An Introduction to (block) design theory

Wednesday 8th May 2013

Abstract

A (block) design is a set together with a collection of subsets that satisfy certain regularity conditions. Although easy to define and parametrise, designs play an important role in many areas of mathematics including geometry and group theory.

In this talk, the basic notions of design theory will be introduced and illustrative examples will be given. The importance of one such design - the Steiner system $S(5, 8, 24)$ - will be explained. If time permits, applications to coding theory will be discussed.[1]

1 Projective Planes

Everybody is familiar with the idea of a projective plane, and $\mathbb{RP}^2$ is one of the first topological spaces that many people consider in a course on topology, but what exactly do we mean by a projective space. In fact what do we mean by an affine space? To define these, we need to consider incidence structures known as geometries[2]:

Definition 1 *A geometry $S = (P, L)$ is a non-empty set P whose elements are called* points*, together with a set L of non-empty subsets of P called* lines *satisfying:*

(G1) For any two distinct points $p_1, p_2 \in P$, there exists exactly one line $l \in L$ such that both $p_1 \in l$ and $p_2 \in l$.

(G2) There exists a set of four points, such that given any set of three of these points, no line exists that contains all three points. We call such a set of points a quadrangle

So Axiom (G1) says that any two points are incident to a unique line, whilst Axiom (G2) asserts that there are 4 points no three of which are incident to a given line.

Example 2 *One of the easiest classes of examples is given by the complete graph K_n for $n \geq 4$, with the point set taking the form of $V(K_n)$ and the line set being $E(K_n)$.* •

[1] The material for Sections 1 is taken from [GGL95], the material from Section 2 is taken from [Gro10] and [GGL95] and the material for Section3 is taken from [GGL95].

[2] Geometries should not be confused with geometries over a set Δ. These are defined as follows: **Definition:** A *geometry over a set* Δ is a triple $(\Gamma, *, \tau)$, where;

- Γ is a set (the *elements* of Γ);
- $*$ is a symmetric relation on Γ (the *incident relation* of Γ);
- $\tau : \Gamma \twoheadrightarrow \Delta$ is a surjective map (the *type function* of Γ).

such that if $x, y \in \Gamma$ and $x * y$, then $\tau(x) \neq \tau(y)$

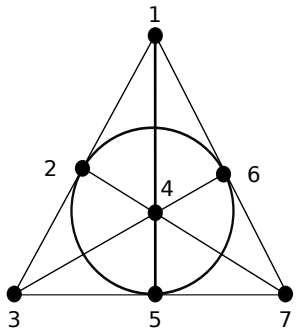

Figure 1: The Fano Plane

We now define affine spaces and projective spaces in terms of geometries:

Definition 3 *(i) A geometry, A, satisfying the additional condition that for any line l, and any point p not on l, there exists a unique line l on p that does not intersect l is called an* affine plane.[3]

(ii) A geometry, P, satisfying the additional condition that any two lines intersect in a unique point is called a projective plane.

From this point forwards we will restrict our attention to the world of finiteness. The most famous example of a finite projective plane is given when $P = \{1, \ldots, 7\}$ and $L = \{l_1 \ldots, l_7\}$ where $l_1 = \{1, 2, 3\}$, $l_2 = \{1, 4, 5\}$, $l_3 = \{1, 6, 7\}$, $l_4 = \{2, 4, 7\}$, $l_5 = \{3, 4, 6\}$, $l_6 = \{3, 5, 7\}$ and $l_7 = \{2, 5, 6\}$, as shown in Figure 1. This projective plane is know as the *Fano plane*.

The following combinatorial result summarises the situation with projective planes:

Theorem 4 *Let Π be a projective plane. Then the following conditions hold:*

(i) If l is a line of Π and p is a point of Π not on l, then l has exactly $n+1$ points for some integer n if and only if there are $n+1$ points on p.

(ii) Each point of Π is on $n+1$ lines and each line of Π is on $n+1$ points.

(iii) The number of points of Π is $n^2 + n + 1$.

We note that the integer n is known as the *order* of Π.

Proof: (i): Since every line on p intersects l in a unique point (by (ii)), the number of lines on p is equal to the number of points on l.

(ii): Let $p_1, \ldots, p_4$ be a quadrangle of Π. Let $n > 1$ be the number of lines on p_1. As $p_1, \ldots, p_4$ form a quadrangle, we may apply (i) to see that each of the lines p_2p_3, p_3p_4 and p_2p_4 are on exactly $n+1$ points. Then for any point $q \in \Pi$, q will not be on one of these lines. Hence by (i), there are exactly $n+1$ lines on q.

[3]This is simply Euclid's parallel postulate.

To obtain the result for lines, just interchange lines and points in the above argument.

(iii): There are $n+1$ lines on p each of which contains n points other than p. Since every point of Π is on such a line, we have that the number of points of Π is $n(n+1)+1 = n^2+n+1$. □

It follows that the Fano Plane is a smallest projective plane, and is actually *the* smallest projective plane.

Considering the situation above, we see that for an arbitrary finite projective plane P of order n, we have n^2+n+1 points and a collection of subsets of these points each of size $n+1$, such that each pair of points is contained in a unique subset. A (block) design is a generalisation of this notion.

2 Block Designs

2.1 Setting the scene

Designs arose initially in statistics and in the theoretical study of the design of experiments in agriculture by Sir Ronald Fisher FRS (1890-1962). Indeed, as a basic example, Fisher described how to test the hypothesis that a certain lady could distinguish by flavour alone whether the milk or the tea was first placed in the cup. [Fis35]. We begin with the most general of formal definitions:

Definition 5 *A* (block) design *is a pair* $(X, \mathcal{B})$ *where* X *is a set (the* point set*) and* $\mathcal{B}$ *(the* family of blocks*) is a collection of subsets of* X *satisfying a regularity condition.*

So we may think of a design as a generalisation of a multigraph - indeed, this is a good example to keep in mind. However, any subset of $\mathcal{P}(X)$ - the power set of X can be a design. We call a design *simple* if no two blocks of the design are identical. If $x \in X$, then the *valence* of x or *replication number of* x is the number of bloacks of $\mathcal{B}$ containing x, and is sometimes denoted $r(x)$ or r_x. If $r(x)$ is constant for all $x \in X$, then we call our design regular (generalising the notion of a regular graph). If $x, y \in X$, then the *covalence of the pair* x, y is the number of blocks of $\mathcal{B}$ containing both x and y. So for a multigraph, the valence of x is the valency of the vertex x and the covalence of the points x and y will be the number of edges from x to y. At this point we note that to obtain graphs with loops, we would either need to reformulate our definition to allow blocks to be multisets, or we would need to have our blocks as sets of size 1 and 2, and then to identify the singleton set $\{x\}$ with a loop at the vertex x.

Usually we consider regularity conditions as given above for finite projective planes. This gives rise to designs given by four parameters:

Definition 6 *A* t-(v, k, λ)*-design is a block design on a set* X *of cardinality* v*, such that every block has cardinality* k*, and every set of* t *points is contained in precisely* λ *blocks.*

We see that a finite projective plane of order n is a 2-$(n^2+n+1, n+1, 1)$ design. We call the integer k the *blocksize* of our design.

The most commonly studied types of design are *balance incomplete block designs* (or *BIBD*'s for short). These are just 2-(v, k, λ) designs, where the incompleteness asserts that $k < v$ (so X is not a block of our design). In other words, the valence of any two points of the design is equal to λ. Sometimes the incompleteness assertion is dropped from the definition.

2.2 Constructing Designs

We have seen above that there are many examples of designs, including power sets, multigraphs and projective planes. However, for given integers t, v, k and λ, does there exist a t-(v, k, λ) design. In general this is a very difficult problem to address, especially in the case that t is large. However, we will consider two approaches to constructing designs:

2.2.1 Constructions using group actions

Let Ω be a set of v points and let B be a k-subset of Ω. Take $G = \mathrm{Sym}(\Omega)$ - the symmetric group on Ω. Then by allowing G to act on Ω, and considering the G-orbit of B, we arrive at a t-(v, k, λ) design, where the value of λ is determined by the value of t and vice versa.

Example 7 *Let $\Omega = \{1, \ldots, 7\}$ and let $B = \{1, 2, 3\}$ a 3-set. Then the orbit of Ω is just the set of all 3-subsets of Ω. Thus*

$$(t, \lambda) \in \{(1, 15), (2, 5), (3, 1)\}.$$

•

Indeed, we see that such a construction will always result in a t-$(v, k, \binom{v-t}{k-t})$ design. More generally, we may take G to be any group that acts t-transitively on Ω. This will give a t-(v, k, λ) design, where now the value of λ will depend entirely on the group action. If the action is simply t-transitive, then clearly $\lambda = 1$.

This idea can be generalised by combining more than one G-orbit. In such a situation the condition on t-transitivity is no longer required.

2.2.2 New designs from old designs

If we have a t-(v, k, λ) design, then we may construct "smaller" designs quite easily. Indeed suppose that $\mathcal{D} = (X, \mathcal{B})$ is a t-(v, k, λ) design and that $x \in X$. Then we may construct the *derived design at x*, denoted $\mathcal{D}_x$, by considering all blocks of $\mathcal{D}$ that contain x, and removing x from them, so

$$\mathcal{D}_x = (X \setminus \{x\}, \{B \setminus \{x\} | x \in B \in \mathcal{B}\}).$$

We may also define the *residual design* at x, denoted $\mathcal{D}^x$, by just considering those blocks of $\mathcal{D}$ that do not contain x:

$$\mathcal{D}^x = (X \setminus \{x\}, \{B | x \notin B \in \mathcal{B}\}).$$

We see that $\mathcal{D}_x$ is a $(t-1)$-$(v-1, k-1, \lambda)$ design, whilst it can be shown that $\mathcal{D}^x$ is a $(t-1)$-$(v-1, k, \lambda(\frac{v-t+1}{k-t+1}-1))$ design.

Building a "larger design" from a given design is more difficult. In 1975, William Alltop proved that if t was even, then by adding a new point ∞ to the blocks of any t-$(2k+1, k, \lambda)$ design, and also adding the complements of all blocks, then you obtain a $(t+1)$-$(2k+2, k+1, \lambda)$ design. [All75]

Tran van Trung also proved that if there exists a t-(v, k, λ) design, and λ is not too large[4], then there exists a t-$(v+1, k, (v+1-t)\lambda)$ design. [vT84].

3 Steiner Systems

A specific type of block design is given when $\lambda = 1$. We call such designs *Steiner systems* and denote a t-$(v, k, 1)$ design by $S(t, k, v)$. We see that any finite projective plane is a Steiner system having the form $S(2, n+1, n^2+n+1)$ for some $n \geq 2$.

One of the most important Steiner systems is the *Witt design*. This is the unique $S(5, 8, 24)$ Steiner system. To construct it, we first construct the *extended binary Golay code*. Before doing so, we recall a few definitions about codes.

Definition 8 *Let V be a vector space over a field $\mathbb{F}_q$.*

(a) A code *is a subset of V and a* linear code *is a subspace of V.*

(b) For $u, v \in V$, we define the Hamming distance *$d_H(u, v)$ to be the number of coordinates in which u and v differ. The weight of v is defined to be $d_H(\mathbf{0}, v)$ and the* minimum distance *of a code $\mathcal{C}$ is defined to be $\min\{d_H(u, v) | u, v \in \mathcal{C}\}$.*

(c) The support *of a vector is the set of coordinate positions where it has a nonzero coordinate.*

To construct the extended binary Golay code, write the elements of $\mathbb{F}_2^{24}$ in ascending order, and delete those elements v such that $d_H(u, v) < 8$ for some u previously defined. So the first few elements will be

$$\begin{array}{cccccccccccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0
\end{array}$$

[4]Indeed, in his paper [vT84] he stated the following:

> Let I be an i-subset of X and let λ_i be the number of blocks in $\mathcal{B}$ which contain I. It is well known that
>
> $$\lambda_i = \lambda\binom{v-i}{t-i}/\binom{k-i}{t-i}.$$
>
> **Theorem A.** If there exists a $t-(v, k, \lambda)$ design with $v \cdot \lambda_0(\lambda_0 - \lambda_1) < \binom{v}{k}$, then there exists a $t-(v+1, k, (v+1-t)\lambda)$ design.

It can be shown (but not in this seminar!) that this is the unique code (up to isomorphism) of length 24, over $\mathbb{F}_2$ having 4096 codewords and minimum distance 8. This gives the extended binary Golay code.

From this, we may construct an $S(5, 8, 24)$ Steiner system by taking $X = \{1, \ldots, 24\}$ and considering our blocks to be the support of those codewords $u \in \mathcal{C}$ such that $d_H(\mathbf{0}, u) = 8$. By definition our blocks have size 8 and no 5-subset of X can be contained in two distinct blocks. Moreover, there are 759 blocks in total, each of which will contain $\binom{8}{5}$ subsets of size 5. Since $\binom{24}{5} = 759 \cdot \binom{8}{5}$, and no 5-set is contained in more than one block, it follows that each 5-set is contained in a unique block, and hence we have a Steiner system as claimed.

The importance of $S(5, 8, 24)$ is that it's automorphism group (so the group of all permutations of $\{1, \ldots, 24\}$ that map blocks to blocks), is the sporadic simple group M_{24}. Morover, the Steiner system also encodes the other large Mathieu groups:

(i) M_{23} is the set of all automorphisms of $S(5, 8, 24)$ that also fix a point (i.e. the stabiliser of a point in M_{24}).

(ii) M_{22} is the set of all automorphisms of $S(5, 8, 24)$ that fix two points pointwise (i.e. the stabiliser of a point in M_{23}).

It can also be shown that there is a unique Steiner System $S(5, 6, 12)$. The automorphism group of this system is the Matheiu group M_{12}, whilst the point stabiliser of M_{12} is M_{11}. Thus two Steiner systems give rise to 5 of the 26 sporadic simple groups. Other sporadic simple groups - such as the Conway groups - are formed from the Leech Lattice, which is closely connected with $S(5, 8, 24)$. Thus Steiner systems and designs, can be seen at the heart of parts of the classification of finite simple groups - the most profound proof in the history of mathematics!

References

[All75] W. O. Alltop. Extending t-designs. *Journal of Combinatorial Theory*, A(18):177–186, 1975.

[Fis35] R.A. Fisher. *The Design of Experiments*. Macmillan, 9th edition, 1935.

[GGL95] R.L. Graham, M. Grotschel, and L. Lovasz. *Handbook of Combinatorics*, volume 1. Elsevier Science, Amsterdam, The Netherlands, 1995.

[Gro10] J. L. Gross. Combinatorial designs. January 2010.

[vT84] Tran van Trung. On the existence of an infinite family of simple 5-designs. *Mathematische Zeitschrift*, 187(2):285–287, 1984.