks of the GDD.

Lemma 12. *If there exists a group divisible design* $(V, \mathcal{B}, \mathcal{G})$ *with* $\lambda = 1$*, then there exists a pairwise balanced design* $(V, \mathcal{C})$*, where* $\mathcal{C} = \mathcal{B} \cup \{G \in \mathcal{G} : |G| \geq 2\}$.

Moreover, a GDD$(v, K, G, 1)$ can be used to built a PBD$(v+1, K \cup \{g+1 : g \in G\}, 1)$ 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.

Lemma 13. *Suppose there exists a group divisible design* $(V, \mathcal{B}, \mathcal{G})$*,* $\lambda = 1$ *and* $\infty \notin V$*. Define* $W = V \cup \{\infty\}$ *and* $\mathcal{C} = \mathcal{B} \cup \{G \cup \{\infty\} : G \in \mathcal{G}\}$*. Then* $(W, \mathcal{C})$ *is a pairwise balanced design.*

Certain transversal designs may be obtained using some recursive constructions.

TD$(4, m) \to$ TD$(4, 3m)$ **construction.**
Let $(V, \mathcal{B}, \mathcal{G})$ be a TD$(4, m)$ and let $W = \{1, 2, 3\}$. Let $V' = V \times W$ and define a collection $\mathcal{G}'$ of groups and a collection $\mathcal{B}'$ of blocks as follows:
(1) $\mathcal{G}' = \{G \times W : G \in \mathcal{G}\}$
(2) for each $B \in \mathcal{B}$, let $(B \times W, \{\{a\} \times W : a \in B\}, W(B)\}$ be a TD$(4, 3)$ and place the 9 blocks belonging to $W(B)$ in $\mathcal{B}'$.
Then $(V', \mathcal{B}', \mathcal{G}')$ is a TD$(4, 3m)$.

TD$(4, m)$ **with a parallel class** $\to$ TD$(4, 3m+1)$ **construction.**
Let $(V, \mathcal{B}, \mathcal{G})$ be a TD$(4, m)$ and let Π be a parallel class of blocks. Let $W = \{1, 2, 3\}$ and set $V_1 = \{\infty_1, \infty_2, \infty_3, \infty_4\}$. Let $V' = V \times W \cup V_1$. Define a collection $\mathcal{G}'$ of groups and a

collection $\mathcal{B}'$ of blocks as follows:
(1) $\mathcal{G}' = \{(G_i \times W) \cup \{\infty_i\} : G_i \in \mathcal{G}\}$
(2) for each block $B \in \Pi$, let $((B \times W) \cup V_1, \{(\{a\} \times W) \cup \{\infty_i\} : a \in B \cap G_i,\ i \in W\}, W(B)\}$ be a TD$(4,4)$ with a requirement that $\{\infty_1, \infty_2, \infty_3, \infty_4\}$ is a block; place 15 blocks of $W(B) \setminus \{\infty_1, \infty_2, \infty_3, \infty_4\}$ in $\mathcal{B}'$
(3) for each $B \in \mathcal{B} \setminus \Pi$, let $(B \times W, \{\{a\} \times W : a \in B\}, W(B)\}$ be a TD$(4,3)$ and place the 9 blocks belonging to $W(B)$ in $\mathcal{B}'$
(4) place $\{\infty_1, \infty_2, \infty_3, \infty_4\}$ in $\mathcal{B}'$.
Then $(V', \mathcal{B}', \mathcal{G}')$ is a TD$(4, 3m+1)$.

Exercise 10.
(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 11.
Show that a PBD$(8, \{3,4\}, 1)$ does not exist.

Exercise 12.
(1) Construct a $3-$GDD of type 3^5.
(2) Construct a $4-$GDD of type 3^4.

Exercise 13.
Construct a TD$(4, 13)$.

Steiner triple systems

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

Definition 11. 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 $0 \le i \le k-1$, $\{(i,1),(i,2),(i,3)\} \in \mathcal{B}$,
(2) 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 proven 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 14. 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 $\{0,2k+1,4k+2\}$.

Solutions to both Heffter's difference problems may be reduced to finding certain integer sequences.

A *Skolem sequence* of order n is a sequence $S = (s_1, s_2, \ldots, s_{2n})$ of $2n$ integers satisfying:
(1) for every $k \in \{1,2,\ldots,n\}$ there exist exactly two elements $s_i,\ s_j \in S$ such that $s_i = s_j = k$,
(2) if $s_i = s_j = k$ with $i < j$, then $j - i = k$.

Example 15. A Skolem sequence of order 5:
$S = (2,4,2,3,5,4,3,1,1,5)$.

A Skolem sequence of order n exists if and only if $n \equiv 0,1 \pmod 4$. Given a Skolem sequence S of order n, the collection of triples $\{\{k, n+i, n+j\} :\ s_i = s_j = k, k = 1,2,\ldots,n\}$ is a solution to the first Heffter's problem.

When $n \equiv 2,3 \pmod 4$ we use an extension of a Skolem sequence. A *hooked Skolem*

sequence of order n is a sequence $HS = (s_1, s_2, \ldots, s_{2n+1})$ of $2n+1$ integers satisfying:
(1) for every $k \in \{1, 2, \ldots, n\}$ there exist exactly two elements $s_i,\ s_j \in S$ such that $s_i = s_j = k$,
(2) if $s_i = s_j = k$ with $i < j$, then $j - i = k$,
(3) $s_{2n} = 0$.

Example 16. A hooked Skolem sequence of order 6:
$S = (6, 3, 5, 2, 3, 2, 6, 5, 4, 1, 1, 0, 4)$.

A hooked Skolem sequence of order n exists if and only if $n \equiv 2, 3 \pmod 4$. Given a hooked Skolem sequence S of order n, the collection of triples $\{\{k, n+i, n+j\} :\ s_i = s_j = k, k = 1, 2, \ldots, n\}$ is a solution to the first Heffter's problem.

Extensions of Skolem and hooked Skolem sequences, called *split* and *split hooked Skolem sequences*, with zero on the position $n+1$ and two zeros on the positions $n+1$, $2n+1$, respectively, can be used is similar way in order to obtain solutions to the second Heffter's difference problem.

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, 11,084,874,829 STS(19)'s, and 14,796,207,517,873,771 STS(21)'s.

The existence of Steiner triple systems for each admissible order $v \equiv 1, 3 \pmod 6$ may be also proven by applying two recursive constructions.

$v \to 2v+1$ **construction.**
Let $(V, \mathcal{B})$ be an STS(v) and let $(X, \mathcal{F})$ be a one-factorization of the complete graph of order $v+1$ on the set of vertices X. Let $\mathcal{C} = \{\{v_i, x, y\} :\ v_i \in V,\ \{x, y\} \in F_i \in \mathcal{F}\}$. Then $(V \cup X, \mathcal{B} \cup \mathcal{C})$ is an STS($2v+1$) with a subsystem STS(v).

The second construction uses the existence of one-factorizations in some circulant graphs, determined by Stern-Lenz Lemma.

Lemma 14. *A circulant graph $C(n; d_1, d_2, \ldots, d_s)$ has a 1-factorization if and only if $n/\gcd(d_i, n)$ is even for at least one generator d_i.*

$v \to 2v+7$ **construction.**
Let $(V, \mathcal{B})$ be an STS(v). Let $(X, \mathcal{F})$ be a collection of edge-disjoint one-factors in the complete graph K_{v+7} on the set X, and moreover let T be a set of $v+7$ triples, which together with one-factors in $\mathcal{F}$ form a partition of the edge set of K_{v+7}. Let $\mathcal{C} = \{\{v_i, x, y\} :\ v_i \in V,\ \{x, y\} \in F_i \in \mathcal{F}\}$. Then $(V \cup X, \mathcal{B} \cup \mathcal{C} \cup T)$ is an STS($2v+7$) with a subsystem STS(v).

Another well studied class of Steiner triple systems are projective triple systems. Let W_m be an $(m+1)$-dimensional vector space over $\mathbb{F}_2$. Let $\oplus$ be the operation of vector addition in W_m. Any two nonzero $(m+1)$-vectors $\mathbf{x}$ and $\mathbf{y}$ determine uniquely a third vector $\mathbf{x} \oplus \mathbf{y}$ in W_m, where addition is performed modulo 2 componentwise. Let every nonzero vector in W_{m+1} be represented by a point in a set V of cardinality $2^{m+1} - 1$.

Every two distinct points, corresponding to $\mathbf{x}$ and $\mathbf{y}$, define a unique triple formed by $\{\mathbf{x}, \mathbf{y}, \mathbf{x} \oplus \mathbf{y}\}$. The STS$(2^{m+1} - 1)$ produced in this way is called a *projective triple system* and it is often denoted by $\mathsf{PG}(m, 2)$ (just consider the triples as lines in the projective space over $\mathsf{GF}(2)$). To simplify notation, let every point in V be labeled by an integer whose binary representation is determined by the coordinates of its corresponding vector. Thus $V(\mathsf{PG}(m, 2)) = \{1, 2, \ldots, 2^{m+1} - 1\}$.

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 15. *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 16. *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 14.
Apply Skolem construction to get an STS(13).

Exercise 15.
Show that a cyclic STS(9) does not exist.

Exercise 16.
Find a solution to the Heffer's difference problems when:
(1) v=19
(2) v=21.

Exercise 17.
Construct an embedding of an STS(7) into an STS(27).

Resolvable designs

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

Example 17. A $(9, 3, 1) -$ BIBD is resolvable; parallel classes are R_1, R_2, R_3, R_4:
$V = \{0, 1, \ldots, 9\}$,
$R_1 = \{\{0, 1, 2\}, \{3, 4, 5\}, \{6, 7, 8\}\}$,
$R_2 = \{\{0, 3, 6\}, \{1, 4, 7\}, \{2, 5, 8\}\}$,
$R_3 = \{\{0, 4, 8\}, \{1, 5, 6\}, \{2, 3, 7\}\}$,
$R_4 = \{\{0, 5, 7\}, \{1, 3, 8\}, \{2, 4, 6\}\}$.

Definition 13. 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 18. KTS(15), $V = \{1, 2, \ldots, 15\}$,
$R_1 = \{\{1,2,3\}, \{4,8,12\}, \{5,11,14\}, \{6,9,15\}, \{7,10,13\}\}$,
$R_2 = \{\{1,4,5\}, \{2,12,14\}, \{3,9,10\}, \{6,11,13\}, \{7,8,15\}\}$,
$R_3 = \{\{1,6,7\}, \{2,13,15\}, \{3,8,11\}, \{4,10,14\}, \{5,9,12\}\}$,
$R_4 = \{\{1,8,9\}, \{2,4,6\}, \{3,13,14\}, \{5,10,15\}, \{7,11,12\}\}$,
$R_5 = \{\{1,10,11\}, \{2,5,7\}, \{3,12,15\}, \{4,9,13\}, \{6,8,14\}\}$,
$R_6 = \{\{1,12,13\}, \{2,8,10\}, \{3,5,6\}, \{4,11,15\}, \{7,9,14\}\}$,
$R_7 = \{\{1,14,15\}, \{2,9,11\}, \{3,4,7\}, \{5,8,13\}, \{6,10,12\}\}$.

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

A proof of sufficiency bases on two important facts:

Lemma 18. *For each $v \equiv 1 \pmod 3$, there exists a $(v, \{4,7,10,19\}, 1) - \text{PBD}$.*

Lemma 19. *If there exists a $(v, K, 1) - \text{PBD}$, $v \equiv 1 \pmod 3$, and for each $k_i \in K$ there exists a $\text{KTS}(2k_i + 1)$, then there exists a $\text{KTS}(6v + 3)$.*

Construction of a Kirkman triple system.
Let $v = 6n + 3$ and let $W = V \times \{1, 2\} \cup \{\infty\}$ where $|V| = 3n + 1$.
Let $(V, \mathcal{B})$ be a $(3n + 1, \{4, 7, 10, 19\}, 1) - \text{PBD}$.
For each block $B \in \mathcal{B}$, put on the set $B \times \{1, 2\} \cup \{\infty\}$ a copy of a $\text{KTS}(2|B| + 1)$ with a resolution $\mathcal{R}_B$ in such a way that $\{x_1, x_2, \infty\}$ is a triple for each $x \in B$.
Let R_{Bx} be a parallel class of $\mathcal{R}_B$ containing the triple $\{x_1, x_2, \infty\}$. Then $R_x = \bigcup_{B \in \mathcal{B}} R_{Bx}$ is a parallel class on W and $\mathcal{R} = \{R_x : x \in V\}$ is a resolution of a KTS(v).

The necessary conditions are also sufficient for the existence of a resolvable (v,k,1)-BIBD when k is small, namely:
if $k = 2$, $v \equiv 0 \pmod 2$,
if $k = 3$, $v \equiv 3 \pmod 6$,
if $k = 4$, $v \equiv 4 \pmod{12}$.
For $k = 5$, a resolvable $(v, 5, 1) - \text{BIBD}$ exists if $v \equiv 5 \pmod{20}$ and $v \neq 45, 345, 465, 645$, in which cases the existence problem remains open.

Theorem 20. *A resolvable transversal design $\text{TD}(k, m)$ exists if and only if there exists a set of $k - 1$ $\text{MOLS}(m)$.*

Corollary 21. *A resolvable transversal design $\text{TD}(k, m)$ exists if and only if there exists transversal design $\text{TD}(k + 1, m)$.*

When $v \equiv 1 \pmod 6$, the maximum number of pairwise disjoint triples is $\frac{v-1}{3}$. Then the maximum partial parallel class has to miss one point.

Definition 14. 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 22. *A Hanani triple system of order v exists if and only if $v \equiv 1 \pmod 6$ and $v \notin \{7, 13\}$.*

Exercise 18.
Construct a resolvable $(16, 4, 1) - $BIBD.

Exercise 19.
Construct a resolvable TD$(5, 7)$.

Exercise 20.
Show that an HTS(7) does not exist.

Other classes of designs

Affine and projective planes

A *finite incidence structure* (or *finite geometry*), $P = (\mathcal{P}, \mathcal{L}, I)$ is made of a finite set of points $\mathcal{P}$, a finite set of lines $\mathcal{L}$, and an *incidence* relation I between them.

Definition 15. A *finite affine plane* is a finite incidence structure such that the following axioms are satisfied:
(A1) any two distinct points are incident with exactly one line,
(A2) for any point P outside a line l there is exactly one line through P that has no point in common with l,
(A3) there exist three points not on a common line.

For a finite affine plane A, there is a positive integer n such that any line of A has exactly n points. This number is the *order* of A. A finite affine plane of order n has n^2 points, $n^2 + n$ lines, and $n + 1$ lines through each point.

Lemma 23. *An affine plane or order n is a* BIBD$(n^2, n^2 + n, n, n + 1, 1)$. *Conversely,* BIBD$(n^2, n^2 + n, n, n + 1, 1)$ *is an affine plane of order n.*

Remark. *An affine plane is resolvable.*

Theorem 24. An affine plane of order n exists if n is a prime power.

Construction of an affine plane of a prime power order.
Let $q = p^k$ be a prime power. Let $V = \mathbb{F}_q \times \mathbb{F}_q$.
For any $a, b \in \mathbb{F}_q$, define a line $L_{a,b} = \{(x, y) \in V : \ y = ax + b\}$.
For any $c \in \mathbb{F}_q$, define $L_{\infty,c} = \{(c, y) \in V : \ y \in \mathbb{F}_q\}$.

Finally, define $\mathcal{L} = \{L_{a,b} : a, b \in \mathbb{F}_q\} \cup \{L_{\infty,c} : c \in \mathbb{F}_q\}$.
$(V, \mathcal{L})$ is a $(q^2, q, 1) -$ BIBD.

Remark. The existence of an affine plane of order n is equivalent to the existence a set of $n-1$ MOLS(n).

Definition 16. A *finite projective plane* is a finite incidence structure such that the following axioms are satisfied:
(P1) any two distinct points are incident with exactly one line,
(P2) any two distinct lines are incident with exactly one point,
(P3) there exist four points no three of which are on the same line.

For a finite projective plane P, there is a positive integer n such that any line of P has exactly $n+1$ points. This number is the *order* of P. A finite projective plane of order n has n^2+n+1 points, n^2+n+1 lines, and $n+1$ lines through each point.

Lemma 25. *A projective plane or order n is a* BIBD$(n^2+n+1, n^2+n+1, n+1, n+1, 1)$. BIBD$(n^2+n+1, n^2+n+1, n+1, n+1, 1)$ *is a projective plane of order n.*

Remark. *A projective plane of order n exists if and only if an affine plane of order n exists.*

Exercise 21.
Construct an affine plane of order 4.

Cycle systems

Definition 17. A *k-cycle system* of order n is a pair $(X, \mathcal{C})$ where $\mathcal{C}$ is a collection of edge-disjoint k-cycles which partition the edge set of K_n with $V(K_n) = X$.

Example 19. A 4-cycle system $(X, \mathcal{C})$ of order 9:
$V = \{0, 1, \ldots, 8\}$, $\mathcal{C} = \{(0,1,5,2), (0,3,8,7), (0,4,1,8), (0,5,4,6), (1,2,6,3), (1,6,5,7), (2,3,7,4), (2,7,6,8), (3,4,8,5)\}$.

Theorem 26. *A k-cycle system of order n exists if and only if:*
(1) $n \geq k \geq 3$,
(2) *n is odd,*
(3) $2k | n(n-1)$.

A k-cycle system $(X, \mathcal{C})$ of order n is *resolvable* if the k-cycles belonging to C can be partitioned into parallel classes.

Example 20. A resolvable 5-cycle system $(X, \mathcal{C})$ of order 15:
$V = \{0, 1, \ldots, 14\}$,
$R_1 = \{(0,1,3,6,9), (2,7,8,10,13), (4,11,5,14,12)\}$,
$R_1 = \{(0,2,5,8,6), (1,12,9,7,13), (3,10,4,14,11)\}$,
$R_1 = \{(0,3,13,4,5), (1,8,2,14,9), (6,10,7,12,11)\}$,
$R_2 = \{(0,4,2,1,10), (3,7,11,9,8), (5,12,6,14,13)\}$,

$R_1 = \{(0,7,1,14,8),\ (2,6,4,3,12),\ (5,10,11,13,9)\}$,
$R_1 = \{(0,11,8,13,12),\ (1,4,7,5,6),\ (2,9,3,14,10)\}$,
$R_3 = \{(0,13,6,7,14),\ (1,5,3,2,11),\ (4,8,12,10,9)\}$.

Theorem 27. *A resolvable k-cycle system of order n exists if and only if:*
(1) $n \geq k \geq 3$,
(2) *n is odd,*
(3) $k|n$.

Theorem 28. *Let n be odd, $3 \leq m_1, m_2, \ldots, m_t \leq n$ and $m_1 + m_2 + \ldots + m_t = n(n-1)/2$. Then there exists a decomposition of K_n into t cycles of lengths $m_1, m_2, \ldots, m_t$.*

Oberwolfach Problem. *Let n be odd, $3 \leq m_1, m_2, \ldots, m_t \leq n$ and $m_1+m_2+\ldots+m_t = n$. Does the complete graph K_n have a 2-factorization in which every 2-factor consists of cycles of lengths $m_1, m_2, \ldots, m_t$?*

The Oberwolfach problem has an affirmative solution for $n \leq 100$ and every admissible collection of cycles lengths, with the exception of two cases:
(1) $m_1 = 4$, $m_2 = 5$
(2) $m_1 = m_2 = 3$, $m_3 = 5$.

Exercise 22.
Construct a 5-cycle system of order 11.

Exercise 23.
Construct a resolvable 5-cycle system of order 25.

G-DESIGNS

Definition 18. A *G-design* of order v and index λ (or *$(\lambda K_n, G)$-design*) is a G-decomposition of a complete λ-multigraph λK_n. A $(\lambda K_n, G)$-design is *balanced* if each vertex of λK_n occurs in the same number of copies of G.

Theorem 29. *There exists a $(\lambda K_n, M_k)$-design, where M_k is a matching of size k, if and only if $k \leq \lfloor \frac{n}{2} \rfloor$ and $\lambda n(n-1) \equiv 0 \pmod{2k}$.*

Theorem 30. *There exists a $(\lambda K_n, P_k)$-design if and only if $n \geq k$ and $\lambda n(n-1) \equiv 0 \pmod{(2k-2)}$.*

Example 21. A (K_6, P_4)-design:
$V = \{0,1,2,3,4,5\}$,
$\mathcal{P} = \{(0,1,2,4),\ (0,2,3,5),\ (0,3,4,1),\ (0,4,5,2),\ (0,5,1,3)\}$.

Theorem 31. *There exists a $(\lambda K_n, K_{1,k})$-design if and only if $\lambda n(n-1) \equiv 0 \pmod{2k}$ and*
(1) $n \geq 2k$ for $\lambda = 1$
(2) $n \geq k+1$ for even λ
(3) $n \geq k+1+\frac{k}{\lambda}$ for odd $\lambda \geq 3$.

Conjecture. *There exists a (K_{2n+1}, T)-design for each tree T with n edges.*

Exercise 24.
Construct a $(2K_7, K_{1,6})$-design.

t-DESIGNS

Definition 19. A $t-(v,k,\lambda)$-*design* is a pair $(V,\mathcal{B})$ where $|V| = v$ and $\mathcal{B}$ is a collection of k-element subsets of V (*blocks*) with the property that each t-element subset of V is contained in exactly λ blocks.

An ordered quadruple of positive integers (λ, t, k, v) is called *admissible* if $\lambda_s = \lambda(\binom{v-s}{t-s})/(\binom{k-s}{t-s})$ is an integer for each $0 \leq s < t$.

All known $t-(v,k,\lambda)$-designs without repeated blocks with $k > t \geq 6$ have $\lambda \geq 4$.

A *Steiner quadruple system* of order v (SQS(v)) is a $3-(v,4,1)$-design.

Example 22. A cyclic SQS(10):
$V = \mathbb{Z}_{10}$. The base blocks are: $B_1 = \{0,1,3,4\}$, $B_2 = \{0,1,2,6\}$, $B_3 = \{0,2,4,7\}$.

Theorem 32. *An* SQS(v) *exists if and only if* $v \equiv 2, 4 \pmod 6$.

Exercise 25.
Construct an SQS(8).

Directed designs

An ordered set $A = (a_1, a_2, \ldots, a_m)$ is *contained* in an ordered set $B = (b_1, b_2, \ldots, b_n)$ if $a_i = b_{l_i}$, $i = 1, 2, \ldots, m$ and $l_i < l_j$ for $i < j$.

Definition 20. A *directed* $t-(v,k,\lambda)$-*design* is a pair $(V,\mathcal{B})$ where $|V| = v$ and $\mathcal{B}$ is a collection of ordered k-subsets of V (blocks) with the property that every ordered t-subset of V is contained in exactly λ blocks.

Example 23. A directed $3-(4,4,1)$-design:
$V = \{0,1,2,3\}$, $\mathcal{B} = \{(0,1,2,3), (1,0,3,2), (2,0,3,1), (3,0,2,1),$
$(2,1,3,0), (3,1,2,0)\}$.

The *converse* of a directed design $(V,\mathcal{B})$ is a design $(V,\mathcal{B}^{-1})$ where $\mathcal{B}^{-1} = \{(a_k, a_{k-1}, \ldots, a_1) : (a_1, a_2, \ldots, a_k) \in \mathcal{B}\}$. A directed design is *self-converse* if it is isomorphic to its converse.

The corresponding t-design of a directed design is its *underlying* design.

Exercise 26.
Construct a directed $2-(7,4,1)$-design.

Room squares

Definition 21. 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 24. 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 33. *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 27.
Show that a Room square of side 5 does not exist.

Exercise 28.
Construct a Room square of side 7.

Howell designs

Definition 22. Let S be a set of $2n$ symbols. A *Howell design* $H(s, 2n)$ on the symbol set S is an $s \times s$ array that satisfies the following conditions:
(1) every cell 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 H,
(3) every unordered pair of symbols occurs in at most one cell of H.

Example 25. A Howell design $H(6,8)$:
$S = \{0, 1, \ldots, 7\}$,

02	57	13			46
47	03	56			12
15		04	26	37	
36		27	05	14	
	24		17	06	35
	16		34	25	07

Necessary condition for the existence of Howell designs $H(s, 2n)$ is $n \leq s \leq 2n-1$. A pair of mutually orthogonal latin squares of side n corresponds to a Howell design $H(n, 2n)$. Though a pair of orthogonal latin squares of side 6 does not exist, a Howell design $H(6, 12)$ can be constructed in different way. There in no $H(2, 4)$. In the other extreme case, an $H(2n-1, 2n)$ is a Room square of side $2n-1$. The existence of Howell designs has been completely determined for all remaining values of s.

Theorem 34. *If $n < s < 2n-1$ then there exists an $H(s, 2n)$, except that $H(5, 8)$ does not exist.*

In general, a pair of orthogonal one-factorizations of an s-regular graph G on $2n$ vertices corresponds to the existence of a Howell design of type $(s, 2n)$, for which a graph G is called an *underlying graph*. An important question related to Howell designs concerns properties of graphs which are underlying graphs of Howell designs. While for $s = 2n-1$ and $s = 2n-2$ these graphs are unique (the complete graph K_{2n} and the cocktail party graph $K_{2n} \setminus F$, respectively, where F is a one-factor), determining these graphs in general seems to be hopeless.

An efficient tool to construct Howell designs for some classes of parameters is the starter-adder construction. Let G be an abelian group of order s. A *Howell starter* in G, where $s+1 \leq 2n \leq 2s$, is a set $S_{s,n} = \{\{x_i, y_i\} : 1 \leq i \leq s-n\} \cup \{\{x_i\} : s-n+1 \leq i \leq n\}$ that satisfies:
(1) $\{x_i : 1 \leq i \leq n\} \cup \{y_i : 1 \leq i \leq s-n\} = G$,
(2) $(x_i - y_i) \neq \pm(x_j - y_j)$ if $i \neq j$.
If $S_{s,n}$ is a Howell starter, then an ordered set $A_{s,n} = \{\{a_i\} : 1 \leq i \leq n\}$ is an *adder* for $S_{s,n}$ if elements in $A_{s,n}$ are distinct and $\{x_i + a_i : 1 \leq i \leq n\} \cup \{y_i + a_i : 1 \leq i \leq s-n\} = G$.

Exercise 29.
Construct a Howell design $H(4, 6)$.

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 23. 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 26. $H(4)$:

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

Necessary condition for the existence of an $H(n)$ is $n \equiv 0 \pmod 4$ or $n = 1, 2$. The famous conjecture, stated by Hadamard in 1893, claims that the above condition is also sufficient. The smallest order for which the conjecture remains open is 668.

Definition 24. A *Hadamard design* is a symmetric $(4m-1, 2m-1, m-1) -$ BIBD.

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

Example 27. $(7, 3, 1) -$ BIBD and its corresponding $H(8)$.

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

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

Exercise 30.
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.