Symmetric Designs

Lucia Moura
School of Electrical Engineering and Computer Science
University of Ottawa
lucia@eecs.uottawa.ca

Winter 2017

Symmetric Designs

Definition (Symmetric BIBD)

A BIBD with $v = b$ (or equivalently, $r = k$ or $\lambda(v-1) = k^2 - k$) is called a *symmetric* BIBD.

Example: a $(7,3,1)$-design is symmetric.
$V = \{1,2,3,4,5,6,7\}$
$\mathcal{B} = \{123, 145, 167, 246, 257, 347, 356\}$

	1234567
1	1110000
2	1001100
3	1000011
4	0101010
5	0100101
6	0011001
7	0010110

Symmetric Designs: an intersection property

Theorem (a symmetric design is "linked" i.e. has constant block intersection λ)

Suppose that $(V, \mathcal{B})$ is a symmetric (v, k, λ)-BIBD and denote $\mathcal{B} = \{B_1, \ldots, B_v\}$. Then, we have $|B_i \cap B_j| = \lambda$, for all $1 \leq i, j \leq v$, $i \neq j$, .

	1234567
1	1110000
2	1001100
3	1000011
4	0101010
5	0100101
6	0011001
7	0010110

Proof: We use similar methods as in the proof of Fisher's inequality. Let s_j be column j of the incidence matrix of the BIBD. Let's fix a block h, $1 \leq h \leq b$. Using equations derived for that other proof, we get.

$$\sum_{i \in B_h} \sum_{j : i \in B_j} s_j = \sum_{\{i : i \in B_h\}} ((r-\lambda)e_i + (\lambda, \ldots, \lambda)) =$$

$$= (r-\lambda)s_h + k(\lambda, \ldots, \lambda) = (r-\lambda)s_h + \sum_{j=1}^{b} \frac{\lambda k}{r} s_j$$

We can also compute this double sum in another way

$$\sum_{i \in B_h} \sum_{j : i \in B_j} s_j = \sum_{j=1}^{b} \sum_{i \in B_h \cap B_j} s_j$$

$$= \sum_{j=1}^{b} |B_h \cap B_j| s_j$$

proof (cont'd)
Thus, $(r-\lambda)s_h + \sum_{j=1}^{b} \frac{\lambda k}{r} s_j = \sum_{j=1}^{b} |B_h \cap B_j| s_j$.
Since $r = k$ and $b = v$, this simplifies to

$$(r-\lambda)s_h + \sum_{j=1}^{v} \lambda s_j = \sum_{j=1}^{v} |B_h \cap B_j| s_j.$$

In the other proof, we showed that span$(s_1, \ldots, s_b) = \mathbb{R}^v$.
Since $v = b$, $\{s_1, \ldots, s_v\}$ must be a basis of $\mathbb{R}^v$
Since this is a basis, the coefficients of s_j in the right and left of the equation above must be equal. So, for $j! = h$ we must have $|B_h \cap B_j| = \lambda$.
Since this is true for every choice of h, $|B \cap B'| = \lambda$ for all $B, B' \in \mathcal{B}$. $\square$

Other symmetric designs and properties

Corollary (the dual of a symmetric BIBD is a symmetric BIBD)

Suppose that M is the incidence matrix of a symmetric (v, k, λ)-BIBD. Then M^T is also the incidence matrix of a symmetric (v, k, λ)-BIBD.

Corollary (a linked BIBD must be symmetric)

Suppose that μ is a positive integer and $(V, \mathcal{B})$ is a (v, b, r, k, λ)-BIBD such that $|B \cap B'| = \mu$ for all $B, B' \in \mathcal{B}$. Then $(V, \mathcal{B})$ is a symmetric BIBD and $\mu = \lambda$.

Residual and derived BIBDs

Definition

Let $(V, \mathcal{B})$ be a a symmetric (v, k, λ)-BIBD, and let $B_0 \in \mathcal{B}$. Its derived design is

$$Der(V, \mathcal{B}, B_0) = (B_0, \{B \cap B_0 : B \in \mathcal{B}, B \neq B_0\})$$

and its residual design is

$$Res(V, \mathcal{B}, B_0) = (V \setminus B_0, \{B \setminus B_0 : B \in \mathcal{B}, B \neq B_0\})$$

1	3	4	5	9
4	5	2	6	10
3	5	6	7	0
1	4	6	7	8
5	9	2	7	8
3	9	6	8	10
4	9	0	7	10
1	5	0	8	10
1	9	2	6	0
1	3	2	7	10
3	4	0	2	8

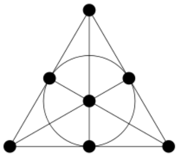
Theorem

Let $(V, \mathcal{B})$ be a a symmetric (v, k, λ)-BIBD.
If $\lambda \geq 2$, then $Der(V, \mathcal{B}, B_0)$ is a $(k, v-1, k-1, \lambda, \lambda-1)$-BIBD.
If $k \geq \lambda + 2$, then $Res(V, \mathcal{B}, B_0)$ is a $(v-k, v-1, k, k-\lambda, \lambda)$-BIBD.

Definition (projective plane)

An $(n^2+n+1, n+1, 1)$ with $n \geq 2$ is called a *projective plane* of order n.

The $(7,3,1)$-BIBD is a projective plane of order 2.



Proposition

A projective plane is a symmetric BIBD.

Proof. $r = \frac{n^2+n}{n} = n+1 = k$; $b = \frac{vr}{k} = v = n^2+n+1$.

Theorem

For every prime power $q \geq 2$, there exists a (symmetric) $(q^2+q+1, q+1, 1)$-BIBD (i.e. a projective plane of order q).

Proof. Let $\mathbb{F}_q$ be the finite field of order q and consider V a tridimensional (3-D) vector space over $\mathbb{F}_q$. The points of the design are the 1-D subspaces of V and let the blocks of the design be the 2-D subspaces of V. The design makes a point incident to a block if the 1-D subspace is contained in the 2-D subspace. There are $\frac{q^3-1}{q-1} = q^2+q+1$ 1-D subspaces of V. So $b = q^2+q+1$. Each 2-D subspace B has q^2 points including (0,0,0); each of the q^2-1 nonzero points together with (0,0,0) defines a 1-D subspace of B; each of them are counted $q-1$ times one for each of the $q-1$ non-zero points inside it. So, there are $\frac{q^2-1}{q-1} = q+1 (= k)$ 2-D subspaces inside B. There is a unique 2-D subspace containing any pair of 1-D subspaces, so $\lambda = 1$. □

Example: $(13,4,1)$-BIBD is a projective plane of order 3

(picture from Stinson 2004, Chapter 2)

$C_1 = \{000, 001, 002\}$	$B_1 = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$
$C_2 = \{000, 010, 020\}$	$B_2 = \{000, 001, 002, 100, 200, 101, 102, 201, 202\}$
$C_3 = \{000, 011, 022\}$	$B_3 = \{000, 001, 002, 110, 220, 111, 112, 221, 222\}$
$C_4 = \{000, 012, 021\}$	$B_4 = \{000, 001, 002, 120, 210, 121, 122, 211, 212\}$
$C_5 = \{000, 100, 200\}$	$B_5 = \{000, 010, 020, 100, 200, 110, 120, 210, 220\}$
$C_6 = \{000, 101, 202\}$	$B_6 = \{000, 010, 020, 101, 202, 111, 121, 212, 222\}$
$C_7 = \{000, 102, 201\}$	$B_7 = \{000, 010, 020, 102, 201, 112, 122, 211, 221\}$
$C_8 = \{000, 110, 220\}$	$B_8 = \{000, 011, 022, 100, 200, 111, 122, 211, 222\}$
$C_9 = \{000, 111, 222\}$	$B_9 = \{000, 011, 022, 101, 202, 112, 120, 210, 221\}$
$C_{10} = \{000, 112, 221\}$	$B_{10} = \{000, 011, 022, 102, 201, 110, 121, 212, 220\}$
$C_{11} = \{000, 120, 210\}$	$B_{11} = \{000, 012, 021, 100, 200, 112, 121, 212, 221\}$
$C_{12} = \{000, 122, 211\}$	$B_{12} = \{000, 012, 021, 101, 202, 110, 122, 211, 220\}$
$C_{13} = \{000, 121, 212\}$	$B_{13} = \{000, 012, 021, 102, 201, 111, 120, 210, 222\}.$

Fig. 2.2. The One-dimensional and Two-dimensional Subspaces of $(\mathbb{Z}_3)^3$

cont'd example: $(13, 4, 1)$-BIBD is a projective plane of order 3

(picture from Stinson 2004, Chapter 2)

$$
\begin{aligned}
A_{B_1} &= \{C_1, C_2, C_3, C_4\} \\
A_{B_2} &= \{C_1, C_5, C_6, C_7\} \\
A_{B_3} &= \{C_1, C_8, C_9, C_{10}\} \\
A_{B_4} &= \{C_1, C_{11}, C_{12}, C_{13}\} \\
A_{B_5} &= \{C_2, C_5, C_8, C_{11}\} \\
A_{B_6} &= \{C_2, C_6, C_9, C_{13}\} \\
A_{B_7} &= \{C_2, C_7, C_{10}, C_{12}\} \\
A_{B_8} &= \{C_3, C_5, C_9, C_{12}\} \\
A_{B_9} &= \{C_3, C_6, C_{10}, C_{11}\} \\
A_{B_{10}} &= \{C_3, C_7, C_8, C_{13}\} \\
A_{B_{11}} &= \{C_4, C_5, C_{10}, C_{13}\} \\
A_{B_{12}} &= \{C_4, C_6, C_8, C_{12}\} \\
A_{B_{13}} &= \{C_4, C_7, C_9, C_{11}\}.
\end{aligned}
$$

Fig. 2.3. The Blocks of the Projective Plane of Order 3

Affine planes

Definition (affine plane)

An $(n^2, n, 1)$ with $n \geq 2$ is called an *affine plane* of order n.

Corollary

For every prime power $q \geq 2$, there exists a $(q^2, q, 1)$-BIBD (i.e. an affine plane of order q).

Proof: Take the residual design of a projective plane of order n. □

Affine planes: exercise

1. Use the $(13, 4, 1) - BIBD$, a projective plane of order 3, to construct a $(9, 3, 1)$-BIBD, an affine plane of order 3.

2. What the elements of the removed block of the projective plane represent in terms of the blocks of the affine plane?

Affine plane of order 3 from projective plane of order 3

$$
\begin{aligned}
A_{B_1} &= \{C_1, C_2, C_3, C_4\}\\
A_{B_2} &= \{C_1, C_5, C_6, C_7\}\\
A_{B_3} &= \{C_1, C_8, C_9, C_{10}\}\\
A_{B_4} &= \{C_1, C_{11}, C_{12}, C_{13}\}\\
A_{B_5} &= \{C_2, C_5, C_8, C_{11}\}\\
A_{B_6} &= \{C_2, C_6, C_9, C_{13}\}\\
A_{B_7} &= \{C_2, C_7, C_{10}, C_{12}\}\\
A_{B_8} &= \{C_3, C_5, C_9, C_{12}\}\\
A_{B_9} &= \{C_3, C_6, C_{10}, C_{11}\}\\
A_{B_{10}} &= \{C_3, C_7, C_8, C_{13}\}\\
A_{B_{11}} &= \{C_4, C_5, C_{10}, C_{13}\}\\
A_{B_{12}} &= \{C_4, C_6, C_8, C_{12}\}\\
A_{B_{13}} &= \{C_4, C_7, C_9, C_{11}\}.
\end{aligned}
$$

How can you prove these affine planes are always resolvable?

Points and hyperplanes of a projective geometry $PG_d(q)$

Theorem

Let q be a prime power and $d \geq 2$ be an integer. Then there exists a symmetric

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^q-1}{q-1}, \frac{q^{d-1}-1}{q-1} \right) - \mathrm{BIBD}.$$

Proof. Let $V = \mathbb{F}_q^{d+1}$. The points are the one-dimensional subspaces of V and the blocks correspond to the d-dimensional subspaces of V (hyperplanes).

- each nonzero point defines a one dimensional subspace together with 0, and each line has $q-1$ of those nonzero points, so $v = \frac{q^{d+1}-1}{q-1}$.
- using a similar argument each subspace of dimension d contains $k = \frac{q^d-1}{q-1}$ one dimensional subspaces.
- each pair of one dimensional subspaces (a plane) appear together in $\lambda = \frac{q^{d-1}-1}{q-1}$ d-dimensional subspaces.

Corollary

Let $q \geq 2$ be a prime power and $d \geq 2$ be an integer. There there exists a

$$\left(q^d, q^{d-1}, \frac{q^{d-1}-1}{q-1}\right) - \mathrm{BIBD}.$$

In addition, if $d > 2$, then there exists a

$$\left(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q(q^{d-2}-1)}{q-1}\right) - \mathrm{BIBD}.$$

Proof: These are residual and derived BIBDs from the BIBD given in the previous theorem. □

Necessary conditions for the existence of symmetric designs

Theorem (Bruck-Ryser-Chowla theorem, v even)

If there exists a symmetric (v, k, λ)-BIBD with v even, then $k - \lambda$ is a perfect square.

The proof involves studying the determinant of MM^T, where M is the incidence matrix of the symmetric design. See page 30-31 of Stinson 2004.

Example: prove that a $(22, 7, 2)$-BIBD does not exist.
Since $b = \frac{\lambda v(v-1)}{k(k-1)} = \frac{2\times 22\times 21}{7\times 6} = 22$, if it exists it would be a symmetric design. However, $k - \lambda = 5$ is not a perfect square, so this design does not exist.

(continued) Necessary conditions for symmetric designs

Theorem (Bruck-Ryser-Chowla theorem, v odd)

If there exists a symmetric (v, k, λ)-BIBD with v odd, then there exist integers x, y and z (not all zero) such that

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

Together with some other number theorem results, the above theorem can be used to show a condition to rule out the existence of some projective planes.

Theorem

Suppose that $n \equiv 1, 2 \pmod 4$, and there exists a prime $p \equiv 3 \pmod 4$ such that the largest power of p that divides n is odd. Then a projective plane of order n does not exist.

Examples: projective planes do not exist for $n = 6, 14, 21, 22, 30$.

References

- D. R. Stinson, “Combinatorial Designs: Constructions and Analysis”, 2004 (Chapter 2).