Introduction to Block Designs

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

Winter 2017

What is Design Theory?

Combinatorial design theory deals with the arrangement of elements into subsets satisfying some "balance" property.
Many types of combinatorial designs: block designs, Steiner triple systems, t-designs, Latin squares, orthogonal arrays, etc.
Main issues in the theory:

- Existence of designs
- Construction of designs
- Enumeration of designs

There are many applications of designs.

- cryptography
- coding theory
- design of experiments in statistics
- others: interconnection networks, software testing, tournament scheduling, etc.

Balanced Incomplete Block Designs

Definition (Design)

A *design* is a pair $(V, \mathcal{B})$ such that

1. V is a set of elements called *points*.
2. B is a collection (multiset) of nonempty subsets of V called *blocks*.

Definition (Balanced Incomplete Block Design)

Let v, k and λ be positive integers such that $v > k \geq 2$. A (v, k, λ)-BIBD is a design $(V, \mathcal{B})$ such that

1. $|V| = v$,
2. each block contains exactly k points, and
3. every pair of distinct points is contained in exactly λ blocks.

BIBD examples

$(7,3,1)$-BIBD: (Note: we write abc to denote block $\{a,b,c\}$)

$$\begin{aligned} V &= \{1,2,3,4,5,6,7\} \\ \mathcal{B} &= \{123,145,167,246,257,347,356\} \end{aligned}$$

$(9,3,1)$-BIBD:

$$\begin{aligned} V &= \{1,2,3,4,5,6,7,8,9\} \\ \mathcal{B} &= \{123,456,789,147,258,369, \\ &\quad 159,267,348,168,249,357\} \end{aligned}$$

$(10,4,2)$-BIBD

$$\begin{aligned} V &= \{0,1,2,3,4,5,6,7,8,9\} \\ \mathcal{B} &= \{0123,0145,0246,0378,0579,0689,1278,1369, \\ &\quad 1479,1568,2359,2489,2567,3458,3467\} \end{aligned}$$

Theorem (constant replication number r)

In a (v, k, λ)-BIBD, every point is contained in exactly $r = \frac{\lambda(v-1)}{k-1}$ blocks.

Proof: Let $(V, \mathcal{B})$ be a (v, k, λ)-BIBD. For $x \in V$, let r_x denote the number of blocks containing x. Define a set

$$I_x = \{(y, B) : y \in X, y \neq x, B \in \mathcal{B}, \{x, y\} \subseteq B\}$$

We compute $|I_x|$ in two ways.

- There are $(v-1)$ ways to choose $y \neq x$ and for each one there are λ blocks containing $\{x, y\}$. Thus, $|I_x| = \lambda(v-1)$.
- There are r_x ways to choose B such that $x \in B$. For each choice of B there are $k-1$ ways to choose $y \neq x$, $y \in B$. Thus, $|I| = r_x(k-1)$.

Combining the two equations, we get $r_x = \frac{\lambda(v-1)}{k-1}$, which is independent of x. $\square$

Theorem (number of blocks b)

A (v, k, λ)-BIBD, has exactly $b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{k^2-k}$ blocks.

Proof:
Let $(V, \mathcal{B})$ be a (v, k, λ)-BIBD. Define the set

$$J = \{(x, B) : x \in X, B \in \mathcal{B}, x, \in B\}$$

Computing $|J|$ in two ways:

- There are v ways to choose x and there are r blocks containing x. Thus, $|J| = vr$.
- There are b ways to choose B and for each B there are k ways to choose $x \in B$. Thus, $|J| = bk$.

Thus, $bk = vr$. This gives $b = \frac{vr}{k}$ and substituting $r = \frac{\lambda(v-1)}{k-1}$ completes the proof. $\square$

Necessary conditions for existence

Corollary

If there exist a (v, k, λ)-BIBD then

$$\begin{aligned} \lambda(v-1) &\equiv 0 \pmod{k-1} \\ \lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \end{aligned}$$

Examples of consequences for Steiner triple systems
(note: an STS(v) is a $(v, 3, 1)$-BIBD)

- There exist no STS(8).
- An STS(v) exists only if $v \equiv 1, 3 \pmod{6}$.

Parameters (v, b, r, k, λ) satisfying the trivial necessary conditions above are called *admissible*.
These necessary conditions in the theorem are not always sufficient.

Existence table - sample of admissible parameters

No	v	b	r	k	λ	Nd	Nr	Comments, Ref	Where?
31	7	21	9	3	3	10		- 3#1 [696]	1.20
32	28	63	9	4	1	≥ 4747	≥ 7	[1346, 1533, 1548]	III.1.8
33	10	18	9	5	4	21	0	R#41,×3 [898]	VI.16.85
34	46	69	9	6	1	0		- [1138]	
35	16	24	9	6	3	18920		- R#40 [1938]	II.6.30
36	28	36	9	7	2	8	0	R#39,×3 [124]	
37	64	72	9	8	1	1	1	R#38,AG(2,8)	
38	73	73	9	9	1	1		- PG(2,8)	VI.18.73
39	37	37	9	9	2	4		- [124]	II.6.47
40	25	25	9	9	3	78		- [694]	II.6.47
41	19	19	9	9	4	6		- [898]	1.33
42	21	70	10	3	1	≥ 62336617	≥ 63745	[518, 1263]	VI.16.12
43	6	20	10	3	4	4	1	2#4 [1241, 976]	
44	16	40	10	4	2	$\geq 2.2 \cdot 10^6$	339592	2#5 [696, 1267]	
45	41	82	10	5	1	≥ 15		- [1347]	VI.16.16
46	21	42	10	5	2	≥ 22998		- 2#6 [2064]	
47	11	22	10	5	4	4393		- 2#7,D#63 [323]	
48	51	85	10	6	1	?		-	
49	21	30	10	7	3	3809	0	R#54,×3 [1016, 1241, 1946]	
50	36	45	10	8	2	0		- R#53*,×2	
51	81	90	10	9	1	7	7	R#52,AG(2,9) [679, 1373]	
52	91	91	10	10	1	4		- PG(2,9) [679, 1373]	VI.18.73
53	46	46	10	10	2	0		- ×1	
54	31	31	10	10	3	151		- [1941]	II.6.47

(source: Colbourn and Dinitz, Handbook of Combinatorial Designs, 2006)

Constructions: building new block designs from old

Example: Add the blocks of two $(7, 3, 1)$-BIBDs to form a $(7, 3, 2)$-BIBD.

Example 1

124	126
235	237
346	341
457	452
561	563
672	674
713	715

Example 2

124	124
235	235
346	346
457	457
561	561
672	672
713	713

Theorem (Sum construction)

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

Constructions: building new block designs from old

Theorem (Block complementation)

If there exists a (v, b, r, k, λ)-BIBD then there exists a $(v, b, b-r, v-k, b-2r+\lambda)$-BIBD.

(7,7,3,3,1)-BIBD:
124
235
346
457
561
672
713

(7,7,4,4,2)-BIBD:
3567
4671
5712
6123
7234
1345
2678

Constructions: building new block designs from old

Theorem (Block complementation)

If there exists a (v, b, r, k, λ)-BIBD, where $k \leq v - 2$, then there exists a $(v, b, b - r, v - k, b - 2r + \lambda)$-BIBD.

Proof:
Build the design $(V, \mathcal{B}')$, where $\mathcal{B}' = \{X \setminus B : B \in \mathcal{B}\}$.
It is easy to see that this design has v points, b blocks, block size $k' = v - k \geq 2$ and each point appears in $r' = b - r$ blocks.
We just need to show that every pair of points x, y $(x \neq y)$, occurs in $\lambda' = b - 2r + \lambda$ blocks. Define
$a_{xy} = |\{B \in \mathcal{B}' : x, y \in B\}|$,$a_{x\overline{y}} = |\{B \in \mathcal{B}' : x \in B, y \notin B\}$,
$a_{\overline{x}y} = |\{B \in \mathcal{B}' : x \notin B', y \in B\}$,$a_{\overline{xy}} = |\{B \in \mathcal{B}' : x, y \notin B\}$,
We get: $a_{xy} = \lambda'$, $a_{x\overline{y}} = a_{\overline{x}y} = b - r - \lambda'$, $a_{\overline{xy}} = \lambda$ and
$a_{xy} + a_{x\overline{y}} + a_{\overline{x}y} + a_{\overline{xy}} = b$. Substituting we get $\lambda' = b - 2r + \lambda$. $\square$

Theorem (Fisher's inequality)

In any (v, b, r, k, λ)-BIBD we must have $b \geq v$.

Proof. For each block B_j in the BIBD, consider its incidence vector s^j, where $(s^j)_i = 1$ if $i \in B_j$ and $(s^j)_i = 0$, otherwise. Let $S = span(s_j : 1 \leq j \leq b)$, that is S is the subspace of $\mathbb{R}^v$ spanned by the s_j's: $S = \{\sum_{j=1}^{b} \alpha_j s_j : \alpha_1, \ldots, \alpha_b \in \mathbb{R}\}$. We will prove $S = R^v$; once we do that, we can conclude that since S is spanned by b vectors and it has dimension v, then we must have $b \geq v$.
To show that $S = \mathbb{R}^v$, it is sufficient to show how to write each elements of a basis of $\mathbb{R}^v$ as a linear combination of the vectors in $\{s_j : 1 \leq j \leq b\}$. We will chose the canonical basis $\{e_1, \ldots, e_v\}$ where e_i is formed by a 1 in coordinate i and zero on the other coordinates. It is enough then to show how to write e_i as a linear combination of s_j's. We do this in the next page.

(continuing the proof of Fisher's inequality)
Note that $\sum_{j=1}^{b} s_j = (r, \ldots, r)$, thus $\sum_{j=1}^{b} \frac{1}{r} s_j = (1, \ldots, 1)$.
Then, fix a point i, $1 \leq i \leq v$. We have

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

.
We claim $r - \lambda \neq 0$. Indeed, since $\lambda(v-1) = r(k-1)$ and $v > k$ we get $r > \lambda$. So, since $r - \lambda \neq 0$, we can combine the equations and get

$$e_i = \sum_{\{j : x_i \in B_j\}} \frac{1}{r - \lambda} s_j - \sum_{j=1}^{b} \frac{\lambda}{r(r-\lambda)} s_j.$$

So we can write every member of a basis of R_v as a linear combination of the S_j's. $\square$

Using Fisher's inequality

Note that we can express the same conclusion $b \geq v$ equivalently as $r \geq k$ and $\lambda(v-1) > k^2 - k$.

Consider the parameter set of a $(16, 6, 1)$-BIBD. We would have $r = 3 < k$. So no such design can exist.

Resolvable BIBDs

Definition (resolvable BIBD)

In a BIBD, a parallel class is a set of blocks where each element of V appear in exactly one block. A $(v, k, 1)$-BIBD is *resolvable* if their blocks can be partitioned in r paralel classes.

Example: The $(9, 3, 1)$-BIBD is resolvable:

$$\begin{aligned} V &= \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \\ \mathcal{B} &= \{123, 456, 789, 147, 258, 369, \\ &\quad 159, 267, 348, 168, 249, 357\} \end{aligned}$$

paralel classes:
p1: 123, 456, 789,
p2: 147, 258, 369,
p3: 159, 267, 348,
p4: 168, 249, 357

Resolvable BIBDs: example of infinite families

There exist a resolvable Steiner triple system, i.e. a $(v, 3, 1)$-design, for every $v \equiv 3 \pmod 6$.

Kirkman schoolgirl problem (1850) "Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast."

Sun	Mon	Tue	Wed	Thu	Fri	Sat
01, 06, 11	01, 02, 05	02, 03, 06	05, 06, 09	03, 05, 11	05, 07, 13	11, 13, 04
02, 07, 12	03, 04, 07	04, 05, 08	07, 08, 11	04, 06, 12	06, 08, 14	12, 14, 05
03, 08, 13	08, 09, 12	09, 10, 13	12, 13, 01	07, 09, 15	09, 11, 02	15, 02, 08
04, 09, 14	10, 11, 14	11, 12, 15	14, 15, 03	08, 10, 01	10, 12, 03	01, 03, 09
05, 10, 15	13, 15, 06	14, 01, 07	02, 04, 10	13, 14, 02	15, 01, 04	06, 07, 10

Resolvable BIBDs: example of infinite families

Afine planes are $(n^2, n, 1)$-BIBDs.

Theorem

For every prime power q, there exist an afine plane with $n = q$.

The construction uses finite fields.

Examples: (9,3,1)-BIBD, (16,4,1), (25,5,1), etc.

Theorem

Every affine plane is resolvable.

Threshold schemes for secret sharing

"Suppose that a bank has a vault that must be opened every day. The bank employs three senior tellers, but they do not want to trust any individual with the combination. Hence, they would like to devise a system that enables any two of the three senior tellers to gain access to the vault." (see Stinson 2004, chapter 11.2)

Definition

Let t and w be integers such that $2 \leq t \leq w$. A (t, w)-threshold scheme is a method to share a secret value K among a finite set $\mathcal{P} = \{P_1, P_2, \ldots, P_w\}$ of w participants in such way that any group of t or more participants can compute the value K but no group of $t-1$ (or less) can determine the secret. If no group of $t-1$ or less participants can obtain any information about the value of K from the information they collective hold, the scheme is called *perfect*.

Theorem

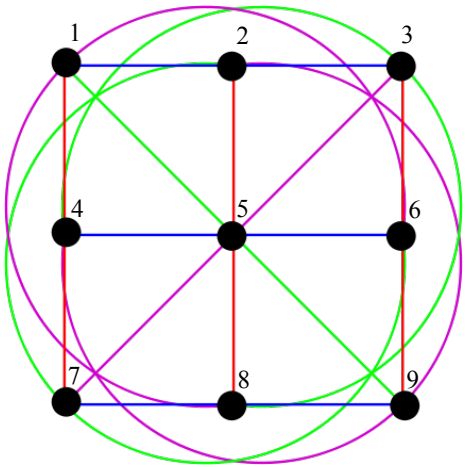
If there exist a resolvable $(v, w, 1)$-BIBD then there exist a perfect $(2, w)$-threshold scheme.

A resolvable $(v, w, 1)$-BIBD $(X, \mathcal{B})$ has r paralel classes. Suppose the dealer $\mathcal{D}$ wants to share a secret K, $1 \leq K \leq r$.

1. $\mathcal{D}$ choses a random block B of $\mathcal{B}$ contained in parallel class K.
2. The w values in B are distributed among the w participants.

Resolvable BIBDs: perfect threshold schemes

group of $w = 3$ managers
any 2 can open the safe
own share reveals no info



Example: key b
M_1 gets "5"
M_2 gets "2"
M_3 gets "8"

shares ($w = 3$ people)	key (secret)
1, 2, 3	a
4, 5, 6	a
7, 8, 9	a
1, 4, 7	b
2, 5, 8	b
3, 6, 9	b
1, 5, 9	c
2, 7, 6	c
3, 4, 8	c
1, 6, 8	d
2, 4, 9	d
3, 5, 7	d

Justification

- Two participants determine a unique block (BIBD with $\lambda = 1$), and therefore know its resolution class (the secret K).
- A share s appears in a block in each of the r resolution classes; therefore, a participant with share s is consistent with any of the r possible secrets.

Therefore, we have a perfect threshold scheme.
Because a $(q^2, q, 1)$-BIBD exists for any q that is a prime power, we can build a perfect $(q, 2)$-threshold schemes to share a secret among q people. In this case, the number of possible secrets is $r = \frac{q^2-1}{q-1} = q + 1$,

References

- D. R. Stinson, "Combinatorial Designs: Constructions and Analysis", 2004.