KRYSTAL GUO

GRAPH SYMMETRIES AND COMBINATORIAL DESIGNS

Contents

Note to my students

The lecture notes from class will be placed here, after a bit of formatting to make it nicer to read.

1
Graph Symmetries

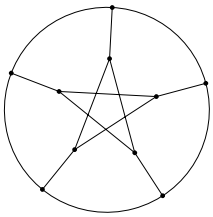
1.1 Introduction to Graph Symmetries

We want to study symmetries of graphs and also graphs which have many symmetries. Many of these graphs come from incidence graphs or points graphs of combinatorial designs.

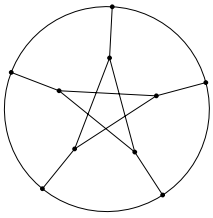
Algebraic graph theory is is concerned with use of algebraic techniques in graphs. We take properties of graphs and we express it as some algebraic property and then we apply some tools from linear algebra or group theory to deduce properties about the graph. Combinatorial designs has applications in coding theory, quantum information theory, networks and finance. We will look at topics from both these areas through the lens of symmetry and regularity.

What do we mean by "symmetry and regularity"?

A symmetry property of a graph is related to whether or not some automorphism exist. What do I mean by automorphism? Here is a graph.



Casually speaking, an automorphism is something I do to the graph, and you don't notice that I've done it.



I did something. What did I do? I rotated the whole thing by $\frac{2\pi}{5}$.

This graph is called the Petersen graph and we will revisit it many times. Less informally, an automorphism is a permutation

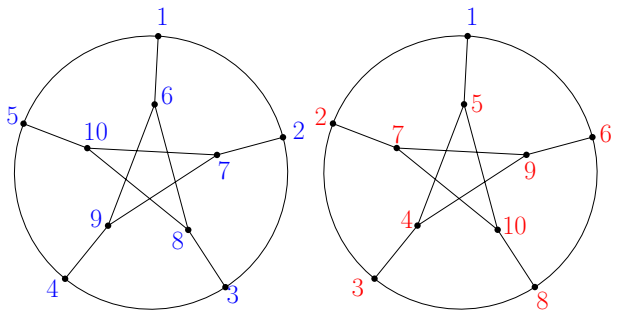


Figure 1.1: The Petersen graph.

of the vertices, which preserves the edges. We can capture all the information about a graph in a table such as the one in Table 1.1.

Vertex	Neighbours
1	2,5,6
2	1,3,7
3	2,4,8
4	2,5,9
5	1,4,10
6	1,8,9
7	2,9,10
8	3,6,10
9	4,6,7
10	5,7,8

Table 1.1: The vertices and their neighbours of the Petersen graph.

We can use the red and blue labels in Figure 1.1 to give an automorphism; see Table 1.2.

blue	red
1	1
2	6
3	8
4	3
5	2
6	5
7	9
8	10
9	4
10	7

Table 1.2: The red and blue labels of the vertices of the Petersen graph.

Defining ϕ as the map taking the blue names of the vertices to the red name, would give us an automorphism. Even less informally, an automorphism of a graph (V, E) is a permutation of V such that $u, v \in V$ is an edge if and only if $\phi(u), \phi(v)$ is an edge.

A regularity property is defined in purely numerical terms. When we have symmetries, often we also get regularity properties. We will study elementary properties of automorphisms and how effect eigenvalues of the adjacency matrix. There is a general tendency that if a graph has many automorphism, then it has few distinct eigenvalues.

What are some examples of symmetry conditions?

- every vertex is alike;
- every pair of adjacent vertices is alike;
- a snake of length s crawling on the graph thinks everywhere is the same.

A snake of length 2 crawling on the Petersen graph thinks that everything looks the same.

Combinatorial designs is conglomeration of things. A block design consists some points P and some blocks B; the blocks are k-subsets of points. Every point is on r blocks and each pair of distinct points is on λ blocks, where r, λ are constants. Examples of block designs include projective plane, affine planes, and Steiner triple systems.

Block designs often give rise to graphs with symmetries and regularity and we can apply tools from the first half of the class to study them.

Other topics: Hadamard matrices, (spherical) t-designs, equiangular lines, etc.

1.2 *Groups acting on graphs*

We will follow the Godsil and Royle book when it comes to notation; G, H are groups, X, Y are graphs, f, g, h are group elements, x, y, z, u, v, w are vertices (or ground set elements).

$\mathrm{Sym}(V)$ denotes the set of all permutations of a set V, which forms a group under composition. If $|V| = n$, we can also write $\mathrm{Sym}(n)$ or S_n. A *permutation group* is a subgroup of $\mathrm{Sym}(V)$.

Notation: each $g \in \mathrm{Sym}\, V$ is a permutation on V. For $x, y \in V$, we write

$$x^g = y$$

to indicate that g sends x to y. Note

$$(x^g)^h = x^{gh}$$

and $x^1 = x$ where 1 is the identity of G. This is an example of G acting on V.

The *action* of a group G on V is a homomorphism from G into $\mathrm{Sym}(V)$. The action is faithful if the kernel of the homomorphism is trivial, ie. $G \cong H \leq \mathrm{Sym}(V)$.

Examples:

(i) S_n acts on $\{1, 2, \ldots, n\}$.

(ii) D_{2n} acts on the regular n-gon.

(iii) $GL(n, \mathbb{F})$ acts on the vector space $\mathbb{F}^n$.

(iv) G acts on itself by left or right multiplication.

Consider $V = \{1, 2, 3\}$ and let's see some examples of action on this set.

(i) $G = \mathrm{Sym}(V)$ acts on V. What is the homomorphism? It's the identity homomorphism.

(ii) $\langle(123)\rangle \leq S_3$ acts on $\{1,2,3\}$. Homomorphism: we map to this subgroup of $\mathrm{Sym}(V)$ with the identity map.

(iii) S_{100} acts of V by fixing every element. We can take a homomorphism from S_{100} to $S_1 \leq \mathrm{Sym}(V)$ by sending every element to the identity. This action is not faithful.

The *orbit* of a point $x \in V$ is $x^G = \{x^g \mid g \in G\}$. The *stabilizer* of a point $x \in V$ is

$$G_x = \{g \in G \mid x^g = x\} \leq G.$$

1.2.1 Lemma. *For $x, y \in V$ such that there exists $h \in G$ such that $x^h = y$, we have*

1. *$H = \{g \in G \mid x^g = y\} = G_x h$ (is a coset of the stabilizer of x).*

2. *$G_y = h^{-1} G_x h$.*

Proof. For part 1, we have $x^h = y$ and so $x^h = x^g$ and so $x^{gh^{-1}} = x$, for all $g \in H$. We sse that $gh^{-1} \in G_x$. This happens if and only if $g \in G_x h$ for all $g \in H$.

For part 2, consider a stabilizer of y, say $y^g = y$. Thus $x^{hg} = x^h$ and so $x^{hgh^{-1}} = x^{hh^{-1}} = x$. We have shown that $hgh^{-1} \in G_x$ and so $g \in h^{-1} G_x h$. □

1.2.2 Lemma (Orbit-Stabilizer Theorem)**.** *Suppose G acts on V and $x \in V$. Then,*

$$|x^G||G_x| = |G|.$$

Proof.

$$\begin{aligned} |G| &= \sum_{y \in x^G} |\{g \in G \mid x^g = y\} \\ &= \sum_{y \in x^G} |G_x| \\ &= |x^G||G_x|. \end{aligned}$$

□

1.2.3 Lemma. *(Burnside) The number of orbits in action of G on V is*

$$\frac{1}{|G|} \sum_{g \in G} fix(g).$$

where $fix(g)$ is the number of $y \in V$ such that $y^g = y$.

Proof. Count the number pairs (x, g) such that $x^g = x$. Let N be this number. Each $g \in G$ fixes $fix(g)$ elements x, so this gives us that

$$N = \sum_{g \in G} fix(g).$$

On the other hand, we can also count by choosing x and then choosing g such that g fixes x. We get

$$N = \sum_{x \in V} |G_x|.$$

The two expressions for N gives us

$$\sum_{g \in G} fix(g) = \sum_{x \in V} |G_x|.$$

Dividing both sides by $|G|$, we then apply the Orbit-Stabilizer Theorem to obtain that the RHS is the number of orbits. □

The action of G on V is said to be *transitive* if there is exactly one orbit, ie for all $x, y \in V$ there exists some group element g such that $x^g = y$.

A graph X is *vertex-transitive* if for each $x, y \in V(X)$ there exists a $g \in Aut(X)$ such that $x^g = y$.

How do we construct vertex-transitive graphs? We start with the group. Let G be a group and $C \subseteq G$. The *Cayley digraph* $X(G, C)$ is a graph whose vertices are the elements of G and edge set

$$E(X(G, C)) = \{(g, h) \mid hg^{-1} \in C\}.$$

If C does not contain the identity and is closed under taking inverses, then $X(G, C)$ is a graph (we call it a *Cayley graph*).

Next time: a Cayley graph is vertex-transitive. And in fact, G is a subgroup of its automorphism group.

The action of G on V is *transitive* if there is exactly one orbit; that is for all $x, y \in V$, there exists $g \in G$ such that $x^g = y$. The action of G on V is *regular* if for every $x, y \in V$, there is a unique $g \in G$ such that $x^g = y$.

Note that G acts regularly on V, this action corresponds to G acting on G by right multiplication.

1.2.1 *Group actions on graphs*

A *homomorphism* from graph X to graph Y is a mapping $\phi : V(X) \to V(Y)$ such that whenever xy is an edge of X then $\phi(x)\phi(y)$ is an edge of Y. The map ϕ is an *isomorphism* from X to Y if ϕ is a bijective homomorphism; that is ϕ is bijective and its inverse map is also a homomorphism.

1.2.4 Example. If X is a subgraph of Y, then X has a homomorphism to Y, given by the identity map, restricted to the vertices of X.

1.2.5 Example. A (proper) *colouring* of a graph X is an assignment of colours to the vertices of X such that adjacent vertices get different colours. A colouring with k colours is equivalent to a homomorphism from X to K_k.

An *automorphism* of X is a bijection $\phi : V(X) \to V(X)$ which is a homomorphism. The *automorphism group* of a graph X, denoted $\mathrm{Aut}(X)$, is the set of all automorphisms of X under composition. A group G acting on a graph X is a homomorphism from G to $\mathrm{Aut}(X)$.

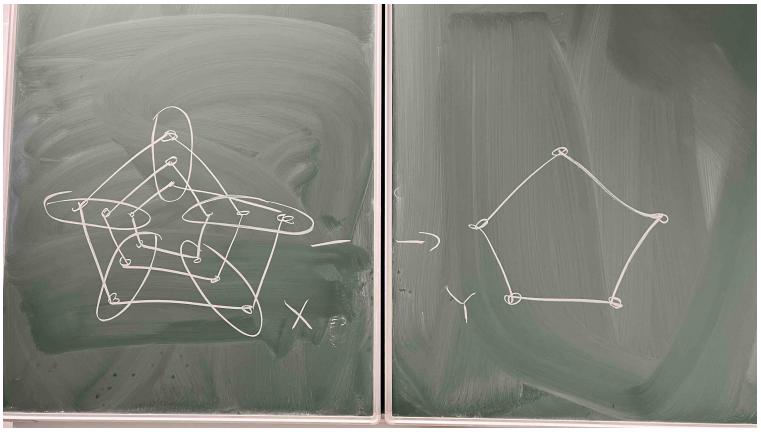


Figure 1.2: Graph X has a homomorphism to Y given by taking the groups of encircled vertices to vertices of Y.

1.2.6 Example. Recall the Petersen graph from last class. We observed that D_5 is a subgroup of the automorphism of the graph. The automorphism group of this graph is actually S_5.

1.2.2 *Higher transitivity*

We consider G acting on a set V. Here, G has a natural action on $V \times V$ by $(x, y)^g \mapsto (x^g, y^g)$. The orbits of G on $V \times V$ are called *orbitals*. The elements of $V \times V$ of form (x, x) are called the *diagonal*. We can see that if V has at least 2 elements, there will be at least 2 orbitals (under the action of any group) since a diagonal element cannot be mapped to a non-diagonal element.

More generally, G acts on V^n by

$$(x_1, x_2, \ldots, x_n)^g \mapsto (x_1^g, x_2^g, \ldots, x_n^g).$$

The action of G on V is said to be t-transitive if for any two $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ in V^t such that $y_i = y_j$ whenever $x_i = x_j$, there exist a $g \in G$ such that $(x_1, \ldots, x_t)^g = (y_1, \ldots, y_t)$.

1.2.7 Theorem. *(Cameron) If G (a finite group) acts 6-transitively on V then this action consists of* $\mathrm{Sym}(V)$ *or $A(V)$, the alternating group acting on V.*

Intuitively, this means that t-transitivity is a very strong requirement and it "stops" at $t = 6$.

Let us return to G acting on $V \times V$. If the action of G on V is transitive then, the set $\{(x, x) \mid x \in V\}$ will be an orbital of G acting on $V \times V$ (called the diagonal orbital).

Let $\Omega \subseteq V \times V$, we define its transpose Ω^T to be

$$\{(y, x) \mid (x, y) \in \Omega\}.$$

We say that Ω is G-invariant if $(x, y)^g \in \Omega$ for all $(x, y) \in \Omega$. The set Ω is G-invariant if and only if Ω^T. Since orbits are either equal or disjoint, if Ω is an orbital of G then either $\Omega = \Omega^T$ or $\Omega \cap \Omega^T = \emptyset$. If $\Omega = \Omega^T$, we say that the orbital is *symmetric*.

1.2.8 Lemma. *Let G act on V transitively. Let $x \in V$. Then there is a one-to-one correspondence between the orbitals of G and the orbits of G_x (on V).*

Proof. Let Ω be an orbital of G. Define:

$$Y_\Omega = \{y \mid (x, y) \in \Omega\}.$$

We will that Y_Ω is an orbit of G_x acting on V. First we note that Y_Ω is non-empty. Since Ω is non-empty, it contains some element (z_1, z_2). Since G is transitive on V, there exists some element g such that $z_1^g = x$ and so $(z_1, z_2)^g \in \Omega$. Then $z_2^g \in Y_\Omega$.

Let $y, y' \in Y_\Omega$. This occurs if and only if $(x, y), (x, y') \in \Omega$, which is if and only there exists $g \in G$ such that $(x, y)^g = (x, y')$. This occurs if and only if there exists $g \in G$ such that $x^g = x$ and $y^g = y'$. This happens if and only y, y' are in the same orbit of G_x.

Thus V is partitioned by the set Y_Ω where Ω ranges over the orbital, and the lemma follows. □

Some other transitivity conditions are as follows. The action of G on V is *generously transitive* if for any $x, y \in V$ there exists $g \in G$ such that g swaps x and y; i.e. $x^g = y$ and $y^g = x$. All orbitals of G are symmetric if and only G is generously transitive.

1.2.3 Johnson graphs

Let v, k, i be positive integers such that $v \geq k \geq i$ and let Ω be a fixed set of size v. The *Johnson graph* $J(v, k, i)$ is a graph whose vertices are the k-subsets of Ω and two k-subsets S, T are adjacent if $|S \cap T| = i$.

The graph $J(v, k, i)$ has $\binom{v}{k}$ vertices. This graph is regular (every vertex has the same degree) with valency

$$\binom{k}{i}\binom{v-k}{k-i}.$$

As an exercise, convince yourself of the following: $J(v, k, i)$ is isomorphic to $J(v, v-k, v-2k+i)$. (Hint: consider the complement of the k-subsets, which form the vertex of the first graph). We may assume from now on that $v \geq 2k$.

There are some special members of the family. The Johnson graph (in the literature) is $J(v, k, k-1)$. The Kneser graph is $J(v, k, 0)$. The Petersen graph is $J(5, 2, 0)$.

Let g be a permutation of Ω and let $S \subseteq \Omega$. We write

$$S^g = \{s^g \mid s \in S\}.$$

Each element g gives a permutation of the k-subsets and for $S, T \in \Omega$ we have that $|S \cap T| = |S^g \cap T^g|$.

1.2.9 Lemma. *If $v \geq k \geq i$, then* $\mathrm{Aut}(J(v, k, i))$ *contains a subgroup isomorphic to* $\mathrm{Sym}(v)$.

If this the whole automorphism group of $J(v, k, i)$? Not always. We will show that for the Petersen graph, this is the whole automorphism group, but in general it's not true. Ex. $J(6, 3, 2)$ has a larger automorphism group

1.2.10 Example. Prove that the automorphism group of $J(7,3,1)$ contains a subgroup isomorphic to S_8.

- Idea: if you take 3-subsets of $[1,\ldots,8]$, which do not contain 8, these are 3-subsets of $[1,\ldots,7]$. If you take 4-subsets of $[1,\ldots,8]$, which do contain 8, these are also the 3-subsets of $[1,\ldots,7]$.
- There are 35 partitions of 8 into two sets of size 4. Take Y such that these are the vertices. Two vertices of Y are adjacent if the intersection of a 4-set from one partition with one 4-set from the partition has size 2.
- Observe that S_8 is a subgroup of the automorphism group of Y.
- Show that Y is isomorphic of $J(7,3,1)$. (Each partition has a part containing 8).

1.3 Groups acting on graphs continued

1.3.1 Theorem. *The Cayley graph $X(G,C)$ is vertex-transitive.*

Proof. Let $x,y \in G$. For each $g \in G$, let $\rho_g : x \mapsto xg$. We note that ρ_g is a permutation of the elements of G and is an automorphism of graph since

$$(yg)(xg)^{-1} = ygg^{-1}x^{-1} = yx^{-1}$$

thus yg, xg are adjacent if and only if x,y are adjacent. For x,y, $\rho_{x^{-1}y}$ is an automorphism sending x to y. □

In the big picture, it's not very difficult to construct vertex-transitive graphs. We actually showed $G \leq \mathrm{Aut}(X(G,C))$.

Special Cayley graphs: a *circulant* is a Cayley graph $X(\mathbb{Z}_n, C)$. A *cube-like* graph is Cayley graph $X(\mathbb{Z}_2^n, C)$. In particular the cube graph (or hypercube) is the Cayley graph $X(\mathbb{Z}_2^n, \{e_1,\ldots,e_n\})$, where e_i is the elementary basis vector which as a 1 in the ith position and 0 elsewhere. The hypercube is always a bipartite graph (exercise for the reader).

1.4 t-transitivity in graphs

An arc in a graph is an ordered pair of adjacent vertices, and so a graph is *arc-transitive* if its automorphism group acts transitively on the set of arcs.

An s-arc in a graph is a sequence of vertices $(v_0, v_1, \ldots, v_s)$ such that consecutive vertices are adjacent and $v_{i-1} \neq v_{i+1}$ for $0 < i < s$. Note that an s-arc doesn't have to correspond to a path; repetition of vertices can happen and can be useful to consider. We will only consider s-arcs in graph with minimum degree 2.

A graph is s-arc-transitive if its automorphism group acts transitively on the s-arcs of the graph. If a graph is s-arc-transitive, it is also $s-1$-arc-transitive. Arc-transitivity is equivalent to 1-arc-transitivity. In particular, any s-arc-transitive graph where $s \geq 1$, is also vertex-transitive.

"Truth and utility are different concepts." A cycle on n vertices is s-arc-transitive for all s. Tutte showed that for any s-arc-transitive cubic graph, $s \leq 5$. Weiss shows for any valency, if X is s-arc-transitive then $s \leq 7$.

Let G be a transitive group acting on V. A non-empty subset $S \subseteq V$ is a *block of imprimitivity* for G if for any $g \in G$ either $S^g = S$ or $S^g \cap S = \emptyset$. Since G is transitive on V, the translates of S form a partition of V. The set of translates is said to be a *system of imprimitivity*.

For example, the cube graph Q has a transitive automorphism group $\mathrm{Aut}(Q)$. But Q is bipartite, the bipartition is a system of imprimitivity.

The partition of V into singletons is a system of imprimitivity, as is the partition into 1 cell. All other partitions are non-trivial. A group with no non-trivial systems of imprimitivity is *primitive*; otherwise it is *imprimitive*.

As an exercise, show that the action of $\mathrm{Aut}(Q)$ on the arcs of Q is also imprimitive.

If a graph is not connected, its components will form a system of imprimitivity. Thus we will only consider connected graphs from now on. If X is s-arc-transitive, then X is regular (every vertex has the same valency). We can talk about k, the valency of graph. When $k = 0$, it is K_1. When $k = 1$, we have K_2. When $k = 2$, the graph must be a cycle. We will focus on $k \geq 3$.

1.4.1 Theorem (Tutte)**.** *If X is an s-arc-transitive graph with valency at least 3 and girth g, then $g \geq 2s - 2$.*

Proof. We may assume that $s \geq 3$. First we will show that $s \leq g$. Suppose $s > g$; X is also g-arc-transitive. But X has a cycle of length g and also a path of length g. These give two different types of g-arcs which cannot be mapped to each other by an automorphism, giving a contradiction.

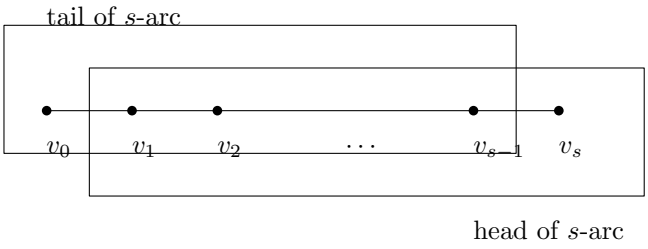
Now we may suppose that $s \leq g$. Let $\alpha = (v_0, \ldots, v_s)$ is and s-arc on some shortest cycle C. We observe that v_{s-1} has degree at least 3, and so it is adjacent to some vertex $w \notin \{v_s, v_{s-2}\}$. Let $\beta = (v_0, \ldots, v_{s-1}, w)$. We see that β is an s-arc and, since $\mathrm{Aut}(X)$ is transitive on the s-arcs, we must be able to map α to β. Thus β must lie on a shortest cycle C' of length g. Thus C, C' are distinct cycles and they have $s - 1$ edges in common.

If we delete $v_i v_{i+1}$ for $i = 0, \ldots, s-2$, the graph still has a cycle (formed by the union of C and C' with these edges deleted) of length at most $2g - 2s + 2$. Hence $2g - 2s + 2 \geq g$. □

1.4.1 Arc graph

Let $s \geq 1$ and we let $\alpha = (v_0, v_1, \ldots, v_{s-1}, v_s)$ be an s-arc of X. We define the *head* of α to be the $(s-1)$-arc $(v_1, \ldots, v_{s-1}, v_s)$ and the *tail* of α to be $(v_0, v_1, \ldots, v_{s-1})$.

Let α, β be s-arcs. We say that β *follows* α if there is an $(s+1)$-arc



γ such that the head of γ is β and the tail of γ is α. We "shunt" α into β.

Let s be a non-negative integer. $X^{(s)}$ is the directed graph with the s-arcs of X as its vertices such that (α, β) is a directed edge of $X^{(s)}$ if and only if β follows α. If X is s-arc-transitive, then $X^{(s)}$ is vertex-transitive.

Recall that a directed graph is *strongly connected* if for any pair of vertices x, y there is a directed path from x to y and from y to x.

1.4.2 Lemma. *Let X be a connected graph with minimum valency 2 such that X is not a cycle. Then $X^{(s)}$ is strongly connected for all $s \geq 0$.*

Proof. Left as an exercise (for the second half of the class). □

Though we will not show that for any s-arc-transitive cubic graph that s at most 5, we will see some of the group theory setup in the proof.

1.4.3 Lemma. *Suppose X is a strongly connected directed graph and $G \leq \mathrm{Aut}(X)$ is transitive. For $u \in V(X)$, let $N(u) = \{v \mid uv \in E(X)\}$. If there exists $u \in V(X)$ such that all elements of G_u act as the identity on $N(u)$, then G is regular.*

Proof. For any $v \neq u$, recall that G_v is conjugate to G_u, thus G_v also fixes $N(v)$, the out-neighbours of v.

If G_u is not trivial, then it contains some element which is not the identity. Let w be a vertex which is not fixed by G_u. Since X is strongly connected, there is a directed path P of shortest length from u to w where $P = (v_0 = u, v_1, \ldots, v_{k-1}, v_k = w)$. There is a largest index i such that v_i is fixed by every element of G_u and v_{i+1} is not; this exists since v_1 is fixed by G_u and w is not.

We observe that since G_u also fixes v_i, we have that $G_u \leq G_{v_i}$ and so G_u also fixes $N(v_i)$ element-wise. But $v_{i+1} \in N(v_i)$ is not fixed by G_u, by our choice of i, a contradiction. □

A graph is s-arc-regular if for any two s-arcs there is a unique automorphism mapping the first arc to the second.

1.4.4 Lemma. *Let X be a connected cubic graph that is s-arc-transitive but not $(s+1)$-arc-transitive. Then X is s-arc-regular.*

Proof. Observe that if X is cubic, then $X^{(s)}$ has out-valency 2. Let $G = \mathrm{Aut}(X)$ and let α be an s-arc in X. Let $H \leq G$ fixing each vertex in α. We observe that action of G on $X^{(s)}$ is vertex-transitive and H is the stabilizer of α in $X^{(s)}$.

If H does not fix both out neighbours of α (element-wise), then H must swap them. Then these $(s+1)$-arcs in the original graph X can be swapped by the action of H. Any $(s+1)$-arcs can be mapped to an $(s+1)$-arc that starts with α. Then, since G is transitive on the two $(s+1)$ arcs which start with α, G acts transitively on the $(s+1)$-arcs of X, which gives a contradiction. Thus H must fix the two neighbours of α and so, by the previous lemma, G acts regularly on $X^{(s)}$. □

If X is a directed graph such that $\mathrm{Aut}(X)$ acts regularly on $V(X)$. What is $|\mathrm{Aut}(X)|$? It is just $|V(X)|$. If X is s-arc-regular, then $|\mathrm{Aut}(X)|$ is the number of s-arcs of X.

Let X be a graph of valency k on n vertices and let $s \geq 1$. There are exactly

$$nk(k-1)^{s-1}$$

s-arcs. If X is s-arc-regular, then

$$|\mathrm{Aut}(X)| = nk(k-1)^{s-1}.$$

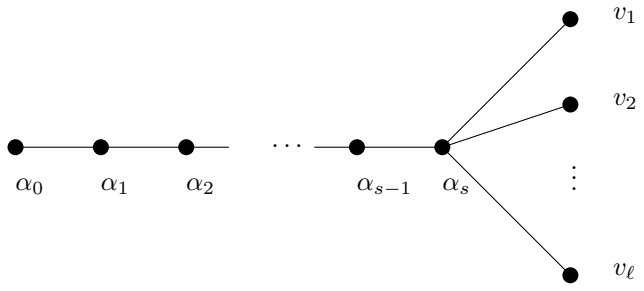
If X is s-arc-transitive, $nk(k-1)^{s-1}$ divides $|\mathrm{Aut}(X)|$.

In particular, suppose X is cubic and s-arc-regular then

$$|\mathrm{Aut}(X)| = (n3)2^{s-1}.$$

1.5 *Symmetric Graphs continued*

For the whole lecture today, we will work with an s-arc $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_s)$ where α_s has neighbours α_{s-1} and $v_1, \ldots, v_\ell$.



1.5.1 Lemma. *For any connected graph of minimum degree at least* 3*. If* $s \geq 1$*, then the s-arc graph is strongly connected.* □

Let $\beta_i = (\alpha_1, \ldots, \alpha_s, v_i)$ for $i = 1, \ldots, \ell$; each β_i is a successor of α.

1.5.2 Theorem. *Let X be a connected k-regular graph with $\ell = k-1 \geq 2$ and let α be as above. Then* $\mathrm{Aut}(X)$ *is transitive on the s-arcs if and only if it contains automorphism $g_1, \ldots, g_\ell$ such that g_i takes α to β_i, for $i = 1, \ldots, \ell$.*

Proof. The condition is clearly satisfied if $\mathrm{Aut}(X)$ is transitive on the s-arcs.

Conversely, suppose $g_1, \ldots, g_\ell$ do exist. Let $H = \langle g_1, \ldots, g_\ell \rangle$ be a subgroup of $\mathrm{Aut}(X)$. We will show that H acts transitively on the s-arcs.

Let θ be α^h for some $h \in H$. If ϕ is any successor of θ, then $\phi^{h^{-1}}$ is a sucessor of α and so is β_i, say. Then $\phi = \alpha^{g_i h}$ and is thus in the same orbit as α under the action of H. By iteratively applying this argument, we have shown that if there is a path from θ, in the s-arc graph, to some s-arc ϕ, then ϕ is in the same orbit as α.

Since the s-arc graph is strongly connected, we obtain that all s-arcs are in the same orbit as α. □

1.5.3 Example. Recall that the Petersen graph has vertices which are 2-subsets of $\{1,2,3,4,5\}$ and disjoint subsets are adjacent (it is also the Johnson graph $J(5,2,0)$). Recall that S_5 acts on the Petersen graph. The girth of the Petersen graph is 5 so it can be at most 3-arc-transitive. Is it 3-arc-transitive? The 3-arc

$$\alpha = (12, 34, 15, 23)$$

has two successors, namely, $\beta_1 = (34, 15, 23, 14)$ and $\beta_2 = (34, 15, 23, 45)$. The automorphism $(13)(245)$ takes α to β_1, and (13524) takes α to β_2. Our theorem now gives that the Petersen graph is 3-transitive.

This gives us a useful test for s-arc-transitivity, but also we will use it to look at the structure of s-arc-transitive groups.

Let X be a s-arc transitive graph with s-arc α as before. The *stabilizer sequence* of α is the sequence

$$\mathrm{Aut}(X) = G > F_s > F_{s-1} > \cdots > F_1 > F_0$$

of subgroups of G where F_i is the point-wise stabilizer of $\{\alpha_0, \ldots, \alpha_{s-i}\}$.

1.5.4 Example. In the Petersen graph, look again at $(12, 34, 15, 23)$.

$$\begin{aligned} F_0 &= \langle \varepsilon \rangle \\ F_1 &= \langle (34) \rangle \\ F_2 &= \langle (12), (34) \rangle \\ F_3 &= \langle (12), (34), (45) \rangle \end{aligned}$$

whose orders are 1, 2, 4, 12, respectively.

What are the orders of the subgroups in general? It is determined by the order of F_0.

What is the order of F_s? Since F_s is the stabilizer of the single vertex α_0 and $G = \mathrm{Aut}(X)$ is vertex-transitive, we can apply the Orbit-Stabilizer theorem and obtain $|G : F_s| = n$, where n is the number of vertices of X.

Since G is transitive on the 1-arcs, F_s acts transitively on the k vertices adjacent to α_0. Now F_{s-1} is the stabilizer of α_1 in this action. Thus $|F_s : F_{s-1}| = k$ by the Orbit-Stabilizer theorem.

Since G is transitive on the j-arcs for $2 \leq j \leq s$, the group F_{s-j+1} acts transitively on the $k-1$ vertices adjacent to α_{j-1}, other than α_{j-2}. Now F_{s-j} is the stabilizer of α_j in this action. Thus $|F_{s-j+1} : F_{s-j}| = k-1$ by the Orbit-Stabilizer theorem.

Thus we have

$$|F_j| = (k-1)^j |F_0|, \quad 0 \le j \le s-1$$
$$|F_s| = k(k-1)^{s-1}|F_0|$$
$$|G| = nk(k-1)^{s-1}|F_0|.$$

This is consistent with what we found for the Petersen graph.

There are no 8-arc transitive graphs; Weiss showed (1983) uses classification theorems in group theory to show that no finite graph, other than cycles, admit a transitive action on its 8-arcs. 7-arc transitive graphs do exists. Smallest is on 728 vertices and is 4-regular and bipartite.

Recall $\{g_1, \ldots, g_\ell\}$, which are $\ell = k-1$ automorphism whose existence is guaranteed. We will take an increasing sequence of subsets of G, $\{\varepsilon\} = Y_0 \subseteq Y_1 \subseteq \cdots$ as follows:

$$Y_i = \{g_a^{-j} g_b^j \mid a, b \in \{1, 2, \ldots, \ell\},\ 1 \le j \le i\}.$$

1.5.5 Lemma. *(i) If $1 \le i \le s$, then $Y_i \subseteq F_i$, but not a subset of F_{i-1}.*

(ii) If $0 \le j \le s$, the group F_i is the subgroup of G generated by Y_i and F_0.

Proof. (Sketch) For (i), observe that $g_a^{-j} g_b^j$ fixes $\alpha_0, \alpha_1, \ldots, \alpha_{s-i}$, for all $j \le i$.

For part (ii), suppose $f \in F_i$. We know that

$$\alpha^f = (\alpha_0, \alpha_1, \ldots, \alpha_{s-i}, \gamma_1, \ldots, \gamma_i).$$

Consider $\alpha^{f g_b^j a^{-j}}$ and eventually show that $f \in \langle Y_i, F_0 \rangle$. □

All elements of $Y_0, Y_1, \ldots, Y_s$ fix the vertex α_0 and so belong to F_s, the stabilizer of α_0. Now we look at Y_{s+1}. This has elements not fixing α_0. Naturally, we would like to know if Y_{s+1} and F_0 generated all of G. The answer is yes, except when the graph is bipartite.

If X is a 1-arc-transitive bipartite graph with colour classes V_1 and V_2, then the automorphisms which fix V_1 and V_2 setwise form a subgroup of index 2 in $\mathrm{Aut}(X)$. We say that this subgroup *preserves the bipartition*.

1.5.6 Theorem. *Suppose X is s-arc-transitive with $s \ge 2$ and girth > 3. Let G^* be the subgroup of $G = \mathrm{Aut}(X)$ generated by Y_{s+1} and F_0. Then either $G = G^*$ or X is bipartite, $|G : G^*| = 2$, and G^* is the subgroup of G preserving the bipartition.*

Proof. Let u be any vertex at distance 2 from α_0.

First we will show that there is some element of G^* taking α_0 to u. Since the girth is bigger than 3, the neighbours of α_s are not adjacent to each other. So $d(v_i, v_j) = 2$. Pick a, b and let $v_a = \alpha_0^{g_a^{s+1}}$ and $v_b = \alpha_0^{g_b^{s+1}}$, which are also at distance 2. We have that G^* contains F_s and F_s is transitive on 2 arcs that begin at α_0. So G^* contains some f which fixes α_0 and takes $x = \alpha_0^{g_a^{s+1} g_b^{-(s+1)}}$ (which

is at distance 2 from α_0, since v_a and v_b are distance 2 from each other) to u and now g^* is the composition of $g_a^{s+1}g_b^{-(s+1)}$ and f takes α_0 to u.

Let U be the orbit of α_0 under the action of G^*. We just showed the U contains all vertices at distance 2 from α_0, and, consequently, all vertices whose distance from α_0 is even. If $U = V(X)$, then G^* is transitive on $V(X)$ and also contains F_s. By Orbit-Stabilizer theorem,

$$|G^*| = |V(X)||F_s| = |G|$$

and so $G^* = G$. Otherwise, $U \neq V(X)$ and U contains exactly the even distanced vertices from α_0. □

The girth restriction is not very restriction; the only 2-arc transitive graph of girth 3 are the complete graphs.

1.6 *Symmetric Cubic Graphs*

A graph X is *(sharply) s-transitive* if $\mathrm{Aut}(X)$ acts transitively on the s-arcs but not on the $(s+1)$-arcs. Recall that, in this case, $\mathrm{Aut}(X)$ acts regularly on the s-arcs.

Let X be a cubic, s-transitive graph with s-arc α. The stabilizer sequence is

$$\mathrm{Aut}(X) = G > F_s > F_{s-1} > \cdots > F_1 > F_0.$$

Since the action on the s-arcs is regular and F_0 fixes a s-arc, we have that $|F_0| = 1$. So now we get the orders of the other groups:

$$\begin{aligned} |F_i| &= 2^i, \quad 0 \leq i \leq s-1 \\ |F_s| &= 3(2^{s-1}) \\ |G| &= n3(2^{s-1}) \end{aligned}$$

where n is the number of vertices. For cubic graphs, not only can we say things about the sizes of the groups, but also about the group structure.

We will let g_1, g_2 be as in Figure 1.3 and $x_0 = g_2 g_1^{-1}$.

Let $g = g_1$ and let $x_i = g^i x_0 g^{-i}$

1.6.1 Lemma. *The stabilizer sequence of a cubic s-transitive graph with $s \geq 2$ has the following properties:*

1. $F_i = \langle x_0, x_1, \ldots, x_{i-1} \rangle$ *for* $i = 1, 2, \ldots, s$;
2. *if* $G^* = \langle x_0, x_1, \ldots, x_s \rangle$ *then* $|G : G^*| = 2$;
3. $G = \langle x_0, g \rangle$.

We will not prove this lemma, but we should note a few things. Each x_i is an involution and each element of $f \in F_i$ has a unique expression of the form

$$f = x_{i_1} \cdots x_{i_j}$$

where $i_1 > i_2 > \cdots > i_j$. There are 2^i such expressions and F_i has 2^i elements.

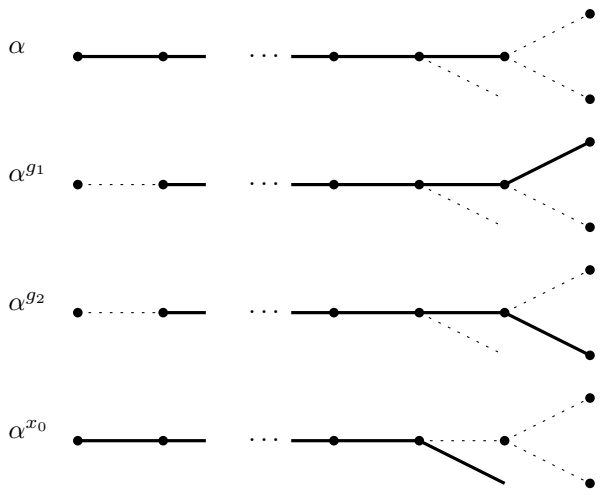


Figure 1.3: A s-arc α in X with g_1, g_2, x_0 acting on it.

What more can we say? Which of these stabilizer groups are abelian? Let λ be the largest natural number such that F_λ is abelian. We know that $\lambda \geq 2$ since F_2 has order 4.

1.6.2 Lemma. *If $s \geq 4$, then $2 \leq \lambda < \frac{1}{2}(s+2)$.*

Proof. Suppose $F_\lambda = \langle x_0, x_1, \ldots, x_{\lambda-1} \rangle$ is abelian. Then its conjugate $g^{s-\lambda+1} F_\lambda g^{-(s-\lambda+1)}$ is also abelian and it is

$$\langle x_{s-\lambda+1}, \ldots, x_s \rangle.$$

If $\lambda - 1 \geq s - \lambda + 1$, then both of these groups have to contain $x_{\lambda-1}$ and together they generate G^*. Now we have that $x_{\lambda-1}$ commutes with all of the elements of G^*, in particular it commutes with g^2 (since $g \in G$ and $|G : G^*| = 2$) and so

$$x_{\lambda-1} = g^2 x_{\lambda-1} g^{-2} = x_{\lambda+1}$$

from whence we will obtain $x_0 = x_2$, which is not possible. □

This gives us an upper bound for λ in terms of s. We can also find a lower bound by doing similar analysis with commutators ($[a,b] = a^{-1}b^{-1}ab$) of x_i's. We will skip the details just state the result. One can show that

$$[x_0, x_\lambda] = x_\nu \cdots x_\mu$$

where the indices are decreasing. Further, we can obtain

$$\mu + \lambda \geq s - 1, \quad 2\lambda - \nu \geq s - 1.$$

1.6.3 Theorem (Tutte 1947)**.** *There is no finite s-transitive cubic graph with $s > 5$.*

Proof. If $s \geq 4$, then we can use the upper and lower bounds that we found for λ in terms of s and get

$$s - 1 - \lambda \leq \mu \leq \nu \leq 2\lambda - s + 1$$

and we can obtain from this that $\frac{1}{2}(s+2) > \lambda \geq \frac{2}{3}(s-1)$. The only integers s for which there exists a positive integer λ that can satisfy this equation are $4, 5, 7$. We leave the proof that no 7-transitive graphs exists to the reader. □

1.6.1 *Foster census*

Foster compiled a list of all cubic arc-transitive graphs up to a certain order. Up to 30 vertices, here is the complete list:

1. K_4;
2. $K_{3,3}$;
3. Q_3 the cube graph;
4. Petersen graph;
5. Heawood graph (14 vertices, bipartite, 4-transitive);
6. Pappus graph;
7. Generalized Petersen graph $P(8,3)$ and $P = (12,5)$;
8. Desargues Graph;
9. Dodecahedron graph;
10. 2 other graphs.

We will in fact meet the more general families that these graph belong to.

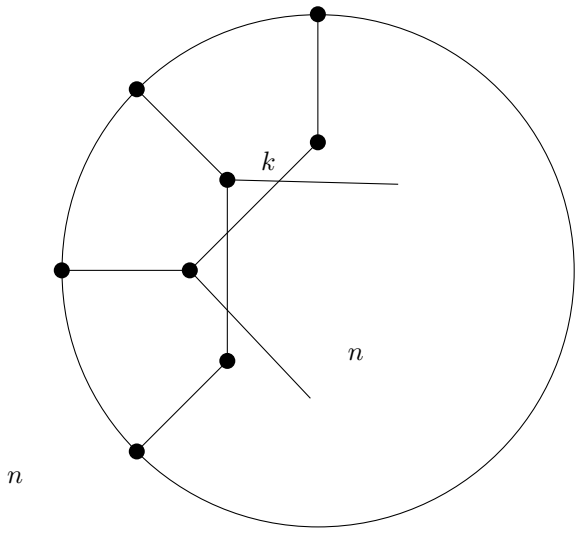


Figure 1.4: Generalized Petersen Graph $P(n,k)$.

The Heawood graph is a very special graph. Consider the following subsets of $\{1,2,\ldots,7\}$:

$$124, 235, 346, 457, 561, 672, 713.$$

This gives the smallest Steiner triple system and the smallest projective plane, which we will study later. The vertices of Heawood graph are the numbers $\{1,2,\ldots,7\}$ and the seven 3-subsets that we've listed; a number j and a 3-subset S are adjacent if $j \in S$. In general, this type of construction is the incidence graph of an incidence structure.

1.7 Edge transitivity

A graph X is *edge-transitive* if $\mathrm{Aut}(X)$ acts transitively on the edges. For example, the complete bipartite graph $K_{m,n}$ is edge-transitive but not arc-transitive or vertex-transitive, when $m \neq n$.

1.7.1 Lemma. *Let X be an edge-transitive graph with no isolated vertices. If X is not vertex-transitive, then $\mathrm{Aut}(X)$ has exactly two orbits and these are a bipartition of X.*

Proof. Suppose X is edge-transitive but not vertex-transitive, as in the statement. Let $\{x, y\}$ be an edge of X. If $w \in V(X)$, then w is on an edge, say $\{w, z\}$, which can be mapped to $\{x, y\}$ by some $g \in \mathrm{Aut}(X)$. Thus w is in the same orbit as x or it is in the same orbit as y. Thus $\mathrm{Aut}(X)$ has two orbits.

An edge with both ends in the same orbit cannot be mapped to an edge with one end in each orbit; in particular, it cannot be mapped to $\{x, y\}$. Thus only edges with ends in different orbits can exists. □

1.7.2 Lemma. *If X is vertex-transitive and edge-transitive, but not arc-transitive, then its valency is even.*

Proof. Let $G = \mathrm{Aut}(X)$ and $x \in V(X)$. Let y be adjacent to x and let Ω be the orbit of G acting on $V \times V$ containing (x, y). Every arc of X can be mapped to (x, y) or (y, x) under G.

If X is not arc-transitive, then (y, x) is not in Ω. Thus every arc of X is in Ω or Ω^T (obtained by reversing the coordinates). The out valency of X is the same in Ω and Ω^T, thus valency of X is even. □

One can obtain as an immediate consequence that if X is vertex-transitive and edge-transitive with odd valency, then X is arc-transitive.

1.8 Distance-transitive

A connected graph X is *distance-transitive* if given any two ordered pairs of vertices (u, u') and (v, v') such that $d(u, u') = d(v, v')$, there exists an automorphism taking (u, u') to (v, v').

Note that any automorphism has to map (u, u') to a pair (v, v') such that $d(u, u') = d(v, v')$. A distance-transitive graph is 1-arc-transitive. Example of distance-transitive graphs include K_n, $K_{m,m}$, C_n, Petersen graph, Heawood graph, dodecahedron graph and many others.

1.8.1 Lemma. *The Johnson graph $J(v, k, k-1)$ is distance transitive.*

Proof. Observe that (u, v) are at distance i if and only if $|u \cap v| = k - i$. □

Consider a distance-transitive graph X of diameter d. There are $d + 1$ orbitals. Let x, y be vertices of X at distance k. Now consider the following set of vertices:

$$S(x, y) = \{z \mid d(z, x) = i,\ d(z, y) = j\}.$$

Let u, v also be vertices at distance k and consider $S(u, v)$ with the same i, j. Since there is an automorphism of X which takes (x, y) to (u, v), we have that

$$|S(x, y)| = |S(u, v)|.$$

This means that this size does not depend on the choice of x, y, but only on k, i, j. For any distance-transitive graph, there exists constants p_{ij}^k such that for any pair of vertices x, y at distance k,

$$p_{ij}^k = |\{z \mid d(z, x) = i,\, d(z, y) = j\}|.$$

A *distance-regular graph* is a connected graph such that there exists constants p_{ij}^k such that for any pair of vertices x, y at distance k,

$$p_{ij}^k = |\{z \mid d(z, x) = i,\, d(z, y) = j\}|.$$

So distance-regular is a "combinatorial relaxation" of an algebraic property. In the case when diameter is 2, the graph is *strongly regular* and we will study many such graphs.

2
Graphs and Matrices

To every graph, one can associate several matrices and then find the eigenvalues of these matrices. Some graph properties can be reconstructed from the eigenvalues of these matrices.

For a matrix A, an *eigenvalue* λ is a number such that there exists a vector $\mathbf{v} \neq 0$. such that

$$A\mathbf{v} = \lambda\mathbf{v}.$$

The vector $\mathbf{v}$ is an *eigenvector*.

For a graph X, the *adjacency matrix*, denoted $A = A(X)$, is a matrix with row and columns index by $V(X)$ such that

$$A(x,y) = \begin{cases} 1, & \text{if } xy \in E(X); \\ 0, & \text{otherwise.} \end{cases}$$

Note that our graph are simple graphs without loops; our adjacency matrices will be 01-matrices that are symmetric and have 0s on the diagonal.

The *minimal polynomial* of A is polynomial ψ of smallest degree in $\mathbb{R}[t]$ such that $\psi(A) = 0$.

The *characteristic polynomial* of A, denoted $\phi(A,t)$, is

$$\phi(A,t) = \det(tI - A).$$

2.0.1 Theorem (Cayley-Hamilton)**.** $\phi(A,A) = 0$.

In otherwise, each matrix satisfies its own characteristic polynomial and thus the minimal polynomial is well-defined. Since we are focussing on adjacency matrices, we will speak of the eigenvalues of $A(X)$ and X interchangeably. For example, we will write $\phi(X,t) = \phi(A(X),t)$.

The minimal polynomial of A divides the characteristic polynomial of A. Suppose that λ is a root of $\phi(A,t)$. We have that $\det(\lambda I - A) = 0$ if and only if $\lambda I - A$ is not invertible, which is if and only if there exists a non-zero vector $\mathbf{v}$ in its kernel;

$$(\lambda I - A)\mathbf{v} = 0 \Leftrightarrow A\mathbf{v} = \lambda\mathbf{v}.$$

So each roots λ of $\phi(A,t)$ is an eigenvalue. The *algebraic multiplicity* of an eigenvalue λ is the multiplicity of λ as a roots of $\phi(A,t)$. The vector space

$$\langle \mathbf{v} \mid A\mathbf{v} = \lambda\mathbf{v} \rangle$$

is the λ-eigenspace of A and its dimension is the *geometric multiplicity* of λ.

2.0.2 Theorem. *(i) If A is symmetric (Hermitian), then the geometric and algebraic multiplicities are equal for every eigenvalue.*

(ii) If A is symmetric (Hermitian), then A has n real eigenvalues with real eigenvectors.

An *eigenbasis* is a basis of $\mathbb{R}^{V(X)}$ of eigenvectors of A.

2.0.3 Example. What are the eigenvalues of C_n, the cycle graph?

Solution. We can write the adjacency matrix of C_n as follows:

$$A(C_n) = D_n + D_n^T$$

where D_n is the permutation matrix taking e_i to e_{i+1}, where the indices are modulo n. For example:

$$A(C_4) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = D_4 + D_4^T.$$

Let ζ be a primitive nth root of unity. Let $\xi = \zeta^k$ for some $0 \leq k \leq n-1$. Let $\mathbf{v}_\xi$ be as follows:

$$\mathbf{v}_\xi = \begin{pmatrix} \xi^0 \\ \xi^1 \\ \xi^2 \\ \vdots \\ \xi^{n-1} \end{pmatrix}.$$

We observe that

$$D_n \mathbf{v}_\xi = \begin{pmatrix} \xi^{n-1} \\ \xi^0 \\ \xi^1 \\ \vdots \\ \xi^{n-2} \end{pmatrix} = \xi^{-1}\mathbf{v}_\xi \text{ and } \quad D_n^T \mathbf{v}_\xi = \begin{pmatrix} \xi^1 \\ \xi^2 \\ \vdots \\ \xi^{n-1} \\ \xi^0 \end{pmatrix} = \xi \mathbf{v}_\xi.$$

And so

$$A(C_n)\mathbf{v}_\xi = D_n\mathbf{v}_\xi + D_n^T\mathbf{v}_\xi = \xi^{-1}\mathbf{v}_\xi + \xi\mathbf{v}_\xi = (\xi^{-1} + \xi)\mathbf{v}_\xi = 2Re(\xi)\mathbf{v}_\xi.$$

If $\zeta = e^{2\pi i/n}$, then $\xi = e^{2\pi ik/n}$ and the eigenvalue is $2\cos(2\pi k/n)$. That these are linearly independent is left as an exercise.

Also an exercise, this above method of finding eigenvectors works for any Cayley of an abelian group. For the cubelike graphs, this is particularly nice because this implies that they have an eigenbasis where every vector is a $1, -1$ vector. What does it mean for the graph to have an eigenvector? For us combinatorialists, this is the meaning: for every vertex x, consider the x row of

$$A\mathbf{v} = \lambda\mathbf{v}.$$

We get

$$\sum_{y \sim x} \mathbf{v}(y) = \lambda \mathbf{v}(x)$$

For any cubelike graph, this shows that every eigenvalue is an integer between $-k$ and k where k is the degree. This is why they were studied; Lovasz needed examples of infinite families of graphs with integer eigenvalues.

An eigenvalue is said to be *simple* if its multiplicity is 1.

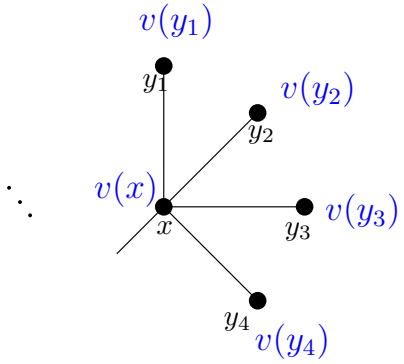


Figure 2.1: We consider an eigenvector as an eigenfunction on the vertices of the graph.

2.0.4 Theorem. *If X is vertex-transitive graph with at least one edge where every eigenvalue is simple, then X is isomorphic to K_2.*

Proof. For any permutation $\sigma \in \mathrm{Sym}(V(X))$, we can represent σ by a permutation matrix P_σ, indexed by $V(X)$, such that

$$P_\sigma e_x = e_{x^\sigma}.$$

One can verify that an automorphism of X is exactly a permutation matrix P which commutes with A (observe that $P^T A P = A$).

Let $\mathbf{v}$ be a real eigenvector of X with eigenvalue λ and we consider $P\mathbf{v}$, for an automorphism P. We see

$$A(P\mathbf{v}) = PA\mathbf{v} = P(\lambda \mathbf{v}) = \lambda(P\mathbf{v})$$

and thus $P\mathbf{v}$ is also an eigenvector of X with the same eigenvalue, λ. Since all eigenvalues of X are simple, we have that $P\mathbf{v}$ is a scalar multiple of $\mathbf{v}$. But P is a permutation matrix: $\|\mathbf{v}\| = \|P\mathbf{v}\|$ and so $P\mathbf{v} = \pm\mathbf{v}$.

Since X is vertex-transitive, for vertices x, y, there exists some automorphism P such that $Pe_x = e_y$ and $e_x^T P^T = e_y^T$, thus

$$(P^T\mathbf{v})(x) = e_x^T P^T \mathbf{v} = e_y^T \mathbf{v} = \mathbf{v}(y).$$

We obtain in this way that there is some real number α such that $\mathbf{v}(y) = \pm\alpha$ for all $y \in V(X)$. We may scale $\mathbf{v}$ and so we can assume without loss of generality that $\alpha = 1$.

Let x be a vertex of X. We have

$$\sum_{y \sim x} \mathbf{v}(y) = \lambda \mathbf{v}(x).$$

Let k be the degree of the graph. Let β be the number of neighbours y of x such that $\mathbf{v}(y) = -1$. Then

$$\pm\lambda = \sum_{y\sim x} \mathbf{v}(y) = \beta(-1) + (k-\beta) = k - 2\beta.$$

Thus, if λ is a simple eigenvalue of a vertex-transitive graph, then $\lambda = k - 2\beta$ for $\beta = 0, \ldots, k$. Thus X has at most $k+1$ simple eigenvalues. If X has n simple eigenvalues, then $n = k+1$ and X is a complete graph. We will show shortly that the eigenvalues of K_n are $n-1$ with multiplicity 1 and -1 with multiplicity $n-1$. So K_2 is the only possibility. □

2.1 *Spectral decomposition*

Suppose θ is an eigenvalue of a symmetric matrix A. Let E_θ be orthogonal projection onto the θ-eigenspace of A; for any vector $\mathbf{v}$, we have that $E_\theta\mathbf{v}$ is an eigenvector of A with eigenvalue θ and $E_\theta^2 = E_\theta$ (thus E_θ is an *idempotent* matrix). If $\tau \neq \theta$ is an eigenvalue, then

$$E_\theta E_\tau = 0.$$

Let $ev(A)$ be the set of distinct eigenvalues of A. Since there exists an eigenbasis,

$$\sum_{\theta\in ev(A)} E_\theta = I$$

where I is the identity matrix. We see that

$$A = \sum_{\theta\in ev(A)} \theta E_\theta. \tag{2.1.1}$$

This equation (2.1.1) is said to be the *spectral decomposition* of A.

A note on eigenvalues; any eigenvalue of a graph must be a real algebraic integer, since the characteristic polynomial is a monic polynomial with integral coefficients. Further, they are *totally real* (all algebraic conjugtes are real) algebraic integers.

2.1.1 Theorem. *If A, B are Hermitian, $n \times n$ matrices that commute, then A, B share a common eigenbasis of $\mathbb{R}^n$.*

This is also true, then, for a set of pariwise commuting matrices.

2.1.2 Example. What are the eigenvalues of K_n?

Solution. $A(K_n) = J_n - I_n$, where J_n is the $n \times n$ all ones matrix. But I_n commutes with any matrix, so there is a common eigenbasis $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Since J_n has rank 1, it has only 1 non-zero eigenvalue, which is n. Let $E_n = \frac{1}{n}J_n$ and $E_0 = I - E_n$. The spectral decomposition of $A(K_n)$ is the following:

$$A(K_n) = (n-1)E_n + (-1)E_0.$$

2.2 Perron-Frobenius

A matrix M is *irreducible* if for all i, j there exists k such that $M^k(i,j) \neq 0$. The adjacency matrix of X is irreducible if and only if X is connected.

A matrix M is *primitive* if for some k, we have that all entries of M^k are positive. We note that if M is irreducible, then $M + I$ will be primitive.

The *period* d of M is the greatest common divisor of all k such that all diagonal entries are positive in M^k.

2.2.1 Theorem (Perron-Frobenius)**.** *Suppose M is an irreducible matrix with non-negative entries. There exists a unique positive $\theta \in \mathbb{R}$ such that*

(i) there exists a real vector $\mathbf{v}_0 > 0$ such that $M\mathbf{v}_0 = \theta\mathbf{v}_0$;

(ii) θ is a simple eigenvalue;

(iii) if $\tau \neq \theta$ is an eigenvalue of M, then $|\tau| \leq \theta$.

(iv) if M is primitive, then if $\tau \neq \theta$ is an eigenvalue of M, then $|\tau| < \theta$.

(v) if M has period d, then M has d eigenvalues τ with $|\tau| = \theta$, namely, $\theta e^{\frac{2\pi ij}{d}}$ for $j = 0, 1, \ldots, d-1$.

2.2.2 Lemma. *If X is a graph with diameter d, then $A(X)$ has at least $d + 1$ distinct eigenvalues.*

Proof. Exercise. □

2.3 Interlacing

Suppose $\lambda_1 \geq \cdots \geq \lambda_n$ and $\mu_1 \geq \cdots \geq \mu_m$ are real numbers. We say that $(\mu_i)_{i=1}^m$ *interlaces* $(\lambda_i)_{i=1}^n$ if

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}$$

for $i = 1, \ldots, m$. When $m = n - 1$, this will say that μ_i is between λ_i and λ_{i+1}. The interlacing is *tight* if there exists $k \in [1, \ldots, m]$ such that

$$\lambda_i = \mu_i, \quad i = 1, \ldots, k$$

and

$$\mu_i = \lambda_{n-m+i}, \quad i = k+1, \ldots, m.$$

2.3.1 Theorem (Interlacing of principal minors)**.** *If A is a Hermitian matrix and B is a prinicipal submatrix of A, then the eigenvalues of B interlace those of A.*

This tells us, for example, that if Y is an induced subgraph of X then the eigenvalues of Y interlace those of X.

It's not immediately apparent, but the following is an equivalent theorem.

2.3.2 Theorem (Cauchy Interlacing)**.** *Let A be a Hermitian $n \times n$ matrix and $S \in \mathbb{C}^{n\times m}$ and $S^*S = I$. If $B = S^*AS$, then the eigenvalues of B interlace those of A. Furthermore, if the interlacing is tight, then $SB = AS$.*

We will not prove either of these, but we will use them. Mainly, for a graph X, we can find some (usually smaller) weighted graph whose eigenvalues interlacing those of X.

Let $\mathcal{P} = \{P_1, \dots, P_m\}$ be a partition of $[1, \dots, n]$ and let A be an $n \times n$ matrix. We assume the rows and columns of A are ordered such that we can write A as a block matrix

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & & & A_{2m} \\ \vdots & & \ddots & \\ A_{m1} & \cdots & & A_{mm} \end{pmatrix}$$

where A_{ij} is the submatrix of A with rows and columns indexed by P_i, P_j, respectively. The *quotient matrix* of A with respect to $\mathcal{P}$ is the $m \times m$ matrix B such that

$$B_{ij} = \frac{1}{|P_i|} 1^T A_{ij} 1$$

that is, B_{ij} is the average row sum of the ij-block of A.

2.3.3 Corollary. *If X is a graph and $\mathcal{P}$ is a partition of the vertices of X. Let B be the quotient matrix of $A(X)$ with respect to $\mathcal{P}$. The eigenvalues of B interlace those of A.*

If A_{ij} is a matrix with constant row sums for all $i, j \in [1, \dots, n]$, then we say that $\mathcal{P}$ is an *equitable* partition of the rows of A. If $A = A(X)$ is the adjacency matrix of X, then we say that $\mathcal{P}$ is an *equitable partition* of X.

2.3.4 Theorem (Equitable Partitions)**.** *If X is a graph and $\mathcal{P}$ is an equitable partition of the vertices of X. Let B be the quotient matrix of $A(X)$ with respect to $\mathcal{P}$. The eigenvalues of B are a subset of those of A.*

Every graph has an equitable partition; the partition into singletons is equitable. If X is k-regular, then the partition into 1 part, is equitable. In this case the quotient is $\begin{pmatrix} k \end{pmatrix}$ whose only eigenvalues is k and is the Perron eigenvalue of X.

2.3.5 Lemma. *A partition of the vertices of X into orbits of a group G acting on X is equitable.*

Proof. We have $G \leq \mathrm{Aut}(X)$ and let $O_1, \dots, O_m$ be the orbits of this action. Note that this is a partition of the vertices and is a system of blocks of imprimitivity.

Let $u, v \in O_i$. Then there is $\alpha \in G$ such that $u^\alpha = v$. Then, α fixes O_i, O_j set-wise. Thus u, v must have the same number of neighbours in O_j for any j. □

We call such partitions *orbit partitions*. An equivalent definition for equitable partition is the following: $\mathcal{P} = \{P_1, \ldots, P_m\}$ is an equitable partition of X if the number of neighbours of a vertex $u \in P_i$ which are in P_j is a constant b_{ij}, which does not depend on the choice of u, for all $i, j \in [1, \ldots, m]$.

Not all equitable partitions are orbit partitions; see Figure 2.2.

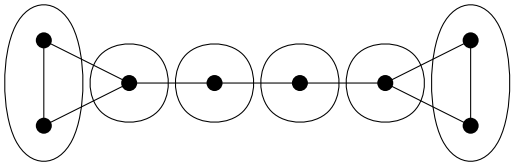


Figure 2.2: An equitable partition.

Another interesting partition that we can take the distance partition. Let X be a connected graph with diameter d. We define

$$X_i(v) = \{u \in V(X) \mid d(u, v) = i\}$$

for a vertex v. Then $X_0 = \{v\}$ and the non-empty parts of

$$X_0(v), X_1(v), \ldots, X_d(v)$$

gives a partition. This is called the *distance partition*.

Figure 2.3 shows the distance partition of $K_{3,3}$. This partition is equitable; we will this is always true for any distance regular graph.

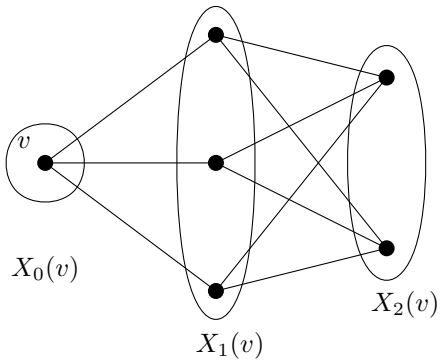


Figure 2.3: The distance partition of $K_{3,3}$, with respect to v.

Though it is not a focus of our course, many graph parameters are bounded by functions of the eigenvalues, which are proven with interlacing. For example, if you take a k-regular graph and you consider an independent set S in it. We take the partition that is $\{S, V \setminus S\}$ and quotient matrix is

$$\begin{pmatrix} 0 & k \\ \frac{|S|k}{n-|S|} & k - \frac{|S|k}{n-|S|} \end{pmatrix}.$$

This gives you a bound on the size of any independent set in terms of k and τ the least eigenvalues of A; after some simplification, we get

$$\tau \geq \frac{-k|S|}{n - |S|}.$$

Rearranging for $|S|$ will give the Delsarte-Hoffman bound.

2.4 *Distance-transitive graphs again*

We could have defined distance-transitive in various other ways and here's a theorem about how we could have defined it with distance partitions.

2.4.1 Theorem. *A connected graph X of diameter d and $G = \mathrm{Aut}(X)$ is distance-transitive if and only if X is vertex-transitive and the orbits of stabilizer G_v is the distance partition of X with respect to v.*

Proof. Suppose that X is distance-transitive. Suppose $d(u,v) = d(x,y)$. If we take $u = v$ and $x = y$, we obtain that X is vertex-transitive. If $v = y$, we get that G_v is transitive on $X_i(v)$, for all i.

Conversely, suppose we have vertices u, v, x, y such that $d(u,v) = d(x,y) = i$. Since X is vertex-transitive, there exists g such that $v^g = y$ and, since G_y is transitive on $X_i(v)$, there exists h such that $u^{gh} = x$. Now the element gh takes (u,v) to (x,y). □

From the previous section, we see that any orbit partition is equitable. For a distance-transitive graph, the distance partition with respect to any vertex is equitable. Further, since the graph is vertex-transitive, all of the quotient matrices obtained in this way should be equal. One can show that the following is equivalent definition of distance-regular graph: a connected graph X of diameter d is distance-regular if and only if the distance partition with respect to any vertex v is equitable and has quotient matrix B, which does not depend on the choice of vertex.

Recall that the *intersection numbers* of distance-transitive (distance-regular) graph are the following:

$$p_{ij}^k = |\{w \in V(X) \mid d(u,w) = i, d(v,w) = j\}| = |X_i(u) \cap X_j(v)|$$

where $d(u,v) = k$. How many intersection numbers are there? There are $(d+1)^3$ intersection numbers. It turns out that they are not all independent of each other; we only need $2d$ of them to determine the rest.

The intersection numbers satisfy the triangle inequality; if the sum of two of $\{i,j,k\}$ is strictly smaller than the third, then $p_{ij}^k = 0$. See Figure 2.4.

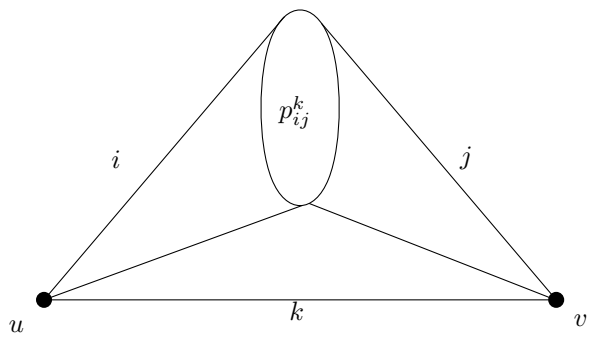


Figure 2.4: Intersection numbers satisfy the "triangle" inequality.

Fix $j = 1$. For j, $p_{i,1}^k$ is. the number of neighbours of v which are distance i from u, for u, v at distance k from each other. The

distance from u to some vertex w in the neighbourhood of v can only be $\{k, k-1, k+1\}$. Let

$$c_i = p^i_{i-1,1}, a_i = p^i_{i,1}, b_i = p^i_{i+1,1}.$$

for $i = 0, \ldots, d$, but we leave c_0 and b_d undefined. See Figure 2.5.

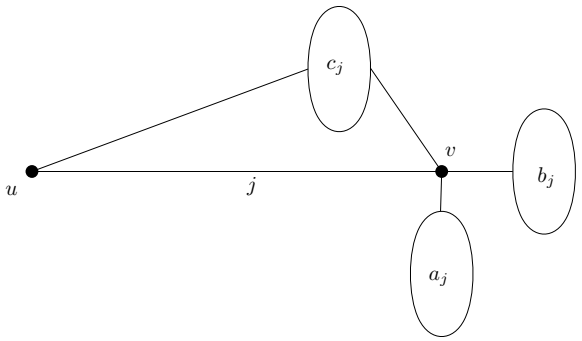


Figure 2.5: Intersection numbers satisfy the "triangle" inequality.

What is b_0? It is the valency of the graph, usually denoted k (since these graphs are regular). Also, $a_0 = 0$ and $c_1 = 1$. These three sets (in the figure) partition the neighbours of v, so

$$b_0 = a_i + b_i + c_i$$

for all i. We don't need all three of these (for each i). This leads us to define the *intersection array* of distance-transitive (-regular) graph to be

$$\{b_0, b_1, \ldots, b_{d-1}; c_1, c_2, \ldots, c_d\}.$$

2.4.2 Lemma. *If X is distance-transitive (-regular) with intersection array $\{b_0, b_1, \ldots, b_{d-1}; c_1, c_2, \ldots, c_d\}$ then,*

(i) $|X_{i-1}(v)|b_{i-1} = |X_i(v)|c_i$ *for* $1 \leq i \leq d$;

(ii) $1 \leq c_2 \leq \cdots \leq c_d$; *and*

(iii) $b_0 = k \geq b_1 \geq \cdots \geq b_{d-1}$.

We are finally ready to give the quotient of X with respect the distance partition. (Since all distance partitions give the same quotient matrix, we are suppressing the choice of vertex.) Let $X_0, X_1, \ldots, X_d$ be the distance partition with respect to some vertex. The quotient matrix is as follows

$$L_1 = \begin{pmatrix} 0 & b_0 & 0 & \cdots & 0 \\ c_1 & a_1 & b_1 & \cdots & 0 \\ 0 & c_2 & a_2 & b_2 & \\ \vdots & & \ddots & & \\ & & & c_d & a_d \end{pmatrix}.$$

This is a tridiagonal matrix with we have $\{a_i\}_{i=0}^d$ on the diagonal, $\{b_i\}_i^{d-1}$ above the diagonal and $\{c_i\}_{i=1}^d$ below the diagonal. We see that this $d+1 \times d+1$ matrix gives $d+1$ eigenvalues of X, since this

partition is equitable. We will see that it in fact gives all the distinct eigenvalues of X.

Some examples will help. The complete graph K_n is distance transitive. Its intersection array is $\{n-1;1\}$. The complete bipartite graph $K_{n,n}$ is also distance-transitive; its intersection array is $\{n, n-1;1,n\}$. The Petersen graph is distance-transitive; its intersection array is? An exercise.

2.5 Matrices

The *distance matrices* of a graph X are the following

$$(A_i)_{u,v} = \begin{cases} 1, & d(u,v) = i; \\ 0, & \text{otherwise} \end{cases}$$

for $i = 0, \ldots, d$, where d is the diameter of the graph. We can see $A_0 = I$, $A_1 = A$ the adjacency matrix, and $\sum_{i=0}^{d} A_i = J$, the all ones matrix.

2.5.1 Lemma. *For X with intersection array*

$$\{b_0, b_1, \ldots, b_{d-1}; c_1, c_2, \ldots, c_d\},$$

the distance matrices satisfy

$$AA_i = b_{i-1}A_{i-1} + a_iA_i + c_{i+1}A_{i+1}.$$

The proof is an exercise, but you only need know how to multiply two matrices. Suppose M, N are matrices index by V then

$$(MN)_{u,v} = \sum_{w \in V} M_{u,w}N_{w,v}.$$

Then, for a distance-regular graph X,

$$\begin{aligned} (A_iA_j)_{u,v} &= \sum_{w \in V(X)} (A_i)_{u,w}(A_j)_{w,v} \\ &= \sum_{w \in X_i(u), w \in X_j(v)} 1 \\ &= |X_i(v) \cap X_j(v)| = p_{ij}^k \end{aligned}$$

where $d(u,v) = k$. Thus

$$A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k.$$

We will next consider the matrix algebra generated by the distance matrices.

2.6 Bose-Mesner algebra

Recall that for a graph X, the distance matrix A_i is a matrix whose rows and columns are indexed by the vertices of X and $(A_i)_{u,v} = 1$

whenever $d(u,v) = i$ in X. Note that this defined for any connected graph and we can the following matrix algebra. Let $\mathcal{A}(X)$ be the matrix algebra generated the distance matrices of X; that is, if d is the diameter of X, we consider the matrix algebra generated by

$$A_0 = I, A_1 = A(X), A_2, \ldots, A_d.$$

This matrix algebra is called the *Bose-Mesner algebra* of X. What is a lower bound on the dimension of this algebra? Since $A_0, \ldots, A_d$ are linearly independent, the dimension of the Bose-Mesner algebra is at least $d+1$.

2.6.1 Theorem. *If X is a distance-regular graph of diameter d, the $\{A_0, \ldots, A_d\}$ is a basis of $\mathcal{A}(X)$, thus the dimension of the Bose-Mesner algebra is $d+1$.*

Proof. We see that $(A^2)_{u,v}$ is the number of walks of length 2 from u, v and so it is the number of common neighbours of u and v. Thus,

$$(A^2)_{u,v} = \begin{cases} b_0, & u = v; \\ 0, & d(u,v) > 2; \\ a_1, & d(u,v) = 1 \\ c_2, & d(u,v) = 2. \end{cases}$$

So we obtain that $A^2 = b_0 I + a_1 A + c_2 A_2$. We see that A_2 is a polynomial in A of degree 2. We can apply the lemma from last class, iteratively, to obtain that A_i is a polynomial in A of degree i. This shows that $\mathcal{A}(X)$ consists of matrices which are polynomials in A.

Since $A_0 + A_1 + \cdots + A_d = J$ and X is regular of degree b_0, so

$$(A - b_0 I)J = 0$$
$$(A - b_0 I)(A_0 + A_1 + \cdots + A_d) = 0$$

The left hand side is a polynomial in A of degree $d+1$. This shows that the dimension of $\mathcal{A}$ is at most $d+1$. □

Here are some more facts about distance-regular graphs (which we will state without proof, but readers are encouraged to prove these):

(a) $A = A_1$ has exactly $d+1$ distinct eigenvalues.

(b) Let π be the distance partition of X with respect to a vertex v. Then the $(d+1) \times (d+1)$ matrix

$$(L_i)_{j,k} = p_{ij}^k$$

is the quotient matrix of π with respect to A_i. Further, this partition is equitable for all A_i.

(c) The intersection array $\{b_0, \ldots, b_{d-1}; c_1, \ldots, c_d\}$ determines all of the L_is and thus all other intersection numbers, as well as the eigenvalues of A_i, for all i.

(d) If X, Y are distance-regular graphs with the same intersection array, then their adjacency matrix have the same eigenvalues.

(e) $p_{ij}^k = p_{ji}^k$. Thus $A_iA_j = A_jA_i$. The Bose-Mesner algebra is commutative.

(f) There are $d+1$ eigenspaces of A. Let E_i be the projection onto the ith eigenspace, and $E_0 = \frac{1}{n}J$. These matrices satisfy some properties:

- $E_i^2 = E_i$;
- $E_iE_j = \delta_{ij}E_i$;
- $\sum_{i=0}^d E_i = I$.

(g) $\mathcal{A} = \langle A_0, \ldots, A_d \rangle$. The Bose-Mesner algebra is also closed under Schur product (also Hadamard product, entry-wise product), denoted $\circ$. Thus

$$E_i \circ E_j = \sum_{k=0}^{d} q_{ij}^k E_k.$$

Thus q_{ij}^k are the eigenvalues of $E_i \circ E_j$. These numbers are called the *Krein parameter* of the distance-regular graph X. They are "dual", in some sense to the intersection numbers;

$$A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k.$$

Since E_i, E_j are positive semi-definite, so is $E_i \otimes E_j$, of which $E_i \circ E_j$ is a principal submatrix. Thus $q_{ij}^k \geq 0$. This is useful in determining if some given array of numbers is the intersection array of a distance-regular graph.

2.7 *Strongly regular graphs*

The empty graph is the only graph with 1 distinct eigenvalue. The only graphs with 2 distinct eigenvalues are the complete graphs. We will see that connected regular graphs with exactly 3 distinct eigenvalues are exactly the class of strongly regular graphs, which makes them an important class.

Let X be a graph that is neither complete nor empty. We say that X is *strongly regular* if every vertex of X has k neighbours, each pair of adjacent vertices has a common neighbours and each pair of non-adjacent vertices has c common neighbours. If X has n vertices, then (n, k, a, c) are said to be the *parameters* of the graph.

For example, the 5-cycle is a strongly regular graph with parameters $(5, 2, 0, 1)$. The Petersen graph is a strongly regular graph with parameters $(10, 3, 0, 1)$.

Suppose that X is a graph such that the action of $\mathrm{Aut}(X)$ on $V(X) \times V(X)$ has exactly 3 orbits. Then X is strongly regular.

Our definition allows mK_n (the disjoint union of m copies of K_n) to be a strongly regular graph with parameters $(mn, n-1, n-2, 0)$.

A distance-regular graph of diameter 2 is strongly regular with parameters (n, b_0, a_1, c_2). As an exercise, take a connected strongly regular graph with parameters (n, k, a, c) and write down its intersection array.

A strongly regular graph is *primitive* if X and its complement $\overline{X}$ are both connected.

Observe that if X is strongly regular with parameters (n, k, a, c) , then $\overline{X}$ is also strongly regular with parameters

$$(n, n-k-1, n-2-2k+c, n-2k+a).$$

2.7.1 Lemma. *Let X be a strongly regular with parameters (n, k, a, c). The following are equivalent:*

(a) X is not connected;

(b) $c = 0$;

(c) $a = k - 1$;

(d) X is isomorphic to the complement of mK_{k+1} for some $m > 1$.

Proof. It's clear that (a) = (b). Suppose X is not connected and $c = 0$. This occurs iff and only if the only non-adjacent pairs of vertices are in different components. Consider a pair of adjacent vertices u, v; every neighbour of u is either equal to v or adjacent to v (because they are in the same component). Thus $a = k - 1$. We can also deduce from this that the component containing u, v is a complete graph. (d) $\Rightarrow$ (a) is trivial. □

This implies that any strongly regular graph that is not primitive is either mK_{k+1} or the complement of mK_{k+1}. Primitive strongly regular graphs are distance-regular graph of diameter 2.

2.7.2 Example. The line graph of K_n is strongly regular with parameters

$$\left(\binom{n}{2}, 2(n-2), n-2, 4\right).$$

2.7.3 Example. The line graph of $K_{n,n}$ is strongly regular with parameters

$$(n^2, 2n-2, n-2, 2).$$

This is called the *square lattice graph*.

Suppose we are given some numbers (n, k, a, c). How do we determine if they are the parameters of some strongly regular graph?

Let X be a primitive strongly regular graph with parameters (n, k, a, c) and we consider the distance partition $\{X_0(v), X_1(v), X_2(v)\}$ of X with respect to a vertex v. This partition is equitable because X is distance-regular.

We will count the number of edges with one end in $X_1(v)$ and the other end in $X_2(v)$. We get

$$k(k-a-1) = c(n-k-1)$$

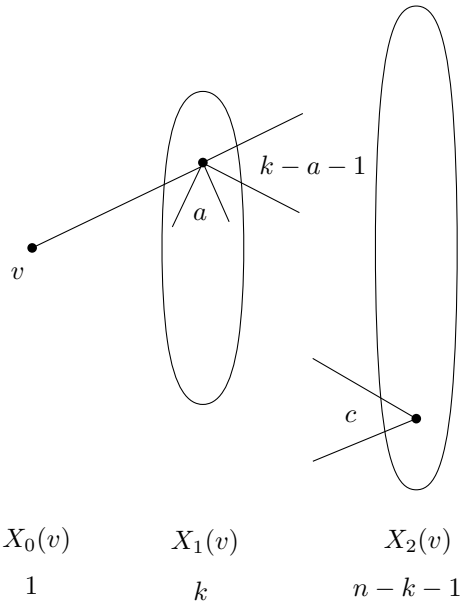


Figure 2.6: The distance partition of a strongly regular graph.

by double-counting. See figure 2.6. This is an example of a feasibility condition.

2.7.4 Example. A *Moore graph* is a graph with girth g and minimum degree r containing $n(r,g)$ vertices, where

$$n(r,g) = 1 + r + r(r-1) + \cdots + r(r-1)^{k-1}$$

where $k = \lfloor g/2 \rfloor$. If $g = 5$, then the Moore graph has to be strongly regular with parameters $(n(r,5), r, 0, 1)$. There is a theorem of Hoffman and Singleton (1960) that if X is a Moore graph of girth 5 and minimum degree $r \geq 3$, then $r \in \{3, 7, 57\}$. If $r = 3$, X is isomorphic to the Petersen graph. If $r = 7$, X is isomorphic to a graph called the Hoffman-Singleton graph. For $r = 57$, this is a long-standing open problem whether or not there exist a strongly regular graph with parameters $(3250, 57, 0, 1)$.

2.8 Eigenvalues of SRGs

Let X be a strongly regular graph and let A be its adjacency matrix. Let's look at the entries of A^2; the (u,v)th entry of A^2 is the number of walks of length 2 from u to v. This is equal to the number of (distinct) common neighbours of u and v. Thus

$$(A^2)_{u,v} = \begin{cases} k, & \text{if } u = v; \\ a, & \text{if } u \sim v; \\ c, & \text{if } u \nsim v. \end{cases}$$

We can then write A^2 as a linear combination of I, A, and $J - I - A$ as follows:

$$A^2 = kI + aA + c(J - I - A)$$

and we can rearrange to obtain

$$A^2 - (a-c)A - (k-c)I = cJ.$$

Since X is regular with valency k, we have that k is an eigenvalue of A with eigenvector $\mathbf{1}$, and every other eigenvector is orthogonal to $\mathbf{1}$. Recall that $J = \mathbf{1}\mathbf{1}^T$. Let $\mathbf{v}$ be another eigenvector of A with eigenvalue λ. We see that

$$\begin{aligned}(A^2 - (a-c)A - (k-c)I)\mathbf{v} &= cJ\mathbf{v}\\ A^2\mathbf{v} - (a-c)A\mathbf{v} - (k-c)I\mathbf{v} &= 0\\ \lambda^2\mathbf{v} - (a-c)\lambda\mathbf{v} - (k-c)\mathbf{v} &= 0\\ (\lambda^2 - (a-c)\lambda - (k-c))\mathbf{v} &= 0.\end{aligned}$$

Thus, if λ is eigenvalue of A, other than k, then λ satisfies

$$\lambda^2 - (a-c)\lambda - (k-c) = 0.$$

Thus, the (distinct) eigenvalues of A are k and the two roots of

$$t^2 - (a-c)t - (k-c) = 0.$$

Let $\Delta = (a-c)^2 + 4(k-c)$ be the discriminant of this polynomial. Then the roots are

$$\theta = \frac{(a-c) + \sqrt{\Delta}}{2}, \quad \tau = \frac{(a-c) - \sqrt{\Delta}}{2}.$$

We still need to find their multiplicities, m_θ and m_τ. First we observe that

$$\theta\tau = (c-k)$$

and, if X is primitive, this is a negative number.

At this point, we have shown a primitive strongly regular graph has three distinct eigenvalues, which are determined by the parameters.

Recalling that there are $n-1$ eigenvalues other than k and the sum of the eigenvalues is equal to $\mathrm{tr}(A)$, we have

$$m_\theta + m_\tau = n - 1$$

and

$$k + \theta m_\theta + \tau m_\tau = 0.$$

Solving this, we obtain

$$m_\theta = \frac{-(n-1)\tau - k}{\theta - \tau}, m_\tau = \frac{(n-1)\theta + k}{\theta - \tau}$$

If we use that fact that $(\theta - \tau)^2 = \Delta$, then we can write m_θ and m_τ in only terms of (n, k, a, c). (Exercise)

2.8.1 Lemma. *Let X be a connected regular graph. The adjacency matrix of X has three distinct eigenvalues if and only if X is a strongly regular graph.*

Proof. (Sketch, details left as exercise.) We have shown that if X is strongly regular, then it has 3 distinct eigenvalues. Suppose X is

a regular graph with three distinct eigenvalues; $A = A(X)$ has eigenvalues k, θ, τ. Consider the following matrix

$$M = \frac{1}{(k-\theta)(k-\tau)}(A - \theta I)(A - \tau I).$$

We see that $M\mathbf{1} = \mathbf{1}$ and if $M\mathbf{v} = 0$, then we can (eventually) conclude that $A\mathbf{v} = \lambda\mathbf{v}$ where $\lambda \in \{\theta, \tau\}$. Then $M = \frac{1}{n}J$ and A^2 is a linear combination of A, I, J. You can rearrange this to find the parameters k, a, c. □

2.8.1 *Paley Graphs*

Let q be a prime power such that $q \equiv 1 \mod 4$. The *Paley graph*, denoted $P(q)$, has vertices that are the elements of $GF(q)$ and $x \sim y$ whenever $x - y = a^2$ for some $a \neq 0 \in GF(q)$. For $q \equiv 1 \mod 4$, we have that -1 is a square in $GF(q)$, so the graph is undirected.

The Paley graph is Cayley graph where the connection set is the set of non-zero squares. The Paley graph $P(q)$ is strongly regular graph with parameters

$$\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right).$$

The eigenvalues are $\frac{q-1}{2}$ and

$$\theta, \tau = \frac{-1 \pm \sqrt{q}}{2}$$

each with multiplicity $\frac{q-1}{2}$. We will not show it in this class, but the Paley graphs are the only self-complementary, arc-transitive strongly regular graphs.

A *conference graph* is a strongly regular graph where $m_\theta = m_\tau$.

2.8.2 *Latin Square Graphs*

A *Latin square* of order n is an $n \times n$ matrix with entries in Ω with $|\Omega| = n$ such that each row and column contains each symbol exactly once. For example, a Sudoku puzzle is a Latin square of order 9.

For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

is a Latin square of order 4. If we place the 4s with 0, this is the addition table of $\mathbb{Z}_4$ (note the row corresponding to 0 is the last row).

In general, the multiplication table of any (multiplicative) group will be a Latin square.

Let $\mathcal{L}$ be a $n \times n$ Latin square. Let X be the graph whose vertices are (i, j) for $i, j \in \{1, \ldots, n\}$ and (i, j) is adjacent to (r, s) whenever

- $i = r$;
- $j = s$; or
- $\mathcal{L}(i,j) = \mathcal{L}(r,s)$.

In other words, two locations in the matrix are adjacent if they are in the same row, in the same column, or contain the same entry. We say that X is a *Latin square graph* of order n.

A Latin square graph of order n is strongly regular with parameters

$$(n^2, 3(n-1), n, 6)$$

with some details.

2.8.3 Steiner Triple Systems Graphs

Let Ω be a set of order v. We consider the 3-subsets of Ω. Let S be a subset of 3-subsets such that each pair of elements of Ω lies in exactly one element of S.

For example, take $\Omega = \{1, \ldots, 7\}$ and take S to be the following:

$$\{124, 235, 346, 457, 561, 672, 713\}.$$

Such a set S is a *Steiner triple system*. We define a graph on a Steiner triple system S as follows: the vertices are the elements of S and $T_1 \sim T_2$ whenever $T_1 \cap T_2 \neq \varnothing$. This graph will be strongly regular with parameters

$$\left(\frac{v(v-1)}{6}, \frac{3(v-3)}{2}, \frac{v+3}{2}, 9\right).$$

There is a classical result of Kirkman that a STS exists if and only if $v \equiv 1, 3 \mod 6$.

2.8.2 Theorem (Neumaier, 1980)**.** *All but finitely many strongly regular graphs with least eigenvalues $-m$ are conference graphs, Latin square graphs or Steiner triple system graphs.*

3
Combinatorial Designs

3.1 Incidence structure

An *incidence structure* $(\mathcal{P}, \mathcal{B})$ consists of a set of *points* $\mathcal{P}$ and a set of *blocks* $\mathcal{B}$ and an incidence relation on $\mathcal{P} \times \mathcal{B}$. A point and a block are either incident or not; if so, we say "the point lies in the block" or "the block lies on the point." In geometry, block are also called lines.

A Steiner triple system is an incidence structure; $\mathcal{P} = \Omega$ and $\mathcal{B} = S$, the 3-subsets we chose, and incidence is containment. In Figure 3.1, the points are $\{a, b, c, d, e, f, g\}$ and the blocks are the colours red, blue, green, yellow, orange, purple, and, black; in the figure, the points are represented by nodes and the blocks are represented by line segments and each block goes through the points with which it is incident.

A *graph* is a triple (V, E, I) where V is a set of vertices, E is a set of edges and $I : V \times E \to \{0, 1\}$ is an incidence related between the vertices and edges, such that each edge is incident with at most two vertices.

In this way, a graph is also an incidence structure.

Let's recall that an incidence structure consists of $(\mathcal{P}, \mathcal{B}, I)$ where $\mathcal{P}$ is a set of points, $\mathcal{B}$ is a set of blocks and I is an incidence relation. In geometry, blocks are called *lines*. We may view $\mathcal{B}$ as the point set and $\mathcal{P}$ as the block set of another incidence structure, with the same incidence relation; this is called the *dual* incidence structure. Note that the dual of the dual is the original incidence structure.

We get three graphs from an incidence structure $(\mathcal{P}, \mathcal{B}, I)$:

(i) *incidence graph*: vertices are $\mathcal{P} \cup \mathcal{B}$ and the adjacency relation is given by incidence;

(ii) *point graph*: vertices are the point $\mathcal{P}$ and two point are adjacent if there exists $\beta \in \mathcal{B}$ incidence to both points (in this case, we say the points are *collinear*; and

(iii) *block graph*: point graph of the dual.

Figure 3.1 show the Fano plane and its incidence graph. The point graph and the block of the Fano plane are isomorphic to K_7. The

incidence graph of the Fano plane known as the *Heawood graph*; it is the dual of K_7 embedded on the torus.

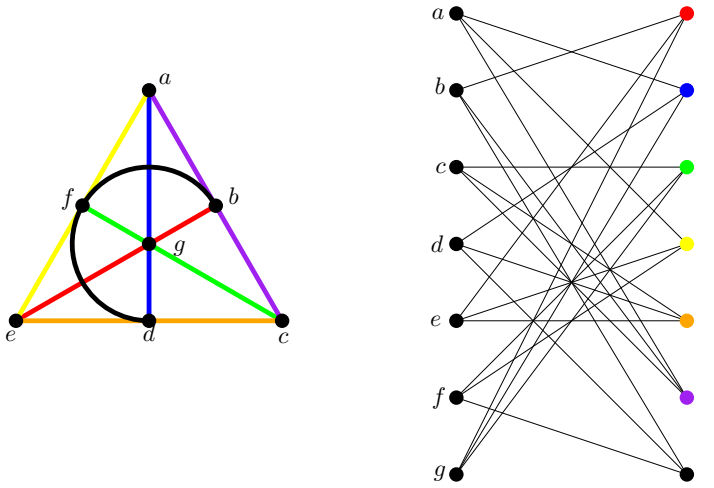


Figure 3.1: An incidence structure and its incidence graph.

An incidence structure $(\mathcal{P}, \mathcal{B})$ is *point-regular* if each point is incident with the same number of blocks. It is *block-regular* if each block is incident with the same number of points. An incidence structure is *uniform* if it is both block- and point-regular. An incidence structure is *thick* if the minimum valency of its incidence graph is at least 3.

An incidence structure is *connected* if the incidence graph is connected. A connected bipartite graph has a unique 2-colouring, so the incidence structure is determined up to duality.

An incidence structure is a *partial linear space* if each pair of points lies in at most one block. It is a *linear space* if each pair of points lies on each one block. In this setting, we will call blocks "lines". A *dual linear space* is an incidence structure whose dual is a linear space.

3.1.1 Lemma. *An incidence structure is a partial linear space if and only if incidence graph has girth* ≥ 6.

Proof. Suppose $a, b \in \mathcal{P}$ and $C, D \in \mathcal{B}$. In the incidence graph, $\{a, C, b, D\}$ forms a 4-cycle if and only if a, b are both incident to $\{C, D\}$. □

3.1.2 Corollary. *The dual of a partial linear space is also a partial linear space.*

Proof. The incidence graph has no 4-cycle. □

Since the incidence graph of partial linear space does not contain a copy of $K_{2,2}$ (also known as a 4-cycle), it also cannot contain $K_{2,m}$ for larger m. Thus, there are no two blocks incidence with exactly the same set of points. We sometimes write a block as the set of points incidence to it.

For example, the Fano plane has points $\{0, 1, 2, \ldots, 6\}$ and blocks 013, 124, 235, 346, 450, 561, 602.

Suppose $(\mathcal{P}, \mathcal{B})$ is an incidence structure. If $a, b \in \mathcal{P}$, we may define the *line through a and b* to be the intersection of all blocks (considered as sets of points that they are incident with) which are incidence with both a and b. The incidence structure formed by the point and the lines (as defined defined just now) is a partial linear space; it is usually interesting if it is thick.

The incidence matrix N of a finite incidence structure $(\mathcal{P}, \mathcal{B})$ is the 01-matrix with rows indexed by $\mathcal{P}$ and columns indexed by $\mathcal{B}$ such that $N_{p,\beta} = 1$ whenever the point p is incident with the block β. Then N^T is the incidence matrix of the dual and the adjacency matrix of the incidence graph is

$$\begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}.$$

A *parallel class* in an incidence structure is a set of blocks that partitions the point set. For example, if X is a graph, then a parallel class is a perfect matching. The Fano plane doesn't have one because 7 is prime. An incidence structure is *resolvable* if we can partition the block set into parallel classes. So, in the case, the graph is resolvable whenever it has a 1-factorization.

3.2 *Designs*

We say that an incidence structure $(\mathcal{P}, \mathcal{B})$ has *strength* at least t if for $s = 1, \ldots, t$ there are constants $\lambda_1, \ldots, \lambda_t$ such that each s-subset of $\mathcal{P}$ is incidence with exactly λ_s elements of $\mathcal{B}$. For example, a point-regular incidence structure has strength 1. A *t-design* is a uniform incidence structure of strength at least t. By convention, "design" and "block design" denotes 2-design.

A design is *simple* if no two blocks are incidence with the same set of points. Generally, our designs will be simple, unless stated otherwise.

A 2-design with $\lambda = \lambda_2 = 1$ is a partial linear space. A *Steiner system* is a t-design with $\lambda_t = 1$.

A *block design* with *parameters* (v, b, r, k, λ) is a 2-design with v points, b blocks, where every point is on $r = \lambda_1$ blocks, every block lies on k points and every pair of points lies on exactly $\lambda = \lambda_2$ blocks. We sometimes call r the *replication number*.

For example, the Fano plane is a block design with parameters

$$(v, b, r, k, \lambda) = (7, 7, 3, 3, 1).$$

What if we the complements of all the blocks? We get a design on 7 points with 7 blocks of size 4. What are its parameters? (Exercise)

In a general block design, b is very large and it may be inconvenient or impossible to write down all of the blocks.

The Fano is an example of a *difference set* construction. A *difference set* S in an abelian group G is a subset of G with the property that each non-zero element of G appears the same number of times

as a difference of two elements of S. In the Fano plane, we take $S = \{0, 1, 3\}$ in $\mathbb{Z}_7$.

If G is an abelian group and $S \subseteq G$, then the set

$$S + g = \{x + g \mid x \in S\}$$

is called a *translate* of S. We obtain a design by taking all translates of a difference set.

Let $V = \mathbb{Z}_{11}$ and let $\alpha = \{0, 2, 3, 4, 8\}$ is a difference set. The set of all translates of α is a 2-design with parameters

$$(11, 11, 5, 5, 2).$$

Example: Let V be a vector space over a field. We construct an incidence structure by taking the point set to the be the 1-dimensional subspaces of V and the block to be the cosets of the 1-dimensional subspaces, where incidence is containment. This is a 2-design with $\lambda = 1$ called an *affine plane*. If $V = \mathbb{Z}_3^2$, we get a 2-design with parameters $(9, 12, r, 3, 1)$.

Finally, here's a non-interesting example. A design is *trivial* whenever $k \in \{0, 1, v-1, v\}$. The *complete design* has point set V and blocks are all k-subsets of V.

Now we will find relations between the parameters by counting some stuff.

Let $(V, \mathcal{B})$ be a block design with parameters (v, b, r, k, λ). First we will count the number of ordered pairs (u, α), where $u \in V$, $\alpha \in \mathcal{B}$ and u is incident with α. This number is

$$vr = bk.$$

Note that this is also the number of edges in the incidence graph.

Now we count triples (u, w, α) where $u \neq w$ and u, w are both incident with α. Each pair of distinct points lies on λ blocks, so this number is:

$$v(v-1)\lambda.$$

On the other hand, each block has k points so this number is also

$$bk(k-1).$$

Thus the number of triple gives us

$$v(v-1)\lambda = bk(k-1)$$

which we can rewrite as

$$\frac{v(v-1)}{k(k-1)} = \frac{b}{\lambda}.$$

Since $vr = bk$, we have

$$\frac{(v-1)}{(k-1)} = \frac{r}{\lambda}.$$

Now we know that b/λ and r/λ are determined by v and k.

For example, suppose $\lambda = 1$ and $k = 3$, then

$$b = \frac{v(v-1)}{6}, r = \frac{v-1}{2}.$$

Thus $v \equiv 1, 3 \mod 6$. These are again the Steiner triple systems. Let's consider a block design with parameters (v, b, r, k, λ); here v is the number of points, b is the number of blocks, r is the replication number, k is the size of the blocks, and λ is the numbers that each pair of points lie on.

3.3 *Incidence matrices*

Let N be the incidence matrix (of an incidence structure); the rows of N are indexed by the points and the columns are indexed by the blocks, and $N_{p,B} = 1$ whenever p and B are incident.

How to multiply matrices:

$$(NN^T)_{u,v} = \sum_{b \in \mathcal{B}} N_{u,B} N_{v,B} = |\{B : u \in B, v \in B\}|.$$

Then, if we have a block design with parameters (v, b, r, k, λ) then

(a) $N\mathbf{1} = r\mathbf{1}$;

(b) $\mathbf{1}^T N = k\mathbf{1}^T$; and

(c) $NN^T = rI + \lambda(J - I) = (r - \lambda)I + \lambda J$, where I is the $v \times v$ identity and J is the $v \times v$ all ones matrix.

3.3.1 Theorem. *If $\mathcal{D}$ is a 2-design with parameters (v, b, r, k, λ) and $\mathcal{D}$ has at least two points and at least two blocks, then $b \geq v$.*

Proof. Observe N is $v \times b$. We will show that the rows of N are linear independent over $\mathbb{R}$ and we can do this by prove that NN^T is invertible.

We already have that $NN^T = (r - \lambda)I + \lambda J$. Note that

$$(xI + J)(yI + J) = xyI + (x + y + v)J.$$

We can see from this that $xI + J$ is invertible when $x \neq 0$. Since our assumptions imply that $r > \lambda$, the result follows. □

Thus $b \geq v$. This called Fisher's inequality. Can we have $b = v$? We've already seen some examples; the Fano plane. A design with $b = v$ is called a *symmetric design*. Note that if $b = v$ then $r = k$. In this case, instead of writing all the parameters, we write only (v, k, λ) and we say that the design is a 2-(v, k, λ) symmetric design. [1]

[1] From the previous lecture, we know that b, r are always determined by v, k, λ, so we often write only 2-(v, k, λ) for any design, not necessarily symmetric.

3.3.2 Theorem. *If $\mathcal{D}$ is a symmetric design with paramters (v, k, λ) , then any two distinct blocks have exactly λ points in common.*

Proof. Since $b = v$, the incidence matrix N is invertible. Then we have

$$(N^T N)_{B_1, B_2} = |\{p : p \in B_1, p \in B_2\}|.$$

Also

$$N^T N = (r - \lambda)I + \lambda J$$

since $NJ = rJ$ and $N^{-1}J = r^{-1}J$. □

We've shown that dual of a symmetric design is a symmetric design. We've actually shown:

$$(r-\lambda)I + \lambda J = NN^T = N^TN$$

and the incidence matrix N is a normal matrix.

3.4 *Constructing symmetric designs*

We know that $\frac{v(v-1)}{k(k-1)} = \frac{v}{\lambda}$ and so

$$v = 1 + \frac{k^2-k}{\lambda}.$$

For $\lambda = 1$, the only possibilities are in Table 3.1. These, in fact, all exists except for $k = 6$ and $v = 31$.

k	v
2	3
3	7
4	13
5	21
6	31
7	43
8	57

Table 3.1: Parameters for possible designs for small k and $\lambda = 1$.

Let q be a prime power and let V be a vector space of dimension d over $GF(q) = \mathbb{F}_q$. We will construct an incidence structure as follows. The points are the 1-dimensional subspace of V. The blocks are the $(d-1)$-dimensional subspaces of V. The incidence relation here is inclusion; p, B are incident whenever p is a subspace of B.

The number of elements of $V = \mathbb{F}_q^d$ is q^d. The number of elements in a 1-dimensional subspace is q. The 1-dimensional subspaces of V partition the non-zero elements of V into sets of size $q-1$. Thus the number of points in our incidence structure is

$$\frac{q^d-1}{q-1}.$$

Each hyperplane, or $(d-1)$-dimensional subspace, is the kernel of a $1 \times d$ matrix $a = [a_1, \ldots, a_d]$; if we take all elements $v \in V$ such that $av = 0$, we obtain a hyperplane, and, conversely, every hyperplane arises in this way (we can always pick a basis of V such that this is true). If a, b are two non-zero $1 \times d$ matrices, then $\ker(a) = \ker(b)$ if and only if b is a non-zero scalar multiple of a. This gives us a bijection between the 1-dimensional subspaces and the hyperplanes and so the number of blocks is also

$$\frac{q^d-1}{q-1}.$$

Suppose $a = [a_1, \ldots, a_d]$, $b = [b_1, \ldots, b_d]$ are non-zero $1 \times d$ matrices. Then a, b denote different hyperplanes if and only if

$$\operatorname{rk} \begin{pmatrix} a_1 & \cdots & a_d \\ b_1 & \cdots & b_d \end{pmatrix} = 2.$$

The kernel of this matrix is the subspace of dimension $d-2$ which lies on both hyperplanes. Thus every pair of distinct blocks are incident with

$$\frac{q^{d-2}-1}{q-1}$$

points. Thus we have a symmetric design with parameters

$$\left(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1} \right).$$

For $d = 3$, we get the parameters in Table 3.2. The only parameters missing from the previous table is because there is no finite field of order 6, so we cannot construct the design in this way; we will see later that is in fact impossible.

q	v	k	λ
2	7	3	1
3	13	4	1
4	21	5	1
5	31	6	1
7	57	8	1

Table 3.2: Parameters for projective designs for small q.

For $d = 3$, this construction of a *projective design* gives us infinitely many designs with $\lambda = 1$ and block size is $q+1$ where q is a prime power.

Now we have reached a main problem in this area: Is there a symmetric design with $\lambda = 1$ where $k-1$ is not a prime power?

A *projective plane* is a thick incidence structure such that

(a) each pair of distinct points lies on exactly one block; and

(b) each pair of distinct blocks have exactly one point in common.

A finite incidence structure is projective plane if and only if it is a symmetric design with $\lambda = 1$. The theory of projective planes is rich and complex. We know comparatively little about symmetric designs with $\lambda \geq 2$.

In particular, we do not (yet) know if there exists infinitely many symmetric designs for fixed $\lambda \geq 2$.

3.5 *An important example*

Let q be a prime power and V be a vector space of dimension 3 over $\mathbb{F}_q$. We will consider the incidence structure as follows: the points are the 1-dimensional subspace of V, the lines are the 2-dimensional subspaces of V, and incidence is given by subspace containment (a 1-dimensional subspace is incident to a 2-dimensional subspace, if it

is a subspace of the bigger space). This incidence structure is called $PG(2,q)$, the projective geometry over $\mathbb{F}_q$ of dimension 2. One can verify that this construction will give a projective plane, as defined in the previous class.

3.6 Bilinear forms

When do designs exist? We want to some more powerful tools to give conditions for the exists of symmetric designs. To do this we need some more maths: we need the theory of bilinear and quadratic forms.

Let V be a vector space over a field $\mathbb{F}$. A *bilinear form* β on V is a function from $V \times V$ to $\mathbb{F}$ which is linear in both variables. If

$$\beta(u,v) = \beta(v,u)$$

for all $u, v \in V$, then we say that β is *symmetric*. The canonical example is to take a symmetric matrix B and define

$$\beta(u,v) = u^T B v.$$

For example, the dot product is what you get when you take B to be the identity matrix.

If β is a bilinear form on V and $v \in V$, then we define

$$v^\perp := \{x : \beta(v,x) = 0\}.$$

If $U \leq V$ (is a subspace), then

$$U^\perp = \bigcap_{u \in U} u^\perp.$$

It is possible that $v \in v^\perp$ and $v \neq 0$.

We see that if $v \neq 0$ then $v^\perp$ is a subspace of V with co-dimension at most 1. We say that β is *non-degenerate* if $v^\perp = V$ implies that $v = 0$.

In general, if we have some bilinear form β, it's not true that $V = U \oplus U^\perp$, but it is true that for a non-degenerate bilinear form β that

$$\dim(U^\perp) = \dim(V) - \dim(U)$$

and $(U^\perp)^\perp = U$.

A *quadratic form* $Q(v)$ over V is a function from V to $\mathbb{F}$ such that

(i) $Q(\alpha u) = \alpha^2 Q(u)$ for all $\alpha \in \mathbb{F}$ and $u \in V$;

(ii) $\beta(u,v) = Q(u+v) - Q(u) - Q(v)$ gives a symmetric bilinear form on V.

For example, if β is a symmetric bilinear form then

$$\beta(x+y, x+y) = \beta(x,x) + \beta(y,y) + 2\beta(x,y)$$

and so $Q_\beta = \beta(x,x)$ is a quadratic form. If 2 is invertible in $\mathbb{F}$, then the quadratic form determines the bilinear form.

For our purposes, we will assume that 2 is an invertible element of $\mathbb{F}$. In fact, we will assume

$$Q(x) = x^T A x$$

for some symmetric matrix A.

Two quadratic forms Q_1 and Q_2 over $\mathbb{F}$ are *equivalent* if there exists and invertible matrix G such that for all $x \in V$,

$$Q_2(x) = Q_1(Gx).$$

It's easy to check that this is an equivalence relation. Two symmetric matrices A, B are *congruent* if there exists and invertible matrix G over $\mathbb{F}$ such that

$$B = G^T A G.$$

We write $A \approx B$ to denote that A, B are congruent. We will also say the bilinear associated with A and B are congruent. If two quadratic forms are equivalent, then associated bilinear forms are congruent.

A good candidate for G is a permutation matrix P. For example

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \approx \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix}$$

via $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. If $c \neq 0$, then

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \approx \begin{pmatrix} c^2 a & 0 \\ 0 & b \end{pmatrix}$$

via $P = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$.

Now we want to relate what we've learned here to a design theory. The existence of a symmetric design implies the congruence of two diagonal matrices.

3.6.1 Theorem. *If there is a symmetric (v, k, λ)-design then*

$$\begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix} \approx (k - \lambda) \begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix}.$$

Proof. Let N be the incidence matrix of a symmetric (v, k, λ)-design. If

$$\widehat{N} = \begin{pmatrix} N & \mathbf{1} \\ \lambda \mathbf{1}^T & k \end{pmatrix}$$

then we see that

$$\widehat{N} \begin{pmatrix} I & 0 \\ 0 & -\lambda \end{pmatrix} \widehat{N}^T = \begin{pmatrix} (k-\lambda) I & 0 \\ 0 & -\lambda(k-\lambda) \end{pmatrix}.$$

That $\widehat{N}$ is invertible is left as an exercise. □

3.7 Cancellation

A *quadratic space* is a pair (V, q), where V is a vector space and q is a quadratic form. Two quadratic space (V_1, q_1) and (V_2, q_2) are *isometric* if there exists an invertible linear map $L : V_1 \to V_2$ such that

$$q_2(Lv) = q_1(v)$$

for all $v \in V_1$. If U is a subspace of V, then U and the restriction of q onto U is a quadratic space.

If $V = U_1 \oplus U_2$ and q_1 and q_2 are quadratic forms for U_1 and U_2 respectively, then if we define

$$q(u_1, u_2) = q_1(u_1) + q_2(u_2)$$

for $u_i \in U_i$, then q is a quadratic form on V. We say that the quadratic space (V, q) is the *sum* of the quadratic space (U_1, q_1) and (U_2, q_2).

If U is a subspace of a quadratic space V, then the *radical* of U is the subspace $U \cap U^\perp$. If the radical of U is 0 then

$$U \oplus U^\perp = V.$$

An *isometry* of V is a map from V to U, which satisfies the conditions for L in the definition of isometric.

3.7.1 Lemma. *Let (V, q) be a quadratic space and suppose u, v are elements of V such that $q(u) = q(v) \neq 0$. Then there is an isometry from V to V that maps u to v.*

Proof. Let's construct some isometries. Let β be the symmetric bilinear form associated with q. If $a \in V$ and $q(a) \neq 0$, then we define the map τ_a on V as follows:

$$\tau_a(v) = v - 2\frac{\beta(a, v)}{q(a)}a.$$

Then τ_a is linear and τ_a^2 is identity. Also $q(\tau_a(v)) = q(v)$ for all v, and thus is an isometry.

As exercise, one can prove that $q(u - v) \neq 0$, then $\tau_{u,v}$ swaps u and v.

Suppose u, v are such that $q(u) = q(v) \neq 0$ and let $a = u - v$. If $q(a) \neq 0$, then τ_a maps u to v. If $q(u + v) \neq 0$, then τ_{u+v} swaps u with $-v$ and so $-\tau_{u+v}$ takes u to v.

If neither of the isometries work, then

$$q(u - v) = q(u + v) = 0$$

then $q(u) = -q(v)$ and

$$0 = q(u - v) + q(u + v) = 2q(u) + 2q(v) = 4q(u) \neq 0$$

cannot happen. □

3.7.2 Theorem. *Suppose U_1, U_2 are non-zero subspace of a quadratic space (V, q) and the radical of U_1 is zero. Then if there is an isometry $\rho : U_1 \to U_2$, there is an isometry of V to itself whose restriction to U_1 is equal to ρ.*

Proof. If q vanishes on V, then the radical of U is U. Since the radical of U is not U, there exists $u \in U_1$ such that $q(u_1) \neq 0$. By the previous lemma, there exists an isometry σ on V such that $\sigma(\rho(u)) = u$. If the dimension of U_1 is 1, we would be done.

Suppose $\sigma\rho$ is an isometry from U_1 to U_2 that fixes u. If $\sigma\rho$ extends to an isometry, say τ of V, then applying τ and then σ^{-1} is an isometry of V that extends ρ.

Now we proceed by induction on $\dim(U_1)$. Now U_1 is the sum of the span of v and the space $v^\perp \cap U_1$, which is a complement to v in U_1. Since $\sigma\rho$ is an isometry, $\sigma\rho(v^\perp \cap U_1)$ is a complement to v in $\sigma(U_2)$. By induction, there exists an isometry ϕ on $v^\perp$ that coincides with $\sigma\rho$ on $v^\perp \cap U_1$. The linear map that fixes v and agrees with ϕ on $v^\perp$ is an isometry of V that agrees with ρ on U_1. □

3.7.3 Corollary. *Let (V_1, q_1) and (V_2, q_2) be isometric quadratic space. Let U_1, U_2 be subspaces of V_1, V_2, respectively. If the radical of U_1 is zero and U_1 is isometric to U_2, then $U_1^\perp$ and $U_2^\perp$ are isometric.*

Proof. Apply the theorem. Exercise. □

If the radical of (V, q) is zero then q non-singular. if 2 is invertible and $q(x) = x^T Ax$ for a symmetric matrix A, then q is non-singular if A is. We will shortly be able to prove statements like the following.

3.7.4 Theorem. *If n is positive integer, then $I_4 \approx nI_4$.*

3.8 Bruck-Ryser-Chowla

Recall the definition of a quadratic form; intuitively, you can think of it is a map taking a vector x to $x^T Ax$ for some symmetric matrix A. If you have two quadratic forms given by matrices A, B then they are equivalent if there exists an invertible matrix G such that $A = G^T BG$.

Suppose f_1, f_2 are two equivalent non-singular quadratic forms on variables $x_1, \ldots, x_m$ and g_1, g_2 are quadratic forms on distinct variables $y_1, \ldots, y_n$. Then if $f_1 + g_1$ and $f_2 + g_2$ are equivalent, the work we did in the previous class implies that g_1 and g_2 are equivalent. This is the form of Witt cancellation that we will use.

3.8.1 Theorem. *If n is a positive integer, then $I_4 \approx nI_4$.*

Proof. Define

$$G = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

and verify that

$$G^T G = (a^2 + b^2 + c^2 + d^2) I_4.$$

By a famous theorem of Lagrange, every positive integer is equal to the sum of four squares and the theorem follows. □

For context, I_2 and $3I_2$ are not equivalent. In fact, I_2 and nI_2 are equivalent if and only n is the sum of two squares.

Recall that we speak of (v, k, λ) designs; we chose to write only these parameters because they are only ones we need for a symmetric design, but we also write this for any design because we can still determine b, r from these. We call $k - \lambda$ the *order* of the design and we denote it by n.

3.8.2 Theorem (Bruck-Ryser-Chowla)**.** *If there is a non-trivial symmetric (v, k, λ)-design, one of the following holds:*

(a) if v is even, then $k - \lambda$ is a square;

(b) if v is odd, then the equation

$$x^2 - ny^2 - (-1)^{\frac{v-1}{2}} \lambda z^2 = 0$$

has a non-zero integer solution (for x, y, z).

Proof. Suppose v is even. Recall

$$\widehat{N} \begin{pmatrix} I & 0 \\ 0 & -\lambda \end{pmatrix} \widehat{N}^T = (k - \lambda) \begin{pmatrix} I & 0 \\ 0 & -\lambda \end{pmatrix}$$

where $\widehat{N}$ is an invertible matrix that we obtain from the design. Taking the determinant on both sides, we obtain

$$\det(\widehat{N})^2 (-\lambda) = (k - \lambda)^{v+1} (-\lambda).$$

Thus, $(k - \lambda)^{v+1}$ is a square. Since v is even, we have that $(k - \lambda)$ is a square.

Suppose v is odd. If $v \equiv 1 \mod 4$, we use Witt cancellation to cancel as many 4×4 blocks as possible and we obtain

$$\begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix} \approx \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix},$$

where $n = k - \lambda$. Thus

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = n.$$

There exists u, v such that

$$n = \begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & -n\lambda \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = n(u^2 - \lambda v^2).$$

After some details, we obtain that there exists $x, y, z \in \mathbb{Q}$ such that

$$nx^2 = y^2 - \lambda z^2.$$

(As an exercise, how do we get x, y, z here from u, v?)

If $v \equiv 3 \mod 4$, we get

$$\begin{pmatrix} -\lambda & 0 \\ 0 & n \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ 0 & -\lambda n \end{pmatrix}.$$

Again we get that that $n = u^2 - \lambda n v^2$ by the same trick as before. The result follows after some algebraic manipulations left to the reader. □

3.9 *Applications*

We can now eliminate some parameters for symmetric designs. In particular, there is no projective plane of order 6.

A projective plane is a 2-design with $\lambda = 1$ and $v = n^2 + n + 1$. If $n \equiv 0, 3 \mod 4$, then $v \equiv 1 \mod 4$ and $nx^2 + y^2 = z^2$ is the equation that we get from the theorem. Here $(x, y, z) = (0, 1, 1)$ is always a non-zero integer solution. If $n \equiv 1, 2 \mod 4$, then $v \equiv 3 \mod 4$ and $nx^2 = y^2 + z^2$ is the equation that we get from the theorem. Thus we have

$$n = \frac{y^2}{x^2} + \frac{z^2}{x^2}$$

which implies that $n = a^2 + b^2$ for some integers a, b. Thus if $n \equiv 1, 2 \mod 4$ and a projective plane of order n exists, then n is the sum of two squares.

3.9.1 Corollary. *There is no projective plane of order 6.*

Due to a difficult computation by Clement Lau, there is also no projective plane of order 10, even though the conditions of the BRC theorem are satisfied. However, this is the only case that we know of where the BRC conditions hold but the design does not exist.

As another example, consider a $(29, 8, 2)$-design. The BRC equation is

$$6x^2 + 2y^2 = z^2.$$

If there exists a non-zero equation then, $2|z$. If $z = 2z_1$, then

$$6x^2 + 2y^2 - 4z_1^2 = 0$$

and so

$$3x^2 + y^2 - 2z_1^2 = 0$$

Here you can use some elementary number theory; if A, B, C satisfy

$$Ax^2 + By^2 + Cz^2 = 0$$

and A is prime, then $-BC$ is square mod A. This implies that this design does not exist.

3.10 Hadamard matrices

A Hadamard matrix is a $n \times n$ matrix H with entries ± 1 such that

$$HH^T = nI.$$

(Note that, if this happens $H^T H = nI$.) Here are some examples,

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, J_4 - 2I_4.$$

There are two families of operations that we can apply to a Hadamard matrix to get another Hadamard matrix;

(a) permute rows and/or columns;

(b) multiply all entries in a row (or a column) by -1.

An arbitrary combination of these operation is a *monomial operation*. A *monomial matrix* is the product of a permutation matrix and a diagonal matrix whose diagonal entries are equal to ± 1; that is $M = PD$. Two Hadamard matrices are *monomially equivalent* if we can get one from the other by monomial operations. That is, if M_1, M_2 are monomial matrices and H is a Hadamard matrix, then $M_1 H M_2$ is also a Hadamard matrix and is monomially equivalent to H.

A Hadamard matrix is *normalized* if all entries in its first row and first column are equal to 1. Note that the equivalence class of H will contain multiple normalized matrices.

3.11 A lower bound

If $\mathcal{D}$ is a symmetric (v, k, λ) design, recall that the order is $n = k - \lambda$.

3.11.1 Theorem. *If $\mathcal{D}$ is a symmetric (v, k, λ) design, then*

$$4n - 1 \leq v (\leq n^2 + n + 1).$$

Proof. We will prove just the lower bound. Let N be the incidence matrix of $\mathcal{D}$. Then each entry of $2N - J$ is ± 1 and

$$(2N - J)\mathbf{1} = (2k - v)\mathbf{1}.$$

Thus

$$\mathbf{1}^T (2N - J)^T (2N - J)\mathbf{1} = v(v - 2k)^2.$$

On the other hand,

$$\begin{aligned} \mathbf{1}^T (2N - J)^T (2N - J)\mathbf{1} &= \mathbf{1}^T (4N^T N - 2N^T J - 2JN + J^2)\mathbf{1} \\ &= \mathbf{1}^T (4nI + 4\lambda J - 4kJ + vJ)\mathbf{1} \\ &= \mathbf{1}^T (4nI - 4nJ + vJ)\mathbf{1} \\ &= 4nv + v^2(v - 4n). \end{aligned}$$

Thus

$$v(v - 4n) + 4n = (v - 2k)^2 \geq 0$$

and thus

$$(v-2n)^2 \geq 4n^2 - 4n.$$

We can do slightly better; if $n > 0$, then $n^2 - n$ is not a square, thus we have

$$(v-2n)^2 \geq (2n-1)^2$$

now we can take the (positive) square roots and obtain the result. □

We showed that if $\mathcal{D}$ is a symmetric (v,k,λ) design, then

$$4n - 1 \leq v$$

where $n = k - \lambda$. What happens when the equality holds?

Let $\mathcal{D}$ be a symmetric (v,k,λ) such that $v = 4n-1$. Let $\overline{N} = 2N - J$, which is a square matrix with entries in ± 1. Then since

$$NN^T = (k-\lambda)I + \lambda J$$

and so

$$\begin{aligned}\overline{N}\overline{N}^T &= (2N-J)(2N^T - J)\\ &= 4NN^T - 4kJ + vJ\\ &= 4nI + 4\lambda J - 4kJ + vJ\\ &= 4nI - J.\end{aligned}$$

Now consider

$$H = \begin{pmatrix} 1 & \mathbf{1}^T \\ \mathbf{1} & -\overline{N} \end{pmatrix}$$

and now you can verify that $HH^T = (4n)I$ and thus is a normalized Hadamard matrix.

Conversely, a normalized $4n \times 4n$ Hadamard matrix gives rise to a symmetric design with $v = 4n-1$. We will leave the details as an exercise, but we will determine the parameters of this design. We have that

$$\lambda \frac{v(v-1)}{2} = v\frac{k(k-1)}{2}$$

and so

$$(v-1) = \frac{k(k-1)}{\lambda}.$$

Here $v - 1 = 4n - 2$ and so

$$(4n-2)\lambda = (n+\lambda)(n+\lambda-1)$$

and after some steps

$$0 = (n-\lambda)(n-\lambda-1)$$

and so either $n = \lambda$ or $n = \lambda + 1$. If $\lambda = n$, then $k = 2n$. If $\lambda = n-1$, then $k = 2n-1$. Thus (v,k,λ) must be one of

$$(4n-1, 2n-1, n-1), \quad (4n-1, 2n, n).$$

Observe that the second parameters is complementary to the first. A design with these parameters is called a *Hadamard design*. Given a Hadamard matrix, we get one Hadamard design for each possible way of normalizing H. In general, they are not isomorphic.

3.12 Graphs from Hadamard matrices

From every Hadamard design, we obtain a distance-regular graph by taking the bipartite incidence graph of the design. This will give a bipartite graph of diameter 3, which are called *Hadamard design graphs* in the literature. But given any Hadamard matrix, we can always construct another distance regular graph, of diameter 4.

For a $n \times n$ Hadamard matrix H, the *Hadamard graph* X is defined as follows. There are two vertices c^+ and c^- for each column of H and two vertices r^+ and r^- for each row of H. If r is a row and c is a column such that the entry of H is $+1$, then we have edges $\{c^+, r^+\}$ and $\{c^-, r^-\}$. If r is a row and c is a column such that the entry of H is -1, then we have edges $\{c^+, r^-\}$ and $\{c^-, r^+\}$. This will give a bipartite on $4n$ vertices of degree n. In fact, we will have a distance-regular graph with parameters

$$\{n, n-1, \frac{n}{2}, 1; 1, \frac{n}{2}, n-1, n\}.$$

If H_1, H_2 are inequivalent Hadamard matrices such that $H_1^T \neq H_2$, then the Hadamard graphs are non-isomorphic. Converse is also true.

3.13 Existence

There is a well-known conjecture that if $4|n$ then there exists some Hadamard matrix of order n.

The *Kronecker product* (or tensor product) of matrices A, B is the block matrix where the (i, j) block is $A_{i,j}B$, and is denoted $A \otimes B$. An important property of Kronkecker product is that if AC, BD are defined, then

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

One can show that if H_1, H_2 are Hadamard matrices, then $H_1 \otimes H_2$ is also a Hadamard matrix. Since there is a 2×2 Hadamard matrix, there exists a $n \times n$ Hadamard matrix whenever n is a power of 2.

3.14 Symmetric and regular Hadamard matrices

Let H be Hadamard matrix of order n. Then H is normal matrix and is thus diagonalizable. Let $\mathbf{z}$ be an eigenvector of H with eigenvalue θ; ie $H\mathbf{z} = \theta\mathbf{z}$. Then

$$n\mathbf{z} = H^T H\mathbf{z} = \theta H^T\mathbf{z}$$

and thus

$$\mathbf{z}^*(n\mathbf{z}) = \theta\mathbf{z}^* H^T\mathbf{z} = \theta\mathbf{z}^* H^*\mathbf{z} = \theta(H\mathbf{z})^*\mathbf{z} = \theta\bar{\theta}\mathbf{z}^*\mathbf{z}.$$

We have obtained that $n = \theta\bar{\theta}$ and thus all eigenvalues of H have absolute values $\sqrt{n}$.

3.14.1 Lemma. *If H is a symmetric Hadamard matrix with constant diagonal of order n, then n is a square.*

Proof. Since real symmetric matrices have only real eigenvalues, the all eigenvalues of H are $\pm\sqrt{n}$. Without loss of generality, we may assume the diagonal consists of all 1s (multiplying by -1 does not change the order of the matrix). Let a be the multiplicity of $\sqrt{n}$ as an eigenvalue of H.

Since $\mathrm{tr}(H)$ is equal to the sum of eigenvalues of H, we have that

$$n = \mathrm{tr}(H) = a\sqrt{n} - (n-a)(\sqrt{n}) = (2a-n)\sqrt{n}$$

and dividing by $\sqrt{n}$ yields that $\sqrt{n} = 2a - n$, which is an integer. □

For example,

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

is a symmetric Hadamard matrix, and

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

is a symmetric Hadamard matrix with a constant diagonal.

If H_1, H_2 are both symmetric Hadamard matrices with constant diagonals, then so is $H_1 \otimes H_2$.

A Hadamard matrix H is *regular* if all row and column sums are equal.

3.14.2 Lemma. *If all rows of H have the same sum than H is regular and its order is a square.*

Proof. Suppose $H\mathbf{1} = k\mathbf{1}$ for some k. Then

$$H^T(k\mathbf{1}) = H^T H\mathbf{1} = n\mathbf{1}$$

and so

$$H^T\mathbf{1} = \frac{n}{k}\mathbf{1}.$$

We have shown the column sums are also constant. If we sum all of the entries in H we get

$$nk = n\frac{n}{k}$$

and so $k = \frac{n}{k} = \pm\sqrt{n}$. □

If H is regular, the sum of the entries of H is $\pm n\sqrt{n}$. It can be shown that if H is a Hadamard matrix of order n then the sum of the entries of H is at most $n\sqrt{n}$ and equality hold if and only if H is regular. In this case, we can get yet another design from the Hadamard matrix.

3.14.3 Lemma. *Let H be a $n \times n$ matrix with entries ± 1. Then H is a regular Hadamard matrix with row sum $2h$ if and only if $N = \frac{1}{2}(J - H)$ is the incidence matrix of a symmetric design with parameters*

$$(4h^2, 2h^2 - h, h^2 - h).$$

Proof. Left as an exercise; here $n = 4h^2$ and expanding NN^T will yield k, λ. □

A design with these parameters (or the complement) is said to be a *Menon design*.

3.14.4 Lemma. *A non-trivial symmetric (v, k, λ)-design is a Menon design if and only if $v = 4n$.*

3.15 Conference matrices

A $n \times n$ matrix C is a *conference matrix* if $C_{i,i} = 0$ for all i, $C_{i,j} \in \{\pm 1\}$ for $i \neq j$, and

$$CC^T = (n-1)I.$$

Examples: $\begin{pmatrix} 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

A conference matrix is *normalized* if all non-zero entries in the first row are equal, and all non-zero entries in the first column are equal.

3.15.1 Lemma. *If C is a skew-symmetric conference matrix, then $I + C$ is a Hadamard matrix.*

Proof.

$$(I + C)(I + C)^T = (I + C)(I - C) = I - C^2 = I + CC^T = nI. \quad \square$$

3.15.2 Lemma. *If C is a symmetric conference matrix then*

$$\begin{pmatrix} C + I & C - I \\ I - C & C + I \end{pmatrix}$$

is a Hadamard matrix.

Proof. Multiply HH^T. □

3.15.3 Lemma. *If C is a normalized conference matrix of order n then either $n \equiv 0 \mod 4$ and C is skew-symmetric or $n \equiv 2 \mod 4$ and C is symmetric.* □

3.15.4 Lemma. *If C is a conference matrix of order n and $n \equiv 2 \mod 4$, then $n-1$ is the sum of two squares.*

Proof. $CIC^T = (n-1)I$ and so I_n and $(n-1)I_n$ are equivalent as symmetric bilinear forms. By Witt cancellation, we deduce that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \approx \begin{pmatrix} n-1 & 0 \\ 0 & n-1 \end{pmatrix}.$$

Thus there is an invertible matrix with integer entries

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $AA^T = \begin{pmatrix} n-1 & 0 \\ 0 & n-1 \end{pmatrix}$. The $(1,1)$ entry of $AA^T = a^2 + b^2$ and the result follows. □

Recall that a conference matrix is a $n \times n$ matrix C such that C has 0 on the diagonal and $\{\pm 1\}$ off the diagonal such that $CC^T = (n-1)I$. If X is a strongly regular graph where $k = \frac{v-1}{2}$, then

$$C = A - (J - I - A)$$

is a conference matrix. These graphs are called *conference graphs*.

3.16 Latin square revisited

A *Latin square* is an $n \times n$ array with entries from $\{1, \ldots, n\}$ such that each integer appears exactly once in each row and in each column.

There is an alternative definition that will suit design theory. Suppose A is a matrix that represents a Latin square of order n. The Latin square actually consists of n^2 triples of the form

$$(i, j, A_{i,j})$$

which are the row number, column number and the entry in the specified row and column. We can write the Latin square as a $n^2 \times 3$ matrix whose rows are given by these triples. This matrix has the property that each ordered pair of columns each ordered pair of elements from $[n]$ appears exactly once.

Note that from a Latin square, one can construct this $n^2 \times 3$ matrix and vice-versa. Note there are many equivalences for Latin squares; in particular, permuting the columns of the $n^2 \times 3$ may give different Latin square matrices (not similar via permutation matrices).

An *orthogonal array* $OA(n,k)$ over $[n]$ is a matrix with k columns such that each ordered pair of column contains each ordered pair of elements from $[n]$ exactly once. It follows that $OA(n,k)$ has n^2 rows. An $OA(n,3)$ is a Latin square. What is $OA(n,2)$? It is the edge set of $K_{n,n}$. Two orthogonal arrays are *equivalent* if we can get one from the other by permuting rows, permuting columns and or permuting symbols.

What about $OA(n,4)$? The first three columns give a Latin square, say L_1, and taking the first two columns with the last column gives another Latin square, say L_2. If we look at all the entries in L_1 where the symbol is i, in L_2, looking in these entries, we should see all of the symbol $[n]$, exactly once. In this case, L_1, L_2 are said to be *mutually orthogonal Latin squares*.

From an orthogonal array $OA(n,k)$, we can get a graph on n^2 vertices. The vertices of the *orthogonal array graph* are the rows of $OA(n,k)$ and two rows are adjacent if they agree in some entry. Constructing $OA(n,4)$ from a Latin square corresponds to a proper colouring of the vertices of the Latin square graph (exercise).

3.16.1 Theorem (Neumaier)**.** *For a fixed τ, a strongly regular graph with least eigenvalue τ is either a conference graph, an orthogonal array graph, a Steiner triple system graph or one of finitely many sporadic graphs.*

This is as close as we can come to a classification of SRGs. Note that we have seen all these graphs in this class.

Here is an application of orthogonal arrays; we will use them to construct designs. Suppose we have a 2-$(v,k,1)$ design $\mathcal{D}$ with point set V and we want to construct 2-$(vk,k,1)$ design. (These parameters work.) We take k disjoint copies of $\mathcal{D}$; we take k copies of the original point set and k copies of each block. Now we have kb blocks and we need

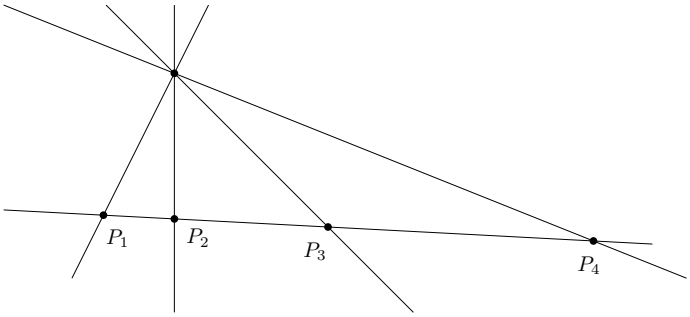
$$\frac{vk(vk-1)}{k(k-1)} - k\frac{v(v-1)}{k(k-1)} = v^2.$$

We need another v^2 blocks which are k-sets, consisting of one point from each copy of the point set. Exercise: show that we can do this using any $OA(v,k)$ and that this set must give an $OA(v,k)$.

Suppose we have a strongly regular graph whose parameter set is equal to the parameters of some orthogonal array graph. When is our graph constructible by an orthogonal array? Bose shows that when n,k are sufficiently large, the graph must be an orthogonal array graph. For Latin square graphs, on 36 vertices, there are 12 non-equivalent Latin square but more than 30000 graphs. But Bose's theorem says if $n \geq 22$, then all strongly regular graphs with the same parameters as Latin squares are in fact Latin square graphs.

3.17 Partial Geometries

A *partial geometry* is a point- and line-regular partial linear space with the property that there is a positive number α such that each point not on a line is collinear with α points on the line.



We write $PG(s,t,\alpha)$ to denote a partial geometry where each line "sits" on $s+1$ points and there are $t+1$ lines *t*hrough each point, such that for a point P and a non-incident line ℓ, there exists points $P_1,\ldots,P_\alpha$ on ℓ which are collinear with P.

So an $OA(n,k)$ is a $PG(k-1,n-1,k-1)$. A 2-design with $\lambda=1$ is $PG(k-1,r-1,k)$.

Facts:

(a) The point graph of a partial geometry is strongly regular.

(b) A $PG(s,t,s+1)$ is a equivalent to a 2-design with parameters $(st+s+1,s+1,1)$.

(c) A $PG(s,t,s)$ is equivalent to $OA(t+1,s+1)$.

(d) Take the incidence structure whose points are the edges of K_6 and blocks are the perfect matchings of K_6, this gives a partial geometry $PG(2,2,1)$.

(e) An incidence structure is a $PG(s,t,1)$ if it is point- and block-regular and its incidence graph has diameter 4 and girth 8.

(f) These partial geometries, where $\alpha=1$, are *generalized quadrangles*, and their point graphs are strongly regular with parameters

$$((s+1)(st+1),s(t+1),s-1,t+1).$$

3.18 Applications

I work in the intersection between algebraic graph theory and quantum computing. Loosely speaking, we can model any quantum algorithm as a quantum process on an underlying graph. Let X be a graph. The transition matrix of the continuous-time quantum walk on X is

$$U(t) = e^{itA}$$

is a matrix-valued function in time, where A is the adjacency matrix and $i = \sqrt{-1}$. Usually, we can take the series for e^x and evaluate $U(t)$ that way. In algebraic graph theory, we take spectral decomposition;

$$A = \sum_{\theta} \theta E_\theta$$

and

$$f(A) = \sum_{\theta} f(\theta) E_\theta$$

holds if f is a polynomial, but also when it any analytic function. In particular,

$$U(t) = \sum_{\theta} e^{it\theta} E_\theta.$$

This allows us to use usual tools in spectral graph theory and study this matrix.

One property that we study is perfect state transfer; if u, v are vertices of X such that there is some time τ such that

$$U(\tau)e_u = \gamma e_v$$

where $|\gamma| = 1$. For example, one can ask if there is PST between the end points of a path. Answer: only P_2 and P_3.

This leads to pretty good state transfer; if u, v are vertices of X such that for every $\epsilon > 0$, there is some time τ such that

$$||U(\tau)e_u - \gamma e_v|| < \epsilon.$$

Is there PGST between the ends of the path? There is PGST between the end points of the path P_n if and only if a) $n+1$ is a power of 2; b) $n+1 = p$ for some prime p; or c) $n+1 = 2p$ for some prime p. In some sense, this is a quantum prime detection algorithm. This is an example of the type of mathematics that done in this area.

Index