11 Block Designs

Linear Spaces

In this section we consider incidence structures $\mathcal{I} = (\mathcal{V}, \mathcal{B}, \sim)$. By convention, we shall always let $v = |\mathcal{V}|$ and $b = |\mathcal{B}|$.

Linear Space: We say that an incidence structure $(\mathcal{V}, \mathcal{B}, \sim)$ is a *linear space* if every line contains at least two points and every pair of points are contained in exactly one line.

Theorem 11.1 (De Bruijn & Erdös) *For every linear space either $b = 1$ or $b \geq v$. Further, equality implies that for any two lines there is exactly one point contained in both.*

Proof: For any point $x \in \mathcal{V}$ we let r_x denote the number of blocks incident with x and for any line $B \in \mathcal{B}$ we let k_ℓ denote the number of points contained in B. Assume there is more than one line and let $x \in \mathcal{V}$ and $B \in \mathcal{B}$ satisfy $x \notin B$. Then $r_x \geq k_B$ since there are k_B lines joining x to the points in B. If we suppose that $b \leq v$ then $b(v - k_B) \geq v(b - r_x)$ and thus

$$1 = \sum_{x \in \mathcal{V}} \sum_{B \not\ni x} \frac{1}{v(b - r_x)} \geq \sum_{B \in \mathcal{B}} \sum_{x \notin B} \frac{1}{b(v - k_B)} = 1$$

Now we must have equality in the above equation, so $v = b$ and $r_x = k_B$ if $x \notin B$. □

Designs

Designs: Let v, k, t, λ satisfy $v \geq k \geq t \geq 0$ and $\lambda \geq 1$. A t-(v, k, λ) *design*, also called a $S_\lambda(t, k, v)$ is an incidence structure $(\mathcal{V}, \mathcal{B}, \sim)$ which satisfies:

(i) $|\mathcal{V}| = v$

(ii) $|B| = k$ for every $B \in \mathcal{B}$.

(iii) For every set $T \subseteq \mathcal{V}$ with $|T| = t$ there are exactly λ blocks containing all points in T.

We call k the *block size* and λ the *index*. We say that a t-(v, k, λ) design is a t-design for short. Although we shall not use the term, it is common to call a 2-design a Balanced Incomplete Block Design (BIBD).

Examples:

1. The vertices and edges of K_n form a 2-$(n, 2, 1)$ design.

2. Every projective plane of order n is a 2-$(n^2 + n + 1, n + 1, 1)$ design.

3. Every affine plane of order n is a 2-$(n^2, n, 1)$ design.

4. Let H be a Hadamard matrix of order $4k$ where every entry in the first row is $+$ and let $\mathcal{V}$ be the columns of this matrix. Now each row other than the first has $2k$ copies of $+$ and $2k$ copies of $-$ so this determines two subsets of $\mathcal{V}$ of size $2k$ each of which we define to be a block. This yields a 3-$(4k, 2k, k-1)$ design called a Hadamard 3-design. To see this, note that for any three columns we can normalize the first to be all $+$, then it follows from the orthogonality relations that the patterns $++, +-, -+, --$ are equally likely over the other two columns.

5. Let the group G act t-homogeneously on the set $\mathcal{V}$ and let $B \subseteq \mathcal{V}$ satisfy $|B| \geq t$. Setting $\mathcal{B} = B^G = \{g(B) : g \in G\}$ yields a t-design.

Proposition 11.2 *Let $J \subseteq \mathcal{V}$ satisfy $|J| = j \leq t$. Then the number of blocks containing J is*

$$b_j = \lambda \binom{v-j}{t-j} \Big/ \binom{k-j}{t-j}$$

(which depends only on $|J|$). In particular, every t-design is also a j-design for all $j \leq t$.

Proof: If b_j is the number of blocks containing J, then counting the number of pairs (T, B) with $B \in \mathcal{B}$ and $J \subseteq T \subseteq B$ with $|T| = t$ in two ways we find $b_j \binom{k-j}{t-j} = \binom{v-j}{t-j} \lambda$. □

Corollary 11.3 *The number of blocks in a t-(v, k, λ) design is*

$$b = b_0 = \lambda \binom{v}{t} \Big/ \binom{k}{t}$$

Replication Number: The replication number, denoted $r = b_1$, is the number of blocks which contain a fixed vertex.

Corollary 11.4 *For every 2-design*

(i) $bk = vr$

(ii) $\lambda(v-1) = r(k-1)$

Proof: Counting the number of incident pairs (x, B) where $x \in \mathcal{V}$ and $B \in \mathcal{B}$ in two ways yields (i). For (ii) simply apply the previous proposition with $t = 2$ and $j = 1$. $\square$

Steiner Systems: We let $S(t,k,v) = S_1(t,k,v)$ and call such designs *Steiner Systems*. A *Steiner Triple System* is a $S(2,3,v)$ and we refer to such designs as $STS(v)$.

Theorem 11.5 *A* $STS(v)$ *exists if and only if* $v \equiv 1, 3 \pmod 6$.

Proof: First suppose that a $STS(v)$ exists. Then it follows from (ii) of Corollary 11.4 that $v - 1 = 2r$ (so v is odd) and then from (i) of the same corollary that $3b = vr = \frac{v(v-1)}{2}$ so either v or $v - 1$ is a multiple of 3. Thus $v \equiv 1, 3 \pmod 6$ as desired.

The proof of the other direction is constructive, and we do just the case $v \equiv 3 \pmod 6$. Let $v = 6t + 3$ and set $n = 2t + 1$. We set $\mathcal{V} = \mathbb{Z}_n \times \mathbb{Z}_3$. Now, for every $x \in \mathbb{Z}_n$ we let $\{(x,0),(x,1),(x,2)\}$ be a block and whenever $x, y \in \mathbb{Z}_n$ with $x \neq y$ and $i \in \mathbb{Z}_3$ we let $\{(x,i),(y,i),(\frac{1}{2}(x+y), i+1)\}$ be a block.

Incidence Matrix: If $\mathcal{I} = (\mathcal{V}, \mathcal{B}, \sim)$ is an incidence structure, the *associated incidence matrix* is the matrix N indexed by $\mathcal{V} \times \mathcal{B}$ with the property that the (x, B) entry is 1 if $x \in B$ and 0 otherwise.

Observation 11.6 *If* N *is the incidence matrix of a* 2*-design then*

$$NN^\top = (r - \lambda)I + \lambda J$$

Theorem 11.7 (Fisher's Inequality) *Every* 2-(v,k,λ) *design with* $v > k$ *satisfies* $b \geq v$.

Proof: It follows from (ii) of Corollary 11.4 and $v > k$ that $r > \lambda$. Since J has one eigenvalue v and all others 0, the matrix $(r-\lambda)I + \lambda J$ has one eigenvalue $r - \lambda + \lambda v = rk$ and all other eigenvalues $r - \lambda$. It follows that $NN^\top$ is invertible, so $b \geq v$. $\square$

Square Design: We say that a design is *square* if $v = b$. This is usually given the unfortunate term: symmetric design. Note that if a design is square, then it follows from Corollary 11.4 that $r = k$.

Corollary 11.8 *For every square (symmetric) 2-design with v even, $k - \lambda$ is a square.*

Proof: Setting N to be the incidence matrix and using the eigenvalue argument from Fisher's Inequality we have

$$(\det N)^2 = \det(NN^\top) = (r - \lambda)^{v-1}(rk) = (k - \lambda)^{v-1}k^2$$

Now, since $v - 1$ is odd, it must be that $k - \lambda$ is a square. $\square$

Bruck-Ryser-Chowla

Theorem 11.9 (Bruck-Ryser-Chowla) *For every square (symmetric) 2-design with v odd, the following equation has a nonzero integral solution:*

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

Proof: Let $N = \{n_{ij}\}_{1\le i,j\le v}$ be the incidence matrix of the design and let $x = (x_1, x_2, \ldots, x_v)$ be a vector of variables. We define the linear forms $L_i = \sum_{j=1}^{v} n_{ij}x_j$ (so L_i is the i^{th} entry of Nx. Setting $m = k - \lambda$ we have $NN^\top = mI + \lambda J$. Multiplying on the left by $x^\top$ and on the right by x yields the following equation:

$$L_1^2 + L_2^2 \ldots + L_v^2 = m(x_1^2 + x_2^2 + \ldots x_v^2) + \lambda(x_1 + x_2 \ldots + x_v)^2 \tag{1}$$

Now, express m as $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and consider the four variables x_1, x_2, x_3, x_4. Using the quaternions, we let

$$y_1 + y_2 i + y_3 j + y_4 k = (a_1 + a_2 i + a_3 j + a_4 k)(x_1 + x_2 i + x_3 j + x_4 k)$$

so each y_s is linear in the variables $x_1 \ldots x_4$ and $y_1^2 + y_2^2 + y_3^2 + y_4^2 = m(x_1^2 + x_2^2 + x_3^2 + x_4^2)$. Now, assume that $v \equiv 1 \pmod 4$ and repeat this process four variables at a time by introducing new variables $y_{4s+1}, y_{4s+2}, y_{4s+3}, y_{4s+4}$ which are linear in $x_{4s+1}, x_{4s+2}, x_{4s+3}, x_{4s+4}$. Now, adding a new variable $w = x_1 + x_2 + \ldots x_v$ permits us to rewrite the above equation as

$$L_1^2 + L_2^2 + \ldots L_v^2 = y_1^2 + y_2^2 + \ldots y_{v-1}^2 + mx_v^2 + \lambda w^2$$

Since the product structure on the quaternions is invertible, we can express $x_1, x_2, \ldots, x_{v-1}$ as linear forms in $y_1, y_2, \ldots, y_{v-1}$. If the linear form L_1 expressed in terms of $y_1, y_2, \ldots, y_{v-1}, x_v$

does not have coefficient 1 for y_1 then set $L_1 = y_1$ and use this to solve for y_1 in terms of the remaining variables y_t and x_v. Otherwise, we set $L_1 = -y_1$ and use this to solve for y_1 in terms of the remaining variables. In either case we can now rewrite our equation as

$$L_2^2 + \dots L_v^2 = y_2^2 + \dots y_{v-1}^2 + mx_v^2 + \lambda w^2$$

(where we update w to be a linear combination of the new variables y_t and x_v). Continuing in this manner for $y_2, \dots y_{v-1}$ we can reduce the original equation to

$$L_v^2 = mx_v^2 + \lambda w^2$$

Where both L_v and w are rational multiples of x_v. Multiplying through by a common denominator brings us an integer equation of the form

$$z^2 = (k - \lambda)x^2 + \lambda y^2$$

as desired. The case when $v \equiv 3 \pmod 4$ is handled in a similar manner. We introduce a new variable x_{v+1} and add mx_{v+1}^2 to both sides of equation (1). Now our reductions bring us to

$$mx_{v+1}^2 = y_{v+1}^2 + \lambda w^2$$

and then multiplying by a common denominator yields the desired result. □

The Small Witt Design

$\mathbf{W_{12}}$: Let $\Omega = PG(1, \mathbb{F}_{11}) = \mathbb{F}_{11} \cup \{\infty\}$ and let $B = \mathbb{F}_q \cup \{\infty\} = \{1, 3, 4, 5, 9, \infty\}$. Now we define the *Small Witt Design*, W_{12}, to be the incidence structure with point set Ω and blocks $\{g(B) : g \in PSL(2, 11)\}$ (with the natural containment as incidence).

A Matthieu Group: We define $M_{12} = Aut(W_{12})$.

Theorem 11.10 *M_{12} acts sharply 5-transitively on the points of W_{12}.*

Complements: Note that the map ϕ given by $\phi(s) = -\frac{1}{s} \in PSL(2, 11)$. Furthermore, $\phi(B) = \{0, 2, 6, 7, 8, X\}$ (here we use X instead of 10). Since $\phi(B)$ and B are complementary subsets of $\mathbb{F}_{11} \cup \{\infty\}$, it follows that the complement of every block of W_{12} is another block of W_{12}.

3-Homogeneous: Note that $PSL(2,11)$ acts 3-homogeneously on $\mathbb{F}_{11} \cup \{\infty\}$.

Distinguishing $\{\infty, 0, 1\}$: Since W_{12} is 3-homogenous, every three element set is equivalent under the symmetry group, and we may (without loss) distinguish the three element set $\{\infty, 0, 1\}$. If we do so, we find that the remaining points form a structure isomorphic to $AG(2,3)$ as follows:

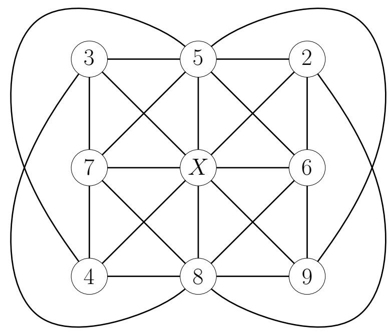

Figure 1: *Our* $AG(2,3)$

The Blocks of $\mathbf{W_{12}}$: The following table indicates some of the types of blocks B in W_{12} relative to their intersection with $\{\infty, 0, 1\}$. Here the lines of our $AG(2,3)$ are indicated in the figure, and fall into the four parallel classes which we denote as follows:

—	the parallel class of $\{7, X, 6\}$
$\vert$	the parallel class of $\{5, X, 8\}$
∕	the parallel class of $\{4, X, 2\}$
∖	the parallel class of $\{3, X, 9\}$

$\mathbf{B \cap \{\infty, 0, 1\}}$	**Description of block B**
$\{\infty, 0, 1\}$	The union of $\{\infty, 0, 1\}$ with a line in our $AG(2,3)$.
$\emptyset$	The union of two parallel lines in our $AG(2,3)$.
$\{\infty\}$	The union of $\{\infty\}$ with two lines in our $AG(2,3)$ with parallel types either {—, $\vert$} or {∕, ∖}.
$\{0\}$	The union of $\{0\}$ with two lines in our $AG(2,3)$ with parallel types either {—, ∖} or {$\vert$, ∕}.
$\{1\}$	The union of $\{1\}$ with two lines in our $AG(2,3)$ with parallel types either {—, ∕} or {$\vert$, ∖}.

Note that although we have not explicitly listed the types of blocks whose intersection with $\{\infty, 0, 1\}$ has size two, each such block is a complement of one that we have listed. In the figure below, we have labelled an edge with $\infty, 0, 1$ if the union of two edges from these parallel classes with the given label form a block.

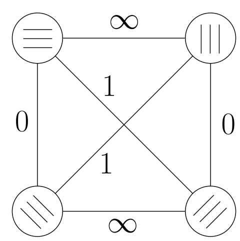

Figure 2: *Edge-Colouring of Slopes*

Fixing $\{\infty, 0, 1\}$: Let ϕ be an automorphism of our $AG(2,3)$. Now, ϕ gives a permutation of the four parallel classes —, |, ⁄, and ∖ and thus permutes the perfect matchings of the graph in the above figure. Since these perfect matchings are labelled with either $\infty, 0, 1$ it follows that ϕ also induces a permutation of $\{\infty, 0, 1\}$. It then follows from our table of block structures that extending ϕ by this permutation of $\{\infty, 0, 1\}$ gives an automorphism of W_{12}. Thus

$$G_{\{\infty,0,1\}} \cong Aut(AG(2,3)) \cong AGL(2,3).$$

Coordinates: We now equip our $AG(2,3)$ with coordinates by assigning X to be $(0,0)$ (the origin) and assigning each other point a vector (a,b) where $a,b \in \{-1,0,1\}$ according to their position in Figure 1. So, for instance $3 = (-1,-1)$. Note that this gives coordinates to our parallel classes as well: — is the set of lines parallel to $(0,1)$, | is the set of lines parallel to $(1,0)$, ⁄ is the set of lines parallel to $(1,1)$ and ∖ is the set of lines parallel to $(1,-1)$.

3-transitivity: Consider the automorphism ϕ of $GL(2,3)$ given by $\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$. This fixes the parallel class $(1,0)$ but permutes the other three cyclically. It follows that ϕ extends to an automorphism of W_{12} which permutes $\infty, 0, 1$ cyclically. The automorphism ψ of $GL(2,3)$ given by $\begin{bmatrix} x \\ y \end{bmatrix} \to \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ fixes the parallel classes $(1,1)$ and $(1,-1)$ but interchanges $(0,1)$ and $(1,0)$. It follows that ψ extends to an automorphism of W_{12}

which fixes 1 but interchanges $0, \infty$. Together, these two automorphisms show that $G_{\{\infty,0,1\}}$ acts 3-transitively on $\{\infty, 0, 1\}$. It now follows from the 3-homogeneousness of G that G is 3-transitive.

4-transitivity: The group of translations of $AG(2,3)$ act transitively on the points, and do not change any of the slopes. It follows that any translation of $AG(2,3)$ extends to an automorphism of W_{12} which fixes $\infty, 0, 1$. It follows from this that G acts 4-transitively.

5-transitivity: Now we restrict our attention to those elements of G which fix $\infty, 0, 1, X$. These are elements of $AGL(2,3)$ which fix the origin X (so have the form $\vec{x} \to A\vec{x}$ for some $A \in GL(2,3)$) and permute the four slopes according to the cycle pattern $(\cdot\cdot)(\cdot\cdot)$. All of the following matrices have this property:

$$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \pm \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \quad \pm \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

Naming the matrices above as $\pm 1, \pm i, \pm j, \pm k$ we see that these four matrices form a multiplicative subgroup which is isomorphic to the finite quaternion group. If we group each of the elements in $\mathbb{F}_3^2 \setminus \{0\}$ into pairs of opposite elements:

$$\{\pm(1,0)\}, \{\pm(0,1)\}, \{\pm(1,1)\}, \{\pm(-1,1)\}$$

We see that each of i, j, k acts on the above pairs with cycle pattern $(\cdot\cdot)(\cdot\cdot)$ in all three possible ways. Since the -1 matrix takes each element to its opposite, it then follows that this group of 8 matrices acts transitively on the 8 points of $\mathbb{F}_3^2 \setminus \{0\}$. Thus, G acts 5-transitively.

Sharp 5-transitivity: We have from above that $|G_{\{\infty,0,1\}}| = |AGL(3,2)| = 48 \cdot 9 = 2^4 3^3$ and then $|G_{(\infty,0,1)}| = 2^3 3^2$, $|G_{(\infty,0,1,X)}| = 2^3$ and $|G_{(infty,0,1,X,2)}| = 1$. Thus G acts sharply 5-transitively on $PG(1, \mathbb{F}_{11})$.

Note: Consider a block B of W_{12} and the subgroup of automorphisms which fix B. It follows immediately from the sharp 5-transitivity that this subgroup is isomorphic to S_6. However, an automorphism which fixes four elements in B and interchanges the other two cannot yield a similarly structured permutation on its complement. It follows that the action of this subgroup on B and its complement are related by an outer automorphism of S_6.