Combinatorial Structures
Part 1: Block Designs
CS 858 Notes

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

May 14, 2019

1 Balanced Incomplete Block Designs (BIBDs)

Suppose $1 < k < v$ are integers and $\lambda \geq 1$ is an integer.

A (v, k, λ)-BIBD is a collection of k-subsets (called *blocks*) of a v-set (whose elements are called *points*), such that every pair of points is in exactly λ blocks.

Question: for what choices of parameters (v, k, λ) can we construct a (v, k, λ)-BIBD?

The case $k = 2$ is trivial— take every pair λ times. For example, a $(3, 2, 1)$-BIBD has blocks $\{1, 2\}, \{1, 3\}, \{2, 3\}$.

The blocks $\{1, 2, 3\}, \{1, 4, 7\}, \{1, 5, 6\}, \{3, 4, 5\}, \{2, 5, 7\}, \{3, 6, 7\}, \{2, 4, 6\}$ form a $(7, 3, 1)$-BIBD.

An alternative construction for a $(7, 3, 1)$-BIBD: The points are the elements of $\mathbb{Z}_7$. Start with the *base block* $\{0, 1, 3\}$. Then develop the base block modulo 7, obtaining the blocks $\{0, 1, 3\}$, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 0\}$, $\{5, 6, 1\}$, $\{6, 0, 2\}$. We add 1 (mod 7) to every point in a block to get the next block.

This works because the base block contains every difference modulo 7 exactly once: $0 - 1 = 6$, $1 - 0 = 1$, $0 - 3 = 4$, $3 - 0 = 3$, $1 - 3 = 5$, $3 - 1 = 2$.

Two other parameters in a (v,k,λ)-BIBD are r and b. Every point occurs in r blocks, where $r = \lambda(v-1)/(k-1)$. The total number of blocks is $b = vr/k$. Note that r and b must be integers.

Example: In a $(7,3,1)$-BIBD, $r = 1 \times 6/2 = 3$ and $b = 7 \times 3/3 = 7$.

Example: If a $(6,3,2)$-BIBD exists, then $r = 2\times 5/2 = 5$ and $b = 6\times 5/3 = 10$.

Sometimes we write the parameters of a BIBD as (v,b,r,k,λ).

Example: If an $(11,3,1)$-BIBD exists, then $r = 5$ and $b = 11\times 5/3 = 55/3$. The value b is not an integer, so the BIBD does not exist.

Example: We construct a $(6,3,2)$-BIBD. Take points $\mathbb{Z}_5 \cup 0\{\infty\}$ and develop the two base blocks $\{\infty,0,2\}$ and $\{0,1,2\}$ modulo 5, using the rule $\infty + i = \infty$ for all i. We obtain 10 blocks: $\{\infty,0,2\}$, $\{\infty,1,3\}$ $\{\infty,2,4\}$, $\{\infty,3,0\}$, $\{\infty,4,1\}$, $\{0,1,2\}$, $\{1,2,3\}$, $\{2,3,4\}$, $\{3,4,0\}$, $\{4,0,1\}$. We can check that every difference occurs twice: $0-2=3$, $2-0=2$, $0-1=4$, $1-0=1$, $1-2=4$, $2-1=1$, $0-2=3$, $2-0=2$. Also, ∞ occurs with every other point twice. So we get a BIBD with $\lambda = 2$.

Fisher's Inequality: If a (v,b,r,k,λ)-BIBD exists, then $b \geq v$. (Equivalently, $r \geq k$.)

Example: If a $(16,6,1)$-BIBD exists, then $r = 3$ and $b = 8$. Therefore, this BIBD does not exist, because Fisher's Inequality is violated.

If a (v,k,λ)-BIBD has $b = v$ (equivalently, $r = k$), then the BIBD is called a *symmetric* BIBD and it is denoted an SBIBD.

Theorem: Any two blocks in a (v,k,λ)-SBIBD contain exactly λ common points.

Example: A $(7,3,1)$-BIBD is symmetric. Therefore, any two blocks intersect in exactly one point.

Example: An $(11,5,2)$-BIBD is symmetric. It can be constructed by developing the base block $\{1,3,4,5,9\}$ modulo 11. Any two blocks of this BIBD intersect in exactly two points. The base block consists of the quadratic residues (i.e., perfect squares) modulo 11: $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 5$ and $5^2 = 3$, where all arithmetic is modulo 11.

An $(n^2+n+1, n+1, 1)$-BIBD is called a *projective plane of order* n. It is a symmetric BIBD, so every pair of blocks intersect in exactly one point.

A projective plane of order n exists if n is a prime power. Therefore projective planes of orders $2,3,4,5,7,8$ and 9 all exist. There is no projective plane of order 6 or 10.

Here is a construction for a projective plane of order q, where q is a prime power. Let $\mathbb{F}_q$ denote the finite field of order q (side comment: $\mathbb{F}_q$ is the same thing as $\mathbb{Z}_q$ if q is prime). The points of the design are the 1-dimensional subspaces of $(\mathbb{F}_q)^3$ and the blocks are the 2-dimensional subspaces of $(\mathbb{F}_q)^3$.

A projective plane of order q, where q is a prime power, can also be constructed from a base block in $\mathbb{Z}_{q^2+q+1}$.

Example: $\{7, 14, 3, 6, 12\}$ is a base block (modulo 21) for a projective plane of order 4.

Bruck-Ryser-Chowla Theorem: Suppose that a (v, k, λ)-SBIBD exists. Then (1) if v is even, then $k - \lambda$ is a perfect square, and (2) if v is odd, then the equation $x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$ has a nontrivial integral solution (i.e., a solution (x, y, z) where x, y and z are integers that are not all equal to 0).

Example: A $(22, 7, 2)$-SBIBD does not exist, because 22 is even and $7-2 = 5$ is not a perfect square.

Example: We can use the Bruck-Ryser-Chowla Theorem to show that a projective plane of order 6 does not exist. Such a BIBD would be a $(43, 7, 1)$-SBIBD. If it existed, then the equation $x^2 = 6y^2 + -z^2$ would have a nontrivial integral solution. It can be shown that the equation has no nontrivial integral solution, which means that the BIBD does not exist.

An $(n^2, n, 1)$-BIBD is called an *affine plane of order* n. It has $r = n+1$ and $b = n^2 + n$.

A projective plane of order n is equivalent to an affine plane of order n.

Example: A projective plane of order 3 can be constructed by developing the base block $\{0, 1, 3, 9\}$ modulo 13. We obtain the following blocks:

$$\begin{array}{l}\{0,1,3,9\},\ \{1,2,4,10\},\ \{2,3,5,11\},\ \{3,4,6,12\},\ \{4,5,7,0\},\\ \{5,6,8,1\},\ \{6,7,9,2\},\ \{7,8,10,3\},\ \{8,9,11,4\},\\ \{9,10,12,5\},\ \{10,11,0,6\},\ \{11,12,1,7\},\ \{12,0,2,8\}.\end{array}$$

To construct an affine plane of order 3, pick a block in the projective plane, say $\{0, 1, 3, 9\}$ and delete the points in this block from all other blocks. Since $\{0, 1, 3, 9\}$ intersects every other block in exactly one point, we are deleting one point from every other block. We obtain the following 12 blocks:

$$\begin{array}{l}\{2,4,10\},\ \{2,5,11\},\ \{4,6,12\},\ \{4,5,7\},\ \{5,6,8\},\ \{6,7,2\},\\ \{7,8,10\},\ \{8,11,4\},\ \{10,12,5\},\ \{10,11,6\},\ \{11,12,7\},\ \{12,2,8\}.\end{array}$$

These are the blocks of an affine plane of order 3 on the nine points 2, 4, 5, 6, 7, 8, 10, 11, 12. Note that this is a $(9, 3, 1)$-BIBD.

The above-described process can be reversed. The 12 blocks of the affine plane can be partitioned into four *parallel classes*, each of which consists of three disjoint blocks. Add a new point x_i to each block in the ith parallel class, for $1 \leq i \leq 4$. Finally, add a new block $\{x_1, x_2, x_3, x_4\}$.

A *Steiner triple system* is a $(v, 3, 1)$-BIBD. It is also denoted as STS(v). It has $r = (v-1)/2$, so r is odd. Then $b = (2r+1)r/3$, so $3|r$ or $3|2r+1$. Hence, $r \equiv 0, 1 \pmod 3$ and $v \equiv 1, 3 \pmod 6$ is a necessary condition for existence of an STS(v). We can also write $b = v(v-1)/6$.

Example: We have already constructed STS(7) and STS(9). An STS(13) has $b = 26$ blocks. It can be constructed by developing the two base blocks $\{0, 1, 4\}$ and $\{0, 2, 8\}$ modulo 13.

Theorem: An STS(v) exists for all $v \equiv 1, 3 \pmod 6$, $v \geq 7$.

A *Hadamard design* is a $(4n-1, 2n-1, n-1)$-BIBD. The Hadamard designs are is a symmetric BIBDs.

Example: We have already constructed a $(7, 3, 1)$-BIBD and a $(11, 5, 2)$-BIBD. These are Hadamard designs corresponding to $n = 2$ and $n = 3$, respectively.

Hadamard designs are known to exist for $2 \leq n \leq 166$. The smallest unknown case is a $(667, 333, 166)$-BIBD.

A *Hadamard matrix of order* $4n$ is a $4n$ by $4n$ matrix H, whose entries are all ± 1, which satisfies the property $HH^T = 4nI_{4n}$ (where I_{4n} is the identity matrix of order $4n$).

A Hadamard matrix of order $4n$ is equivalent to a $(4n-1, 2n-1, n-1)$-BIBD (i.e., a Hadamard design).

Example: We construct a Hadamard matrix of order 8 from a $(7, 3, 1)$-BIBD. Recall that the BIBD has blocks $\{0, 1, 3\}$, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 0\}$, $\{5, 6, 1\}$, $\{6, 0, 2\}$. We first construct the *incidence matrix* of the BIBD. The rows are indexed by the points, the columns are indexed by the blocks, and an entry is 1 if the given point is a member of the given block, and 0, otherwise. The incidence matrix is as follows:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Now replace all 0's by -1's and adjoin a row and column of 1's:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \end{pmatrix}.$$

The result is a Hadamard matrix of order 8.

It is a bit more complicated to construct a $(4n-1, 2n-1, n-1)$-BIBD from a Hadamard matrix of order $4n$. First, the Hadamard matrix must be modified in a suitable manner so it contains a border of 1's. Then the border can be stripped off and all -1's are changed to 0's.

2 t-designs

A t-(v, k, λ)-design is a collection of k-subsets (called *blocks*) of a v-set (whose elements are called *points*), such that every t-subset of points is in exactly λ blocks. If $t = 2$, we have a BIBD.

A *Steiner quadruple system* is a 3-$(v, 4, 1)$-design. It is also denoted as SQS(v). An SQS(v) exists if and only if $v \equiv 2, 4 \pmod 6$.

Example: We construct an SQS(8). We start with two blocks: $\{1,2,3,4\}$ and $\{5,6,7,8\}$. Next we divide these blocks into pairs as follows:

$$\begin{array}{c||c||c} \{1,2\} & \{1,3\} & \{1,4\} \\ \{3,4\} & \{2,4\} & \{2,3\} \\ \hline \{5,6\} & \{5,7\} & \{5,8\} \\ \{7,8\} & \{6,8\} & \{6,7\} \end{array}$$

Now we form 12 blocks as follows:

$$\begin{array}{c||c||c} \{1,2,5,6\} & \{1,3,5,7\} & \{1,4,5,8\} \\ \{1,2,7,8\} & \{1,3,6,8\} & \{1,4,6,7\} \\ \{3,4,5,6\} & \{2,4,5,7\} & \{2,3,5,8\} \\ \{3,4,7,8\} & \{2,4,6,8\} & \{2,3,6,7\} \end{array}$$

These 12 blocks, along with the original two blocks, form the desired SQS(8).

The preceding construction can be generalized to show that an SQS($2v$) can be obtained from an SQS(v).

Another infinite class of 3-designs are the *inversive planes*, which are 3-$(n^2+1, n+1, 1)$-designs. These designs are known to exist if n is a prime power.

If we fix a point x in an inversive plane, delete all blocks that do not contain x, and then delete x from all the remaining blocks, we get an affine plane.

Very few explicit examples of t-designs with $t \geq 4$ are known. However, a result of Keevash from 2014 shows that t-$(v, k, 1)$-design exist for all t, albeit with enormously large values of v.