COMBINATORIAL DESIGNS

dr hab. Mariusz Meszka

Akademia Górniczo-Hutnicza w Krakowie

http://home.agh.edu.pl/∼meszka

Overwiev

1. Latin squares and quasigroups – existence and constructions.
2. Latin squares and rectangles – embeddings, connections to other combinatorial objects, Sudoku squares.
3. Steiner triple systems. Necessary and sufficient conditions for the existence.
4. STS – constructions and properties.
5. Balanced incomplete block designs – examples, necessary numerical conditions, Fischer's inequality.
6. BIBD – basic constructions. Resolvable designs.
7. Pairwise balanced designs – examples and constructions.

Overwiev (cont.)

8. Group divisible designs and transversal designs – examples and constructions.
9. Resolvable designs. Kirkman triple systems – existence and constructions.
10. Affine and projective planes.
11. G-designs, k-cycle systems.
12. t –designs – existence and examples.
13. Directed designs – examples and constructions.
14. Room squares, Howell designs.
15. Hadamard matrices.

References

[1] C.J. Colbourn, J.H. Dinitz (eds.), *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/CRC, 2006.
[2] C.C. Lindner, C.A. Rodger, *Design Theory, Second Edition*, Chapman & Hall/CRC, 2009.
[3] D.R. Stinson, *Combinatorial Designs, Constructions and Analysis*, Springer, 2004.
[4] W.D. Wallis, *Introduction to Combinatorial Designs*, Chapman & Hall/CRC, 2007.
[5] C.J. Colbourn, A. Rosa, *Triple Systems*, Clarendon Press, 1999.

Definition

A *field* is an algebraic structure $(\mathbb{F}, \oplus, \otimes)$ which satisfies the following axioms:

(1) $\forall a, b \in \mathbb{F}$: $a \oplus b \in \mathbb{F}$ and $a \otimes b \in \mathbb{F}$

(2) $\forall a, b, c \in \mathbb{F}$: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ and
$a \otimes (b \otimes c) = (a \otimes b) \otimes c$

(3) $\forall a, b \in \mathbb{F}$: $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$

(4) $\exists 0 \in \mathbb{F}\ \forall a \in \mathbb{F}$: $a \oplus 0 = 0 \oplus a = a$
$\exists 1 \in \mathbb{F}\ \forall a \in \mathbb{F}$: $a \otimes 1 = 1 \otimes a = a$

(5) $\forall a \in \mathbb{F}\ \exists -a \in \mathbb{F}$: $a \oplus -a = -a \oplus a = 0$
$\forall a \in \mathbb{F}$: $a \neq 0\ \exists a^{-1} \in \mathbb{F}$: $a \otimes a^{-1} = a^{-1} \otimes a = 1$

(6) $\forall a, b, c \in \mathbb{F}$: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Lemma

Let n be an integer, $n \geq 2$, and let $a \in \mathbb{Z}_n$, $a \neq 0$. Then a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.
If a has a multiplicative inverse then it is unique.

Corollary

Let n be a prime number. Then each non-zero integer in $\mathbb{Z}_n$ has a multiplicative inverse.

Lemma

If n is a prime number, $n \geq 2$, then $(\mathbb{Z}_n, \oplus, \otimes)$ ia a finite field, where $\oplus$ and $\otimes$ are addition and multiplication modulo n.

Let $\mathbb{Z}_p[x]$ denote the set of all polynomials in the indeterminate x in which coefficients are elements of $\mathbb{Z}_p$.

Definition

A polynomial $f(x) \in \mathbb{Z}_p[x]$ is said to be *irreducible* if there do not exist polynomials $f_1(x), f_2(x) \in \mathbb{Z}_p[x]$ such that $f(x) = f_1(x)f_2(x)$, where $\deg(f_1(x)) > 0$ and where $\deg(f_2(x)) > 0$.

Lemma

For any prime number p and any integer k, $k \geq 1$, there exists an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree k.

Let $f(x) \in \mathbb{Z}_p[x]$ such that $\deg(f(x)) = k$.
For each $g(x) \in \mathbb{Z}_p[x]$ there exist unique quotient $q(x)$ and remainder $r(x)$ such that $g(x) = q(x)f(x) + r(x)$, and $\deg(r(x)) < k$.
Let $\mathbb{Z}_p[x]/f(x) = \{r(x) : r(x) \in \mathbb{Z}_p[x] \text{ and } \deg(r(x)) < k\}$.

Theorem

Suppose that p is prime and $f(x) \in \mathbb{Z}_p[x]$. Then $\mathbb{Z}_p[x]/f(x)$ is a finite field if and only if $f(x)$ is irreducible.

Theorem

There exists a finite field of order n if and only if $n = p^k$, where p is a prime and $k \geq 1$.

Definition

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

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.

Example

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

Definition

A latin square L of side n is *reduced* (or in *standard form*) if in the first row and first column symbols occur in the increasing order.

Definition

A latin square L of side n is *commutative* (or *symmetric*) if $L(i,j) = L(j,i)$ for all $1 \leq i,j \leq n$.

Definition

A latin square 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 $1 \leq i \leq k$.

Remark

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

Remark

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}.

Definition

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'.

Definition

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.

Example

n	♯ non-isotopic latin squares	♯ 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	

Definition

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

A set of three MOLS(4):

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

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

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

Theorem [R. Bose, S. Shrikhande, E.Parker, 1960]

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

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

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

Construction

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 $L_r(i,j) = \alpha_r \times \alpha_i + \alpha_j$.

Definition

A *partial latin square* of order n is an $n \times n$ array in which each cell is either empty or is filled with an element of S, such that each element of S occurs in every row and every column at most once.

Theorem [B. Smetaniuk, 1981]

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

Theorem

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

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

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

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.

Definition

An (a, b)-*Sudoku critical set* is a partial latin square P 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 completion.

(3,3)-Sudoku critical sets are known for all sizes from 17 to 35.

Example

(n, n)	$\sharp$ distinct Sudoku latin squares
$(1, 1)$	1
$(2, 2)$	288
$(3, 3)$	$6,670,903,752,021,072,936,960$

Example

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

Definition

A *Steiner triple system*, STS(v), of order v is a pair $(V, \mathcal{B})$ such that V is a finite set of *points*, where $|V| = v$, and $\mathcal{B}$ is a collection of 3-element subsets of V called *triples* such that any 2-element subset of V is contained in exactly one triple.

The arithmetic necessary conditions for the existence of an STS(v) reduce to $v \equiv 1, 3 \pmod 6$.

Theorem [T. Kirkman, 1847]

A Steiner triple system of order v exists if and only if $v \equiv 1, 3 \pmod 6$.

Bose construction (for $v \equiv 3 \pmod 6$)

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 $0 \leq i \leq 2k$, $\{(i, 1), (i, 2), (i, 3)\} \in \mathcal{B}$

(2) for $0 \leq i < j \leq 2k$, $\{(i, 1), (j, 1), (i \circ j, 2)\} \in \mathcal{B}$,
$\{(i, 2), (j, 2), (i \circ j, 3)\} \in \mathcal{B}$,
$\{(i, 3), (j, 3), (i \circ j, 1)\} \in \mathcal{B}$.

Skolem construction (for $v \equiv 1 \pmod 6$)

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 $0 \leq i \leq k - 1$, $\{(i, 1), (i, 2), (i, 3)\} \in \mathcal{B}$

(2) for $0 \leq i \leq k - 1$, $\{\infty, (k + i, 1), (i, 2)\} \in \mathcal{B}$,
$\{\infty, (k + i, 2), (i, 3)\} \in \mathcal{B}$,
$\{\infty, (k + i, 3), (i, 1)\} \in \mathcal{B}$

(3) for $0 \leq i < j \leq 2k - 1$, $\{(i, 1), (j, 1), (i \circ j, 2)\} \in \mathcal{B}$,
$\{(i, 2), (j, 2), (i \circ j, 3)\} \in \mathcal{B}$,
$\{(i, 3), (j, 3), (i \circ j, 1)\} \in \mathcal{B}$.

Definition

An STS(v) is *cyclic* if it admits an automorphism which is a single cycle of length v.

Definition

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?

[R. Peltesohn, 1939]

Both Heffter's difference problems have solutions except for $v = 9$ (for which no solution exists).

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$(6k + 1)$.

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 $\{0, 2k + 1, 4k + 2\}$.

Definition

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

$n = 5$
$S = (2, 4, 2, 3, 5, 4, 3, 1, 1, 5)$.

Construction

$n = 4t$:

$$
\begin{aligned}
s_{4t+r-1} = s_{8t-r+1} &= 4t - 2r + 2 && r = 1, 2, \ldots, 2t \\
s_r = s_{4t-r-1} &= 4t - 2r - 1 && r = 1, 2, \ldots, t-2 \\
s_{t+r+1} = s_{3t-r} &= 2t - 2r - 1 && r = 1, 2, \ldots, t-2 \\
s_{t-1} = s_{3t} &= 2t + 1 \\
s_t = s_{t+1} &= 1 \\
s_{2t} = s_{4t-1} &= 2t - 1 \\
s_{2t+1} = s_{6t} &= 4t - 1
\end{aligned}
$$

Construction cont.

$n = 4t + 1$:

$$
\begin{aligned}
s_{4t+r+1} = s_{8t-r+3} &= 4t - 2r + 2 && r = 1, 2, \ldots, 2t \\
s_r = s_{4t-r+1} &= 4t - 2r + 1 && r = 1, 2, \ldots, t \\
s_{t+r+2} = s_{3t-r+1} &= 2t - 2r - 1 && r = 1, 2, \ldots, t-2 \\
s_{t+1} = s_{t+2} &= 1 \\
s_{2t+1} = s_{6t+2} &= 4t + 1 \\
s_{2t+2} = s_{4t+1} &= 2t - 1
\end{aligned}
$$

Theorem [T.Skolem, 1957]

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.

Definition

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

$n = 6$
$S = (6, 3, 5, 2, 3, 2, 6, 5, 4, 1, 1, 0, 4)$.

Theorem [E. O'Keefe, 1961]

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.

Example

v	$\sharp\,\mathrm{STS}(v)$
7	1
9	1
13	2
15	80
19	11,084,874,829
21	14,796,207,517,873,771

Construction $v, w \to vw$

Suppose there exist Steiner triple systems STS(v) and STS(w). Then there exists a Steiner triple system STS(vw).

Construction $v \to 2v + 1$

Suppose there exists a Steiner triple systems STS(v). Then there exists a Steiner triple system STS($2v + 1$).

Stern-Lenz Lemma

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.

Construction $v \to 2v + 7$

Suppose there exists a Steiner triple systems STS(v). Then there exists a Steiner triple system STS($2v + 7$).

Definition

A *deficiency graph* is defined to be a graph $G = (V, E)$ with $V = \mathbb{Z}_n \setminus \{0\}$ and $E = \{\{x, -x\}, \{x, -2x\} : x \in V\}$.

Remark

The deficiency graph is cubic.
Moreover, it has a one-factorization $\mathcal{F} = \{F_0, F_1, F_2\}$.

Wilson construction

Let $v \equiv 1$ or $3 \pmod 6$ and set $S = \mathbb{Z}_{v-2} \cup \{\infty_1, \infty_2\}$.
Define $\mathcal{B}$ as follows:
(1) if $x + y + z \equiv 0 \pmod{(v-2)}$ and x, y, z are distinct elements in $\mathbb{Z}_{v-2} \setminus \{0\}$ then $\{x, y, z\} \in \mathcal{B}$
(2) if $\{x, y\} \in F_0$ then $\{0, x, y\} \in \mathcal{B}$
(3) if $\{x, y\} \in F_1$ then $\{\infty_1, x, y\} \in \mathcal{B}$
(4) if $\{x, y\} \in F_2$ then $\{\infty_2, x, y\} \in \mathcal{B}$
(5) $\{0, \infty_1, \infty_2\} \in \mathcal{B}$

Definition

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 x and y determine uniquely a third vector $\mathrm{x} \oplus \mathrm{y}$ 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 x and y, define a unique triple formed by $\{\mathrm{x}, \mathrm{y}, \mathrm{x} \oplus \mathrm{y}\}$. The STS$(2^{m+1}-1)$ produced in this way is called a *projective triple system* and it is often denoted by PG$(m, 2)$ (just consider the triples as lines in the projective space over 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 $V(\mathrm{PG}(m,2)) = \{1, 2, \ldots, 2^{m+1}-1\}$.

Definition

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 $\mathcal{B}$.

Definition

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

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 [J. Doyen, R. Wilson, 1973]

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.

Definition

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*.

Definition

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.

Necessary conditions for the existence of a BIBD(v, b, r, k, λ):
(1) $\lambda(v-1) \equiv 0 \pmod{k-1}$,
(2) $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

$r = \frac{\lambda(v-1)}{k-1} \qquad b = \frac{vr}{k}$

We write (v, k, λ)-*design* (or $(v, k, \lambda) - \mathrm{BIBD}$) to denote a BIBD$(v, b, r, k, \lambda)$.

Example

A $(11, 5, 2) - \text{BIBD}$:
$V = \{0, 1, \ldots, 10\}$,
$\mathcal{B} = \{\{0, 1, 2, 6, 9\}, \{0, 1, 5, 8, 10\}, \{0, 2, 3, 4, 8\}, \{0, 3, 5, 6, 7\},$
$\{0, 4, 7, 9, 10\}, \{1, 2, 3, 7, 10\}, \{1, 3, 4, 5, 9\}, \{1, 4, 6, 7, 8\},$
$\{2, 4, 5, 6, 10\}, \{2, 5, 7, 8, 9\}, \{3, 6, 8, 9, 10\}\}$.

Existence of $(v, k, 1) - \text{BIBDs}$

$k = 2$ iff $v \geq 2$

$k = 3$ iff $v \equiv 1, 3 \pmod 6$ [T. Kirkman, 1847]

$k = 4$ iff $v \equiv 1, 4 \pmod{12}$ [H. Hanani, 1975]

$k = 5$ iff $v \equiv 1, 5 \pmod{20}$ [H. Hanani, 1975]

$k = 6$ if $v \equiv 1, 6 \pmod{15}$ and $v \neq 16, 21, 36, 46;\ 51, 61, 81,$
$166, 226, 231, 256, 261, 286, 316, 321, 346, 351, 376, 406, 411, 436,$
$441, 471, 501, 561, 591, 616, 646, 651, 676, 771, 796, 801$
[R. Abel, M. Greig, 1995,1997);
S. Houghten, L. Thiel, J. Janssen, C. Lam, 2001)]

Definition

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

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 (Fisher's inequality)

If a $(v, k, \lambda) - \text{BIBD}$ exists with $2 \leq k < v$, then $b \geq v$.

Example

A $(21, 6, 1) - \text{BIBD}$ cannot exist since $14 = b < 21 = v$.

Definition

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

Bruck-Ryser-Chowla theorem

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 $k - \lambda$ is a square.
(2) If v is odd, then the equation $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z not all zero.

Definition

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.

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.

Definition

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 $B_2 = \{\alpha(x_i) : x_i \in B_1\}$.

Definition

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.

Definition

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

Definition

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 $d - d'$ with elements from D.

Example

$\{0, 1, 3, 9\}$ is a $(13, 4, 1)$-difference set in the group $\mathbb{Z}_{13}$.

Theorem

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

Definition

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

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

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

Definition

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

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 $(v,k,\lambda)-$BIBD admitting an automorphism group fixing one point and acting sharply transitively on the others.

Example

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

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 ij.
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.

Method of pure and mixed differences - cont.

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 ij for all $i, j \in T$, $i \neq j$.
Then the sets in $\mathcal{D}$ form a *basis* of a $(v, k, \lambda) - \text{BIBD}\ (V, \mathcal{B})$, where $\mathcal{B} = \{D_i + g : \ g \in G,\ i = 1, 2, \ldots s\}$.

Example

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 $(10, 4, 2) - \text{BIBD}$.

Example

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 $(9, 3, 1) - \text{BIBD}$.

Example

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 $(15, 3, 1) - \text{BIBD}$.

Definition

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$(v, b, b - r, v - k, b - 2r + \lambda)$.

Definition

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

Definition

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 $\{\{B_i, B_j\} : \ B_i \cap B_j \neq \emptyset\}$.

For a $(v, k, 1) -$ BIBD, $G(D)$ is strongly regular.

Definition

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

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

Remark

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

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

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

Definition

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) $\lambda u(u-1)m^2 \equiv 0 \pmod{k(k-1)}$.

Theorem

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 $\mathcal{C} = \mathcal{B} \cup \{G \in \mathcal{G} : |G| \geq 2\}$.

Theorem

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.

Definition

A *transversal design*, TD(k, m), is a uniform $k-$GDD of type m^k.

Theorem

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

Construction TD$(4, m) \to$ TD$(4, 3m)$

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$(4, 3m)$.

Construction TD$(4, m)$ with a parallel class $\rightarrow$ TD$(4, 3m+1)$

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$(4, 3m+1)$.

Definition

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

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

Definition

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

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

Theorem [D. Ray-Chaudhuri, R. Wilson, 1971]

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

Lemma

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

Lemma

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 $\text{KTS}(6n + 3)$.

Existence of resolvable $(v, k, 1) - \text{BIBDs}$

$k = 2$ iff $v \equiv 0 \pmod 2$
$k = 3$ iff $v \equiv 3 \pmod 6$
$k = 4$ iff $v \equiv 4 \pmod{12}$
$k = 5$ if $v \equiv 5 \pmod{20}$ and $v \neq 45, 345, 465, 645$

Theorem

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

Corollary

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

Definition

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

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

Definition

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

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

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

Remark

An affine plane is resolvable.

Theorem

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

Construction

Let $n = p^k$ be a prime power. Let $V = \mathbb{F}_n \times \mathbb{F}_n$.
For any $a, b \in \mathbb{F}_n$, define a line $L_{a,b} = \{(x, y) \in V : \ y = ax + b\}$.
For any $c \in \mathbb{F}_n$, define $L_{\infty,c} = \{(c, y) \in V : \ y \in \mathbb{F}_n\}$.
Finally, define $\mathcal{L} = \{L_{a,b} : \ a, b \in \mathbb{F}_n\} \cup \{L_{\infty,c} : \ c \in \mathbb{F}_n\}$.
$(V, \mathcal{L})$ is a $(n^2, n, 1) - \text{BIBD}$.

Definition

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

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.

Definition

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

Theorem [B. Alspach, H. Gavlas, 2001; M. Šajna ,2002] Necessary conditions:

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

Definition

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.

Theorem [D. Ray-Chaudhuri, R. Wilson, 1971; B. Alspach, P. Schellenberg, D. Stinson, D. Wagner, 1989] Necessary conditions:

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 [D. Bryant, D. Horsley, W. Pettersson, 2014]

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 [G. Ringel ,1967]

Let n be odd, $3 \leq m_1, m_2, \ldots, m_t$ 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) $m_1 = m_2 = 3,\ m_3 = 5$.