Math 155r - Combinatorics: Designs and Groups

Taught by Noam D. Elkies
Notes by Dongryul Kim

Spring 2016

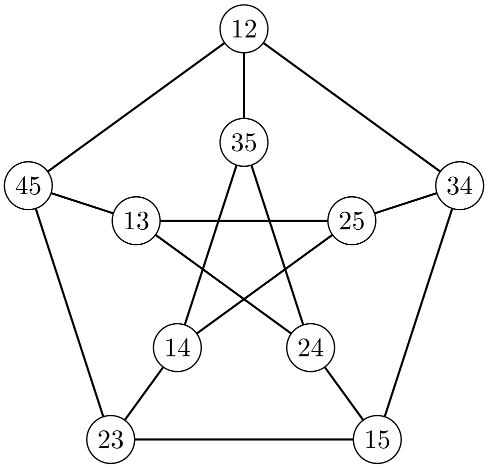
Contents

1 January 25, 2016

There are almost no prerequisites. Only basic knowledge in linear algebra and some group theory (such as the notion simple groups) is assumed. It is encouraged to collaborate, but you must write down the solutions by yourself. There will going to be two exams and one final project.

1.1 Example of a graph

Let us look at a graph. By a graph, I mean a set of vertices and edges connected the vertices.



This is called a Peterson graph. We can observe that the degrees of vertices are all 3. Also, we see that the length of the minimal cycle, which is called the girth, is 5. Also, the diameter, which is the farthest distance two vertices can be apart, is 2.

We can generalize this property.

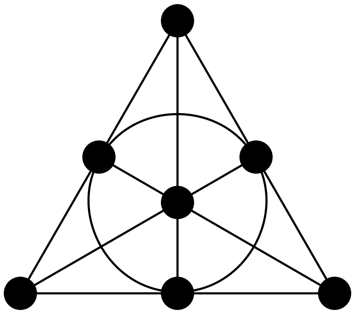
Definition 1.1. A **Moore graph** of degree d is a regular graph of degree d that has girth 5 and diameter 2.

In fact, there can be a Moore graph of degree d only for $d = 2, 3, 7, 57$. The Moore graph of degree 2 is a 5-cycle, of degree 3 is the Petersen graph, of degree 7 is the Hoffman-Singleton graph, and it is an open question whether there is a Moore graph of degree 57.

There is a nice construction for Petersen graph. We take all size 2 subsets of $\{1, 2, 3, 4, 5\}$ and connect two sets if and only if they are disjoint. It follows that there are $\binom{5}{2} = 10$ edges, and each vertex have degree $\binom{3}{2} = 3$. In fact, the automorphism group of the Petersen graph is S_5, which can be seen as permuting the labels.

1.2 Example of a design

We now look at another combinatorial structure.

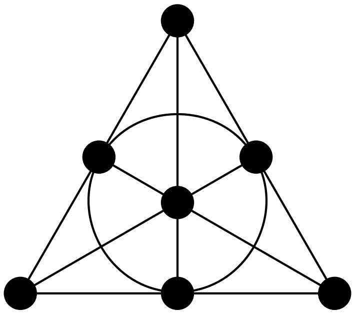


Each point is contained in exactly three lines, and each line contains exactly three points. (The circle actually a line.) Also, each two lines meet at a single point, and any two points determine a unique line. In fact, it is a finite projective plane of order 2. Then the automorphism group will be $GL_2(3)$ which has order 168. In fact, this is isomorphic to $PSL_2(7)$.

We can alternatively require that each line contains q points and each point passes through q lines. Then this is called a finite projective plane of order q. Of course, if q is a power of a prime, then there is a finite field of order q and hence such a projective plane exists, but it is a long-standing conjecture that a projective plane exists only if q is a prime power.

2 January 27, 2016

We will start by defining a block design, which generalized what I called Π_2 last time.



There are 7 points, each point is in 3 lines, each line contains 3 points, each pari of points determine 1 line, each pari of lines intersect at 1 point.

2.1 Block design

Definition 2.1. A $t-(v,k,\lambda)$ **design** is an ordered pair $(X,\mathcal{B})$ where X is the set of v points and $\mathcal{B}$ is the set of k-element subsets (or blocks), such that any t point is contained in λ blocks.

Example 2.2. The Π_2 is a $2-(7,3,1)$ design. It is also a $1-(7,3,3)$ design and a $0-(7,3,7)$ design.

Example 2.3. The cards of the game Set is a $2-(81,3,1)$ design. It is the set $\mathbb{F}_3^4$ where designs are sets of 3 element that add to zero.

Example 2.4. We can let $\mathcal{B}$ be the all k-element subsets of X. This is called the complete design, and it is a design with $\lambda = \binom{v-t}{k-t}$. We will avoid this design.

If $\lambda = 1$, we call a $t-(v,k,\lambda)$ design a **Steiner system** $S(t,k,v)$. If $t=0$ or $t=1$, it is not interesting. In fact, constructing a design become harder if t grows.

2.2 Some properties of designs

Theorem 2.5. *Any $t-(v,k,\lambda)$ design is automatically an $s-(v,k,\lambda_s)$ design for all $s \le t$, where*

$$\lambda_s = \left(\binom{v-s}{t-s}\Big/\binom{k-s}{t-s}\right)\lambda.$$

Proof. We just double count the cardinality

$$\#\{(T,B) : B \in \mathcal{B}, |T| = t, S \subseteq T\}$$

for a fixed set S with size s. Then we get

$$\# = \binom{v-s}{t-s}\lambda = \#\{B : S \subseteq B\} \cdot \binom{k-s}{t-s}.$$

This finishes the proof. □

Using this, we immediately see that a $2-(7,3,1)$ design is also a $1-(7,3,3)$ design.

Corollary 2.6. *A $t-(v,k,\lambda)$ design exists only if λ_s is an integer for each $s \leq t$.*

Also, if we set $s=0$, we get

$$b = |\mathcal{B}| = \left(\binom{v}{t} \Big/ \binom{k}{t}\right)\lambda.$$

If we set $s=1$, we see that each point is contained in

$$r = \left(\binom{v-1}{t-1} \Big/ \binom{k-1}{t-1}\right)\lambda$$

blocks.

Definition 2.7. An **isomorphism** between two $t-(v,k,\lambda)$ designs $(X,\mathcal{B})$ and $(X',\mathcal{B}')$ is a bijection $X \to X'$ that sends $\mathcal{B}$ to $\mathcal{B}'$. If $(X,\mathcal{B}) = (X',\mathcal{B}')$, it is called an **automorphism**, and the set of automorphisms clearly forms a group.

3 January 29, 2016

3.1 Incidence matrix of a design

We have looked at the block design Π_2. Let us form an incidence matrix from this design.

	B	E	D	O	R	U	Y
BUD	1	0	1	0	0	1	0
BYE	0	0	0	0	0	0	0
DOE	0	0	0	0	0	0	0
DRY	0	0	0	0	0	0	0
ORB	0	0	0	0	0	0	0
RUE	0	0	0	0	0	0	0
YOU	0	0	0	0	0	0	0

The rows are blocks, and the columns are points, and you put 1 if the point is in the block and 0 otherwise. The you get a matrix M with zeros and ones. This is called the **incidence matrix**.

The fact that each blocks as k points can be translated to that each row has k ones. Then in terms of matrices, we see that

$$M \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} k \\ \vdots \\ k \end{pmatrix} = k \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

As soon as $t \geq 1$, we also have the condition that each point is in r blocks. This will be equivalent to

$$\begin{pmatrix} 1 & \cdots & 1 \end{pmatrix} \cdot M = r \cdot \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}.$$

We observe that there is some kind of symmetry between the rows and columns. In fact, we can transpose the incidence matrix and define a new design.

Definition 3.1. Let $\mathcal{D} = (X, \mathcal{B})$ be a design. We define the **dual design** $\mathcal{D}^T$ to be the design with incidence matrix M^T, or more formally, $(\mathcal{B}, \{\beta_x : x \in X\})$, where $\beta_x = \{B \in \mathcal{B} : x \in B\}$.[1]

3.2 Fisher's inequality

So far we have only considered $t = 1$. Now let us look at the case $t = 2$. The conditions then can be translated to the fact that the dot product of any two

[1] Actually there is a technical problem here; we have assumed a design to have distinct blocks. But in this might not be true for the dual design. So it is actually just a structure.

different columns is λ. This is equivalent to

$$M^T M = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{pmatrix} = (r-\lambda)I + \lambda J,$$

where J is the matrix whose entries are all ones. By the way, we can write the previous conditions as $MJ = kJ$ and $JM = rJ$ by using J.

We can now do things like taking the determinant or looking at the eigenvalues.

Lemma 3.2. *The eigenvalues of the $n \times n$ matrix $xI + yJ$ are x with multiplicity $n-1$, and one $x + ny$. In particular,*

$$\det(xI + yJ) = (x + ny)x^{n-1}.$$

In our case of a 2-design, we see that $\det(M^T M) = (r + (n-1)\lambda)(r-\lambda)^{n-1}$.

Theorem 3.3. *Assume that $t \geq 2$ and $k < v$. Then the incidence matrix M is invertible.*

Proof. We need only check that $r > \lambda$. This is because $r(k-1) = (v-1)\lambda$ and thus

$$(r-\lambda)(k-1) = (v-1)\lambda - (k-1)\lambda = (v-k)\lambda > 0.$$

□

Corollary 3.4 (Fisher)**.** *Assume that there exists a $t - (v, k, \lambda)$ design where $t \geq 2$ and $1 < k < v$. Then $b \geq v$.*

Proof. This immediately follows from the previous theorem and the fact that the rank of the matrix is at most $\min\{b, v\}$. □

Let us look when the equality can be attained.

Theorem 3.5. *Let $\mathcal{D}(X, \mathcal{B})$ be a 2-design where $1 < k < v$. Then the following conditions are equivalent.*

1) $b = v$, i.e., it is a square design.

2) $k = r$.

3) any 2 blocks have λ points in common.

4) any 2 blocks have the same number of points in common.

5) $\mathcal{D}^T$ is a 2-design.

Proof. Use the fact that M is invertible, and use Fisher's inequality. □

4 February 1, 2016

We are going to look more at the equality case of Fisher's equality.

4.1 More on 2-designs

Theorem 4.1 (Bruck-Ryser-Chowla)**.** *Suppose that there exists a square $2-(v,k,\lambda)$ design. If v is even, then $k-\lambda$ has to be a square. If v is odd, then there exists integers x, y, z, not all zero, such that $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$.*

We will only prove and use the first statement.

Proof. Because M is $v \times v$, we have

$$\begin{aligned}\det M^2 = \det M^T M &= \det((r-\lambda)I + \lambda J) \\ &= ((r-\lambda)+\lambda v)(r-\lambda)^{v-1} = k^2(r-\lambda)^{v-1}.\end{aligned}$$

This implies that $r-\lambda = k-\lambda$ is square. □

Theorem 4.2. *If $\mathcal{D}$ is a $2-(v,k,\lambda)$ design, then for any block B, we have*

$$\#\{B' : B' \cap B \neq \emptyset, B' \neq B\} \geq \frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}.$$

I am not going to require you to memorize this. The important thing is to know the variance trick used in the proof.

If we let

$$\operatorname{var}(E) = \langle E^2 \rangle - \langle E \rangle^2$$

then we have

$$\operatorname{var}(E) = \Big(\sum p_i\Big)\Big(\sum p_i x_i^2\Big) - \Big(\sum p_i x_i\Big)^2 \geq 0.$$

Proof. We let

$$i(B') = \#(B \cap B')$$

and we can write what we want to compute as $\sum_{i(B')\neq 0} 1$. We see that

$$\sum_{i(B')\neq 0} i(B') = \sum i(B') = \sum \#(B \cap B\prime) = k(r-1)$$

and also

$$\sum_{i(B')\neq 0} i(B')^2 = \sum i(B')^2 = k(k-1)(\lambda-1) + k(r-1).$$

Then the Cauchy-Schwartz inequality gives us

$$\sum_{i(B')\neq 0} 1 \geq \Big(\sum_{i(B')\neq 0} i(B')\Big)^2 \Big/ \Big(\sum_{i(B')\neq 0} i(B')^2\Big) = \frac{k(r+1)^2}{(k-1)(\lambda-1)+(r-1)}.$$

□

We know that $\mathcal{D}$ is a square $2-(v,k,\lambda)$ design, then so is $\mathcal{D}^T$. If $\mathcal{D} \cong \mathcal{D}^T$, then we call $\mathcal{D}$ a **self-dual design**. This is the same as saying that there are maps $\sigma : X \to \mathcal{B}$ and $\tau : \mathcal{B} \to X$ such that

$$x \in B \Leftrightarrow \tau(B) \in \sigma(X).$$

If we have a **polarity**, then we have $\sigma\tau = \mathrm{id} = \tau\sigma$. Then there is a incident matrix that is actually symmetric.

5 February 3, 2016

I am going to give you more examples today.

5.1 Finite projective plane

A **finite projective plane** is a $2-(v,k,\lambda)$ design with $\lambda = 1$. If we let $k = n+1$, we see that $v = n^2+n+1$. So a finite projective plane is, in other words, a $2-(n^2+n+1, n+1, 1)$ design. As I have mentioned, it is a long open question of whether there exist a finite projective plane with order that is not a prime power.

We first look at Π_2. The points corresponds to elements of $V = (\mathbb{Z}/2\mathbb{Z})^3$, and the line corresponds to the sets $\{x, y, z\}$ with $x + y + z = 0$. This shows that every element of $GL_3(\mathbb{F}_2)$ gives a automorphism, and because

$$|GL_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-4) = 168$$

we get 168 automorphism. These are in fact all the automorphisms. This is because if we choose a point P, order the three lines passing P, and choose an arbitrary line ℓ' not passing P, we can reconstruct the whole projective plane. Note that we have made $7 \times 3! \times 4 = 168$ choices. This actually also proves the uniqueness of the finite projective plane of order 2.

Proposition 5.1. *Let q be a prime power. Then there is a finite projective plane of order q.*

Proof. Let $k = \mathbb{F}_q$ be the finite field of q elements. Let $V = k^3$ be the three dimensional space over k. We remove $(0,0,0)$, and let

$$X = (V \setminus \{(0,0,0)\})/k^* = \{\text{1-dim. subspaces of } V\}.$$

Now we let the blocks by

$$\mathcal{B} = \{\text{2-dim. subspaces of } V\}.$$

Then each block contains $q+1$ blocks, and two distinct points always determine a single block. □

We can think of its dual design. This dual design can be described in terms of the dual vector space V^*. Then the annihilator of a block is a point in the dual design, and the annihilator of a point is a block in the dual design.

6 February 8, 2016

6.1 Hadamard matrix

We have seen last time that there is a correspondence between **Hadamard designs**, or square $2-(4m-1, 2m-1, m-1)$ design, and **Hadamard matrices**, or $n \times n$ matrices H with entries ± 1 for which $H^T H = nI$. Given a Hadamard design, we can look at its incident matrix, change 0s to -1s, and add one column and one row consisting of 1s.

If H is a Hadamard matrix, then so is any H' obtained by

- permuting rows or columns, and
- multiplying any subset of rows or columns by -1s.

The matrices obtained by these operations are called equivalent Hadamard matrices. Note that we can apply these operations to any Hadamard matrix and make the first rows and columns into all 1s.

Theorem 6.1. *Suppose that exists a Hadamard matrix of order n. Then either $n = 1, 2$ or n is a multiple of 4.*

Proof. We assume without loss of generality that the first row consists of all +s. Then without loss of generality assume that the first half of the second row consists of +s, and the second half of the second row consists of −s.

Now suppose that for the third row, the first a are +s, the next b are −s, the next c are +s, and the last d are −s, with $a + b = c + d = \frac{n}{2}$. Then we have

$$a + c = b + d = \frac{n}{2}, \quad a + d = b + c = \frac{n}{2},$$

and it follows that $a = b = c = d = \frac{n}{4}$. □

We look at one construction of the Hadamard matrix.

Example 6.2 (Sylvester 1867)**.** We let $n = 2^{r+1}$ and let V be a $(r + 1)$-dimensional vector space oner $\mathbb{F}_2$. We identify the rows to V and columns to V^*, and then let the entries be

$$(x, y^*) \mapsto \begin{cases} 1 & \text{if } y^* x = 0, \\ -1 & \text{if } y^* x = 1. \end{cases}$$

Then one can check that it indeed is a Hadamard matrix.

Example 6.3 (Paley 1933)**.** Let $\mathbb{F}_q$ be a finite field of size $q \equiv -1 \pmod 4$. We associate each block and point to an element of $\mathbb{F}_q$. Let the block s' contain the point s if and only $s - s'$ is a nonzero square in k. This gives rise to a Hadamard design, or a Hadamard matrix of order $n = q + 1$.

It follows from the following proposition.

Proposition 6.4 (Legendre et al.)**.** *Let k be a finite field and let $|k| = 2r + 1$. Then (i) every nonzero square has exactly 2 square roots, and (ii) $s^r = 1$ if s is a nonzero square, $s^r = 0$ if $s = 0$, and $s^r = -1$ else.*

7 February 10, 2016

7.1 Complementary designs

Let $\mathcal{D} = (X, \mathcal{B})$ be a $t-(v,k,\lambda)$ design. We define the **complementary design** as the design $\bar{\mathcal{D}} = (X, \bar{\mathcal{B}})$, where

$$\bar{\mathcal{B}} = \{X \setminus B : B \in \mathcal{B}\}.$$

Proposition 7.1. *If $\mathcal{D}$ is a $t-(v,k,\lambda)$ design, then $\bar{\mathcal{D}}$ is a $t-(v,v-k,\bar{\lambda})$ design, with*

$$\bar{\lambda} = \sum_{s=0}^{t} (-1)^s \binom{t}{s} \lambda_s,$$

where λ_s is the the number for which $\mathcal{D}$ is a $s-(v,k,\lambda_s)$ design.

Proof. We use the standard inclusion-exclusion principle. We first fix a subset $T \subset X$ with $|T| = t$. For any $S \subset T$ with $|S| = s$, the number of blocks B containing S is λ_s. Then the number of blocks B disjoint form T will be

$$\sum_{S \subset T} (-1)^{|S|} \#(B \supseteq S) = \sum_{s=0}^{t} (-1)^s \binom{t}{s} \lambda_s. \qquad \square$$

We may now ask whether there are self-complementary designs. To begin with, we would have $v = 2k$ because the size has to match. We note that we do not have any nontrivial square design, because for a square design, $k^2 - k = (v-1)\lambda = (2k-1)\lambda$. Then $k = 1$ and things become boring.

Given a Hadamard matrix, it is possible to construct a self-complementary design. A Hadamard matrix gives a $2-(4m-1, 2m-1, m-1)$ design, and adding a point p and letting the new blocks be [the union of an original block and p] and [the complement of an original block], we get a $3-(4m, 2m-1, m-1)$ design, which is by the construction, self-complementary.

7.2 Derived designs

We can do the reverse process of what we just did. Let $\mathcal{D} = (X, \mathcal{B})$ be a $t-(v,k,\lambda)$ design and $p \in X$. Let

$$\mathcal{D}_p = (X \setminus \{p\}, \{B \setminus \{p\} : p \in B\}).$$

This is called the **derived design** with respect to p, and it is a $(t-1)-(v-1, k-1, \lambda)$ design.

Given a design $\mathcal{D}$, does there exists an extended design $\mathcal{E}$ such that $\mathcal{D} = \mathcal{E}_p$? If yes, then $\mathcal{D}$ is called an **extendable design**. For such an $\mathcal{E}$, it will have to necessarily be a $(t+1)-(v+1, k+1, \lambda)$ design.

Proposition 7.2. *If a $t-(v,k,\lambda)$ design $\mathcal{D}$ is extendable only if $k+1 \mid b(v+1)$.*

Proof. This follows from $bk = vr$ in $\mathcal{E}$. This becomes $b_{\mathcal{E}}(k+1) = (v+1)b_{\mathcal{D}}$ in terms of $\mathcal{D}$. □

This tells us which projective plane can be extendable. From the previous proposition, we would have $(n+2) \mid (n^2+n+1)(n^2+n+2)$, and this implies $n+2 \mid 12$. Then the possible values are $n = 2, 4, 10$. The case $n = 10$ is impossible, because there are no such projective planes. The case $n = 2$, it what we have already seen, and the case $n = 4$ is the beautiful case. The projective plane of order 4 can be extended three times and gives a $5-(24, 8, 1)$ design, which is associated to the Mathieu groups.

8 February 12, 2016

8.1 Arcs and ovals

If $\mathcal{E}_p = \mathcal{D}$ be a projective plane. Then what should the other blocks that does not contain p look like? If we let the order $\mathcal{D}$ be q, then it will be a $2-(q^2+q+1, q+1, 1)$ design. We now want to extend it into a 3-design, and it will be a $3-(q^2+q+2, q+2, 1)$ design. We know all the blocks containing p. A block that does not contain p can meet the original block of $\mathcal{D}$ at meet at most 2 points.

Definition 8.1. An n-**arc** is a subset of n points of a 2-design meeting each block in at most 2 points. (The notion is usually applied to square 2-desingns.) If a line meeting the arc at 2 points is called a **secant**, at 1 point a **tangent**, and at no points at **passant**.

Proposition 8.2. *In square $2-(v,k,\lambda)$ design, a point in an n-arc has $(n-1)\lambda$ secants and $k-(n-1)\lambda$ tangents.*

Proof. We just count the number of secants. □

Definition 8.3. An **oval** is an arc where each point has at most 1 tangent, i.e.,

$$n = \begin{cases} 1 + \frac{k-1}{\lambda} & \text{Type I (1 tangent per point)} \\ 1 + \frac{k}{\lambda} & \text{Type II (no tangents, hyperoval)} \end{cases}$$

We immediately see that a Type I oval can exist only if $k \equiv 1 \pmod{\lambda}$. Likewise, a Type II oval can exist only if $k \equiv 0 \pmod{\lambda}$. Both can exist only if $\lambda = 1$, or in other words, if we are working in a projective plane.

Proposition 8.4. *If there exists an hyperoval S, then $k \equiv \lambda \pmod 2$. (That is, except for the trivial $2-(3,2,1)$ design.*

Proof. We first fix $p \in S$. How many secants does p pass? The number is

$$\frac{n\lambda}{2} = \frac{(1+\frac{k}{\lambda})\lambda}{2} = \frac{k+\lambda}{2}.$$

Thus k and λ must have the same parity. □

Corollary 8.5. *A hyperoval exists in a projective plane only if q is even.*

Let q be an even number. If we have a Type II oval in the projective plane, then we can delete one point and get a Type I oval. In fact, for any Type I oval, every tangent passes through a singe point, and thus we can throw it in to get a Type II oval.

Proposition 8.6. *Let $k \equiv \lambda \pmod 2$, and S be a Type I oval in a square $2-(v,k,\lambda)$ design. Then any point is in either 1 tangent or all of them.*

Proof. Since $k(k-1) = (v-1)\lambda$ and $n-1 = (k-1)/\lambda$ is an integer, we see that k, λ, n must all be odd. We now count for each $i = 0, 1, 2, \ldots,$ the point contained in i of the tangents.

We first note that every point is contained in an odd number of tangents. This is because the passants and secants do not contribute, in parity, to the sum of the number of intersection of the oval and a line passing through a given point, which is $n\lambda$. So each point is contained in an odd number of tangents.

We now let N_i be the number of points contained in i tangents. Clearly we have $N_i = 0$ if i is even. Then we have

$$\begin{cases} \sum N_i = v, \\ \sum iN_i = \#(\text{tangents, points on it}) = nk, \\ \sum (i^2 - i)N_i = \#(t, t', p \in t, t') = n(n-1)\lambda. \end{cases}$$

Combining this, we see that

$$\sum (i-1)(i-n)N_i = 0,$$

but since $(i-1)(i-n) \leq 0$ always, we get that $N_i \neq 0$ only if $i = 1$ or $i = n$. $\square$

The projective plane $\mathbb{P}^2(\mathbb{F})$ contains ovals. We see that

$$\{(r^2 : rs : s^2) \mid (r : s) \in \mathbb{P}^1\}$$

is an oval. If $\mathbb{F} = \mathbb{F}_q$ with $q = 2^r$, then these ovals give rise to hyperovals. If q is odd, then there are no others ovals! (This is known as Segre's theorem.)

9 February 17, 2016

9.1 Residual designs

Let $\mathcal{D} = (X, \mathcal{B})$ be a finite projective plane of order q. Pick any point $B \in \mathcal{B}$ and form the **residual design** by removing B as

$$\mathcal{D}^B = (X \setminus B, \{B' \setminus B : B' \in \mathcal{B}, B' \neq B\}).$$

Then this becomes an affine plane of order q. More generally, if $\mathcal{D}$ is a square $2-(v,k,\lambda)$ design, we see that $\mathcal{D}^B$ is a $2-(v-k, k-\lambda, \lambda)$ design. Because $k(k-1) = (v-1)\lambda$, we have in $\mathcal{D}^B$,

$$k^B(k^B + \lambda^B - 1) = v^B \lambda^B.$$

A 2-design meeting this condition is called **quasi-residual**.

Proposition 9.1. *Every $2-(q^2, q, 1)$ design ,i.e., **affine plane** of order q, is a residual of a projective plane.*

Proof. In an affine plane, we se that $L \parallel L'$ if and only if $L = L'$ or $L \cap L' = \emptyset$. We consider the parallel relation. This is clearly reflexing and symmetric. Also we have the following lemma.

Lemma 9.2 (Playfair's axiom)**.** *For any p and L, there is a unique line L' passing through p that is parallel to L.*

Proof. If $p \in L$ then $L' = L$ is the unique line. If $p \notin L$, then there are $q+1$ lines passing through p and q points on L. Then there will be a unique line passing through p not meeting L. □

Using this lemma, we see that the parallel relation is and equivalence relation, and that an equivalence class form a partition of the plane. Then we can throw in points corresponding to equivalence classes and make a projective plane. □

9.2 Inversive planes

We note that any three points is in a unique circle in $\mathbb{P}^1(\mathbb{C})$. In other words, any three points is in a unique $\mathbb{P}^1(\mathbb{R})$.

Using this as a motivation, we can look at the finite field $k = \mathbb{P}^1(\mathbb{F}_q)$. Then we can look at the degree 2 extension $k' = \mathbb{P}^1(\mathbb{F}_{q^2})$. If we set the image of the embeddings $\mathbb{P}^1(\mathbb{F}_q) \hookrightarrow \mathbb{P}^1(\mathbb{F}_{q^2})$ as blocks, we have a **inversive plane**, which is a $3-(q^2+1, q+1, 1)$ design.

I am going to Arizona on Friday to give a talk, so there will be no class.

10 February 22, 2016

Today we start on chapter 2, which is the part on strongly regular graph.

10.1 Strongly regular graphs

Definition 10.1. A **graph** is an ordered pair sets (V, E), where V is a finite collection of "vertices" and E is a subset of $\binom{|V|}{2}$.

Two vertices v and v' are called to be **adjacent** or **neighbors** if and only if $\{v, v'\} \in E$. We denote by $G(v)$ the set of neighbors of v. The size $\#G(v)$ is called the **degree** of v. We note that these graphs do not have loops, multiple edges, or directions. A graph can be considered as a never reflexing and symmetric relation.

Definition 10.2. An **isomorphism** $\varphi : (V, E) \to (V', E')$ is a bijection $V \to V'$ such that edges are sent to edges and non-edges are sent to non-edges.

The set of automorphisms of a graph form the automorphism group.

A graph can be considered as a design with $k = 2$. The 0-designs and 2-designs are trivial; every graph is a 0-design, and 2-designs are either empty or complete. Also 1-designs are simply regular graphs, i.e., graphs with constant degree. So we impose another condition.

Definition 10.3. A graph G is called **strongly regular** if for any 2 vertices v and v',

$$\#(G(v) \cap G(v')) = \#\{w : v \sim w \sim v'\}$$

depend only on whether $v = v'$, $v \sim v'$, or $v \not\sim v'$.

There are four parameters (n, k, λ, μ). The n is the number of vertices, and k, λ, and μ are common neighbors of v and v' for $v = v'$, $v \sim v'$, and $v \not\sim v'$. A strongly regular graph is necessarily regular of degree k.

A graph G is strongly regular if and only if the complement $\bar{G}$ is strongly regular. The complementary graph $\bar{G}$ has parameters

$$\bar{n} = n, \quad \bar{k} = n - 1 - k, \quad \bar{\lambda} = n - 2 + \mu - 2k, \quad \bar{\mu} = n + \lambda - 2k.$$

Example 10.4. The graph $r \cdot K_m$, which is simply r disjoint copies of K_m, is strongly regular with parameters

$$n = rm, \quad k = m - 1, \quad \lambda = m - 2, \quad \mu = 0.$$

Example 10.5. The graph $T(m)$ has vertices $\binom{\{1,\dots,m\}}{2}$ and two subsets v and v' are connected if and only if v and v' are not disjoint. This is a strongly regular graph with $(n, k, \lambda, \mu) = (\frac{1}{2}(m^2 - m), 2(m-2), m-2, 4)$. We note that this can be drawn on the plane so that the vertices form a triangular shape and the edges consists of pairs of vertices that lie on some curved line.

Example 10.6. The square lattice graph $L_2(m)$ is the graph on $\{1, \ldots, m\} \times \{1, \ldots, m\}$ with adjacency is 1 coordinate overlapping. It is a strongly regular graph with $(n, k, \lambda, \mu) = (m^2, 2m - 1, m - 2, 2)$.

Proposition 10.7. *For any strongly regular graph with* (n, k, λ, μ)*,*

$$k(k - \lambda - 1) = (n - k - 1)\mu.$$

Proof. Consider the set of pairs $(v \sim w \sim x \not\sim v)$ for a fixed v. We can double count and get the desired result. $\square$

11 February 24, 2016

Given a graph G, we can construct its adjacency matrix. Then we can look at its spectrum.

11.1 Adjacency matrix

Let G be a graph with $|V| = n$. Label the vertices $1, 2, \dots, n$ and construct a matrix A so that

$$A_{i,j} = \#\{\text{edges } \{i,j\} \text{ in } G\}.$$

In our case, each entry will be either 0 or 1. We note that since $\{i,j\} = \{j,i\}$, the matrix is symmetric, and its trace is zero. If you are concerned about the matrix being non-canonical, we can simply consider it as a linear transformation from the real vector space generated by the vertices.

The adjacency matrix of the complementary graph $\bar{G}$ is given by

$$A_{\bar{G}} = J - I - A_G.$$

Also,

$$A_G \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = k \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

if and only if A_G is regular of degree k. Moreover, G is strongly regular with parameters (n, k, λ, ν) if and only if

$$A_G j = kj \quad \text{and} \quad A_G^2 = kI + \lambda A_G + \mu(J - I - A_G).$$

We note that multiplying j at the end gives us the identity $k(k-1-\lambda) = \nu(n-1-k)$.

In fact, we can do more than that. Suppose that $Au = \rho u$ with $u \neq 0$ an eigenvector and ρ and eigenvalue. If $\rho \neq k$, then we see that u must be orthogonal to j, and it follows that

$$\rho^2 u = A^2 u = ku + \lambda \rho u - \mu(1+\rho)u.$$

Then we have

$$\rho^2 - (\lambda - \mu)\rho + (\mu - k) = 0.$$

The two roots must be real, since $\mu - k \leq 0$. We let the two roots be $r > s$.

Because A is a symmetric real matrix, the geometric multiplicity and the algebraic multiplicity agree. That is, we can let, without ambiguity,

$$\begin{cases} f = \text{mult. of } r = \dim\ker(A - rI) \\ g = \text{mult. of } s = \dim\ker(A - sI). \end{cases}.$$

Because k has multiplicity 1 as an eigenvalue, we have $f + g = n - 1$, and $rf + sg = -k$. We can solve the system of linear equations, and get

$$f, g = \frac{n - 1 \pm \frac{(n-1)(\mu-\lambda)-2k}{\sqrt{D}}}{2}.$$

What is the point of doing this all?

Theorem 11.1 (Integrality condition)**.** *f and g has to be integers.*

Unless you already have a graph in mind, this will eliminate a lot of possibilities. We see that either $(n-1)(\mu-\lambda) - 2k = 0$, or D has to be a square. The first case is called type I, and the second case is called type II. We note that in the case of a type I design, from $n - 1 > k$, it follows that $\mu - \lambda = 1$ and $n = 2k - 1$. Then it is of form $(n, k, \lambda, \mu) = (4\mu + 1, 2\mu + 1, \mu - 1, \mu)$.

12 February 26, 2016

Today we will prove the degree of a Moore graph is one of $2, 3, 5, 57$.

12.1 Moore graph

Let G be a regular graph of degree k.

Proposition 12.1. *If the diameter of a k-regular graph is at most 2, then $n \leq k^2 + 1$. If the girth is at least 5, then $n \geq k^2 + 1$.*

If a graph has diameter 2 and girth 5, then we say that is a **Moore graph**.

Proof. We fix a point x, and consider the neighbors of x and the neighbors of neighbors of x. Then we have $k^2 + 1$ so far. If the diameter is at most 2, then these contain all the points. If the girth is at least 2, then those points are all distinct. □

We see that a Moore graph is a strongly regular graph with parameters $(n, k, \lambda, \mu) = (k^2 + 1, k, 0, 1)$. We recall that the possible spectrum of the adjacency matrix is

$$r, s = \frac{1}{2}(\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)})$$

with multiplicity

$$f, g = \frac{1}{2}\Big(n - 1 \pm \frac{(n-1)(\mu - \lambda) - 2k}{\sqrt{D}}\Big).$$

If the Moore graph is of Type I, we see that $k^2 - 2k = 0$ and thus $k = 2$. In this case, the graph is a pentagon. If the Moore graph is of Type II, then $D = 4k - 3$ is a square. Let $\sqrt{D} = 2m + 1$ and $k = m^2 + m + 1$. Then we have the condition

$$2m + 1 \mid (m^2 + m + 1)(m^2 + m - 1)$$

and then we get $2m + 1 \mid 15$. Then $m = 0, 1, 2, 7$, and it follows that $k = 3, 7, 57$. Therefore we have the following theorem.

Theorem 12.2. *A Moore graph of degree k exists only for $k = 2, 3, 7, 57$.*

12.2 Bounds on the multiplicity

We look at the eigendecomposition

$$V(G) = (*1) \oplus V_r \oplus V_s.$$

Let e_x be some unit vector $(0, \dots, 1, \dots, 0)$, and let

$$e_x = \frac{1}{n}1 + u_x + v_x.$$

When we take the inner product, we get

$$1 = \langle e_x, e_x \rangle = \frac{1}{n} + \langle u_x, u_x \rangle + \langle v_x, v_x \rangle$$
$$0 = \langle Ae_x, e_x \rangle = \frac{k}{n} + r\langle u_x, u_x \rangle + s\langle v_x, v_x \rangle$$

and we can solve the linear equation and get $\langle u_x, u_x \rangle$ and $\langle v_x, v_x \rangle$.Likewise, we get some a linear equation for $\langle u_x, u_y \rangle$ and $\langle v_x, v_y \rangle$ and just compute them.

Theorem 12.3. *If $S \subset \mathbb{R}^f$ be a set of unit vectors. Suppose that there exists some $b, c \in \mathbb{R}$ such that for any $v \neq v' \in S$ their inner product is $\langle v, v' \rangle = b$ or c. Then $\#S \leq f(f+3)/2$.*

Proof. We note that $f(f+3)/2$ is the dimension of the space of quadratic polynomials minus 1. We construct the polynomials

$$f_v(x) = (\langle v, x \rangle - b)(\langle v, x \rangle - c) - bc(\langle x, x \rangle - 1).$$

By the conditions, the evaluation of the polynomials are

$$f_v(v') = \begin{cases} 0 & \text{if } v' \neq v \\ (1-b)(1-c) & \text{if } v' = v \\ 0 & \text{if } v' = 0. \end{cases}.$$

This shows that the f_vs are linearly independent in the codimension 1 subspace of the space of quadratic polynomials. Therefore the number of f_v is at most $f(f+3)/2$. □

Theorem 12.4 (Delsarte-Goethals-Seidel, 1977)**.** *There exists a strongly regular graph only if*

$$n \leq \min\left\{\frac{f(f+3)}{2}, \frac{g(g+3)}{2}\right\}.$$

13 February 29, 2016

We are going to look at automorphism groups.

13.1 Automorphisms of Π_2 and Π_3

We look at the set of isomorphisms from any arbitrary finite projective plane Π_2' to our favorite projective plane Π_2. We pick any hyperoval in Π_2' and another hyperoval in Π_2. We see that any bijection between the two ovals uniquely extends to an isomorphism between the two projective planes. This means that there are

$$7 \cdot 4! = 168$$

isomorphisms, and thus the automorphism group has size 168 and also that Π_2 is unique. Since $PGL_3(\mathbb{F}_2)$ gives 168 automorphisms already, we see that this is the automorphism group.

Let us now look at Π_3' and Π_3. We claim that if we pick any ordered ovals $O' \subset \Pi_3'$ and $O \subset \Pi_3$, the map $O' \to O$ extends to a unique isomorphism. Given an oval, there are

$$6 \text{ secants } s_{ij}, \quad 4 \text{ tangents } t_i, \quad 3 \text{ passants.}$$

Then the points will be

$$6 \text{ points } t_i \cap t_j, \quad 4 \text{ oval points } p_1, \dots p_4, \quad 3 \text{ points } s_{12} \cap s_{34}, s_{13} \cap s_{24}, s_{14} \cap s_{23}.$$

Now that we know a great deal about the structure, we can determine all the incidence relations. We see that the tangent and secant lines are

$$t_i = \{t_i, t_i \cap t_j, t_i \cap t_k, t_i \cap t_l\},$$
$$s_{ij} = \{p_i, p_j, s_{ij} \cap s_{kl}, t_k \cap t_l\},$$

and then the passant lines must be

$$\{t_i \cap t_j, t_k \cap t_l, s_{ik} \cap s_{jl}, s_{il} \cap t_{jk}\}.$$

Thus the isomorphism is unique, and thus we see that the total number of isomorphisms is the number of ordered ovals, which is

$$13 \cdot 12 \cdot 9 \cdot 4 = 5616.$$

This we can check agrees with the size of $PGL_2(\mathbb{F}_3)$.

Index