

Algebraic Graph Theory

Notes by Zach Schutzman

University of Pennsylvania, Fall 2017

Chapter 1 : Graphs	1	Chapter 4 : Arc-Transitive Graphs	31
Chapter 2 : Groups	8	Chapter 5 : Generalized Polygons and Moore Graphs	41
Chapter 3 : Transitive Graphs	17		

Introduction

Taking notes and working through proofs is the best way for me to teach myself advanced mathematics. Typing (and thoroughly backing up) notes is the best way to make sure they are preserved and readable well into the future. As such, these notes are from my process of working through *Algebraic Graph Theory* by Chris Godsil and Gordon Royle.

I am taking these notes under the assumption that the reader has a familiarity with the basic notions of graph theory and algebra. I omit elementary definitions and proofs from both domains. I may go back and fill some of these in if there comes a need or demand for it, but for now, they will be skipped.

My notation differs slightly from that used by Godsil and Royle, and is slightly more consistent with conventions from computer science and algorithmic graph theory at the expense of diverging from algebraic convention.

These notes are being written intermittently, as Algebraic Graph Theory is (currently) not my main research focus. I am using the editor TeXstudio. The template for these notes was created by Zev Chonoles and is made available (and being used here) under a Creative Commons License.

I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to the authors and those mathematicians they reference.

Please email any corrections or suggestions to ianzach+notes@seas.upenn.edu.

Chapter 1 : Graphs

What is Algebraic Graph Theory?

Algebraic graph theory (abbreviated **AGT** here ¹ is the subject which explores the relationship between algebra, which broadly studies the properties of abstract mathematical structures, and graph theory, which broadly studies a very particular kind of concrete mathematical structure. Among these subjects are graph groups and morphisms, spectral graph theory, graph cuts and flows, colorings, and knots.

Definitions and Fundamentals

If X is a graph, we let $V(X)$ and $E(X)$ denote the vertex set and edge set of X , respectively, using $A(X)$ for the arc set of X in settings with directed graphs. Unless otherwise specified, we assume all graphs are undirected. If vertices $u, v \in V(X)$, then we write $(u, v) \in E(X)$ to represent the edge between u and v (or $(u, v) \in A(X)$ to denote the arc *from* u *to* v).

Definition. Two graphs X and Y are **isomorphic** if there exists a bijective function $\phi : V(X) \rightarrow V(Y)$ such that $(\phi(u), \phi(v)) \in E(Y)$ if and only if $(u, v) \in E(X)$.

Definition. A **subgraph** Y of a graph X is a graph such that $V(Y) \subset V(X)$ and $E(Y) \subset E(X)$. An **induced subgraph** is one such that $E(Y)$ consists exactly of the edges (u, v) in X such that u and v are both in $V(Y)$. That is, an induced subgraph is one which can be realized by deleting vertices from X and removing only those edges incident to those removed vertices. A **spanning subgraph** is one such that $V(Y) = V(X)$.

Definition. A **cycle** is a subgraph such that every vertex has degree 2. A **tree** is a graph such that no subgraph is a cycle. A **spanning tree** is a spanning subgraph with no cycles.

Definition. A set of vertices which induce an empty (edge-free) subgraph is called an **independent set**. A set of vertices which induces a complete graph is called a **clique**. The largest independent set and clique in a graph X are denoted $\alpha(X)$ and $\omega(X)$, respectively.

These values $\alpha(X)$ and $\omega(X)$ will come back later.

Definition. A **connected component** of a graph is a collection of vertices such that there exist a path between all pairs.

While adjacency in a graph is not an equivalence relation (it's not transitive), membership in connected components is, hence a graph can be partitioned into disjoint connected components.

Graph Automorphisms

Definition. An **automorphism** of a graph X is an isomorphism $X \rightarrow X$.

The set of automorphisms of a graph form a group. The identity function is clearly an automorphism, and if g is an automorphism, then its inverse, g^{-1} is as well. We can also compose automorphisms to get another automorphism, and this inherits associativity from function composition. By Cayley's theorem, we can think about $Aut(X)$ as being a subgroup of $Sym(V(X))$, the symmetric group on

¹Not to be confused with *algorithmic game theory*, an area of mathematics and computer science much closer to my primary research interests...

the vertices of X . We'll write $Sym(n)$ for $n = |V(X)|$ to denote the symmetric group on n elements in place of $Sym(V(X))$.

In general, it is difficult to determine whether two graphs are isomorphic (this is a well-known NP problem) or whether a graph has a nontrivial automorphism. However, some cases are easy. For a complete graph K_n , $Aut(X) = Sym(n)$, and the same holds for an empty graph on n vertices.

If v is a vertex and g a group element, we denote v^g the action of g on v . If $g \in Aut(X)$ and Y is a subgraph of X , then we denote $Y^g = \{x^g | x \in V(Y)\}$. Then we have that $E(Y^g) = \{(u^g, v^g) | (u, v) \in E(Y)\}$. The graphs Y and Y^g are isomorphic, and Y^g is a subgraph of X .

Definition. The **valency** of a vertex x is the number of neighbors of x in the graph X . We can talk about the maximum and minimum valencies over all vertices of a graph.

Lemma. *If x is a vertex of a graph X and g is an automorphism of X , then the vertex $y = x^g$, has the same valency as x .*

Proof. Let $N(x)$ be the subgraph of X induced by x and its neighbors. Then $N(x)^g \cong N(x^g) \cong N(y)$, so $N(x) \cong N(y)$ as subgraphs of X , so they have the same number of vertices. Thus the valencies of x and y are equal. \square

Corollary. *An automorphism of a graph necessarily permutes vertices of the same valency.*

Definition. A graph where every vertex has valency k is called **k -regular**.

Definition. The **distance** between vertices x and y is the length of the shortest path in X between x and y , denoted $d_X(x, y)$ or $d(x, y)$ if it is clear which graph we are talking about.

Lemma. *If g is an automorphism of a graph X , then $d_X(x, y) = d_X(x^g, y^g)$ for all pairs of vertices.*

Proof. If they are the same vertex, the distance $d(x, y) = d(x^g, y^g) = 0$ is trivially preserved. If $d(x, y) = 1$, then x and y are adjacent, so their images x^g and y^g must be adjacent as well, by definition of graph isomorphism.

Suppose, for the sake of contradiction that $d(x, y) \leq d(x^g, y^g)$. Then there is some path $x, r_2, r_3, \dots, r_{n-1}, y$ such that r_{n-1}^g is not adjacent to y^g . But this is impossible, as automorphism preserves adjacency, and r_{n-1} is adjacent to y . A symmetric argument on g^{-1} gives the case where $d(x, y) \geq d(x^g, y^g)$. \square

Definition. The **complement** of a graph X , denoted \overline{X} , is the graph such that $V(\overline{X}) = V(X)$ and $E(\overline{X}) = \{(u, v) | (u, v) \notin E(X)\}$. That is, the complement of a graph is the one which has an edge between two vertices if and only if the original graph does not.

Lemma. $Aut(X) = Aut(\overline{X})$.

Proof. Since automorphisms preserve adjacency, they also preserve non-adjacency. Thus x^g is not adjacent to y^g if and only if x and y are not adjacent. Therefore, $g \in Aut(\overline{X})$. \square

We'll quickly note that automorphisms of directed graphs also preserve the direction of the arcs.

Graph Homomorphisms

Definition. A **graph homomorphism** is a function $\phi : V(X) \rightarrow V(Y)$ such that if u and v are adjacent in X , they are adjacent in Y .

We'll quickly contrast this to isomorphisms, which preserves adjacency in both directions, whereas a homomorphism only requires that adjacent vertices in X are still adjacent in Y under ϕ . Every isomorphism is a homomorphism, but not every homomorphism is an isomorphism.

Definition. A graph is **bipartite** if there exists a partition of $V(X)$ into disjoint sets A and B such that every edge has one end in A and the other in B . Analogously, we can define **k -partite** graphs as being those which admit a partition into k components such that no edge has both endpoints in the same component.

If a graph is bipartite, there exists a homomorphism $X \rightarrow K_2$ where the image of each component is one of the vertices in K_2 . Similarly, there is a homomorphism from a k -partite graph onto K_k .

This leads to the notion of *proper colorings*.

Definition. A **proper coloring** is a map from $V(X)$ to a finite set of colors such that for any edge $(u, v) \in E(X)$, u and v are assigned different colors.

Definition. The **chromatic number** of a graph, denoted $\chi(X)$ is the minimum number k such that X can be properly k -colored.

Nonempty bipartite graphs have chromatic number 2. Complete graphs K_n have chromatic number n .

Let's observe that the set of vertices assigned some particular color, called a *color class*, forms an independent set in X .

Lemma. *The chromatic number of a graph $\chi(X)$ is the minimum number r such that there exists a homomorphism from X to K_r .*

Proof. Suppose $\phi : V(X) \rightarrow V(Y)$ is a homomorphism. For $y \in V(Y)$, define $\phi^{-1}(y)$ to be $\phi^{-1}(y) = \{x \in V(X) \mid \phi(x) = y\}$, the set of elements in $V(X)$ which map to Y under ϕ . As y is not adjacent to itself, $\phi^{-1}(y)$ is an independent set. Hence if Y has r vertices, each of the r sets is independent and forms a color class of an r -coloring, so X can be properly r -colored. Conversely, suppose that X can be properly r -colored. Then there exists a homomorphism onto K_r which sends each color class to a unique vertex. \square

Definition. A **retraction** is a homomorphism ϕ from X to Y where Y is a subgraph of X such that the restriction of X to Y is the identity map.

If X is a graph with a k -clique, then any k -coloring of X determines a retraction of X onto the clique.

When we think about directed graphs, we will also stipulate that homomorphisms preserve the directions of arcs.

Definition. An **endomorphism** of a graph is a homomorphism from a graph to itself. The set of endomorphisms, $End(X)$, forms a monoid. An automorphism is a special case of an endomorphism, so $Aut(X)$ is a submonoid of $End(X)$.

Circulant Graphs

Let's give a more particular definition of a *cycle* in a graph. We can think of a cycle of n vertices as a set $C_n = \{0, 1, 2, \dots, n-1\}$ of vertices such that i and j are adjacent if and only if $j - i \equiv \pm 1 \pmod n$.

Let's look at some automorphisms of the cycle. The set of permutations which map i to $i + 1$ (and $n - 1$ to 0) forms a subset of $\text{Aut}(C_n)$. By composition, we can realize an entire copy of the cyclic group on n elements (\mathbb{Z}_n) in this way. Also, the permutation h which sends i to $-i \pmod n$ is an element of $\text{Aut}(C_n)$. We have that $h(0) = 0$ but the cyclic group is fixed point-free, so this automorphism isn't contained in that subgroup. Also, $h = h^{-1}$, so there are two cosets induced by this element, and the order of $\text{Aut}(C_n)$ is at least $2n$. (In fact, it's equal to $2n$, but we can't quite prove that yet...)

The cycles are a subclass of the *circulant graphs*. If $C \subset \mathbb{Z}_n \setminus \{0\}$, then we can construct the directed graph $X = X(\mathbb{Z}_n, C)$ through the following process. First, let $V(X)$ be the elements of \mathbb{Z}_n and let $(i, j) \in A(X)$ if and only if $j - i \in C$. This graph $X(\mathbb{Z}_n, C)$ is called a *circulant of order n* and C is its *connection set*. If C itself is also closed under additive inverses (modulo n), then (i, j) is an arc in X if and only if (j, i) is, so we can view the graph as being undirected. In this case, the map which sends i to $-i$ is an automorphism, and the map which sends i to $i + 1$ is always an automorphism of a circulant graph, so the automorphism group of a circulant graph with an inverse-closed connection set is at least $2n$. We can think of the ordinary cycle on n vertices as being $X(\mathbb{Z}_n, \{-1, 1\})$. The complete graph is a circulant graph with connection set \mathbb{Z}_n , and an empty graph is one with empty connection set. Since these graphs have automorphism groups with order $n!$, we clearly have examples of circulant graphs with orders much larger than $2n$.

Johnson Graphs

Now we consider another family of graphs, denoted $J(v, k, i)$ for positive integers $v \geq k \geq i$. Let Ω be some fixed set of size v . The vertices of $J(v, k, i)$ are the subsets of Ω with size k , and two vertices are adjacent if and only if their corresponding sets have intersection size i . Thus $J(v, k, i)$ has $\binom{v}{k}$ vertices, and it is a regular graph in which each vertex has valency $\binom{k}{i} \binom{v-k}{k-i}$. We'll assume $v \geq 2k$.

Lemma. *The function which maps a set of size k to its complement in Ω is an isomorphism between the graphs $J(v, k, i)$ and $J(v, v - k, v - 2k + i)$.*

Proof. The proof of this is just a DeMorgan's Laws definition-chase.

If $|A| = |B| = k$, then $|\overline{A}| = |\overline{B}| = v - k$.

If A and B are adjacent, then $|A \cap B| = i$, so $|\overline{A} \cap \overline{B}| = |\overline{A \cup B}| = v - 2k + i$.

Therefore, if we define a map by mapping a set to its complement and adjacency occurs if and only if the intersection of the sets is size $v - 2k + i$, this is indeed an automorphism, as A and B are adjacent if and only if \overline{A} and \overline{B} are adjacent, and set complements is an obvious bijection between the vertex sets.

□

A graph is called a *Johnson graph* if it is isomorphic to $J(v, k, k - 1)$. The *Kneser graphs* are isomorphic to $J(v, k, 0)$. As an example, the Petersen graph, which we will study later, is $J(5, 2, 0)$ and is therefore a Kneser graph.

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

Proof. Let g be a permutation of Ω and $S \subset \Omega$, and let S^g denote the image of S under g . Any such g also determines a permutation of the subsets S of size k . In particular, if S and T are of size

k , then $|S \cap T| = |S^g \cap T^g|$, so g is an automorphism of $J(v, k, i)$. \square

We note that $\text{Aut}(J(v, k, i))$ acts on a set of size $\binom{v}{k}$, so when this quantity is not equal to v , it's not equal to $\text{Sym}(v)$, but it is *usually* isomorphic, which is often not an easy thing to prove.

Line Graphs

Definition. If X is a graph, the **line graph** of X , denoted $L(X)$ is the graph where the vertices of $L(X)$ correspond to edges of X and two vertices in $L(X)$ are adjacent if and only if the corresponding edges in X are incident to the same vertex.

As examples, the star $K_{1,n}$ (one hub with n ‘spokes’) has line graph K_n , as all n edges in the star are incident to the center vertex. The path graph on n vertices P_n has $L(P_n) = P_{n-1}$. The cycle C_n is isomorphic to its own line graph.

Lemma. *If X is regular with valency k , then $L(X)$ is regular with valency $2k - 2$.*

Proof. Each vertex has degree k , so when we translate each edge into a vertex, for each original vertex, we get a k -clique, but each of these new vertices belongs to two such cliques. Thus each vertex has $k - 1$ adjacent vertices in each of the cliques it belongs to, thus a total valency of $2k - 2$. \square

Theorem. *A graph is the line graph of some other graph if and only if there exists a partition of its vertex set into cliques such that each vertex belongs to at most two cliques.*

Proof. To see that the condition is necessary, observe that the process of constructing a line graph necessarily turns the neighborhood of each vertex into a clique, and since an edge connects two vertices, each new vertex belongs to at most two such cliques.

To see that it is sufficient, we will construct a graph from a line graph which decomposes into cliques in this way. Let S_1, S_2, \dots, S_k be the cliques, and let v_1, v_2, \dots, v_m be the vertices (if there are any) which are in exactly one S_i . The vertex set of our graph will be $S_1, \dots, S_k, \{v_1\}, \dots, \{v_m\}$ with an edge between sets if and only their intersection is nonempty. It is clear that the line graph of this graph is our original graph, and we are done. \square

Observe that if X and Y are isomorphic, then $L(X)$ and $L(Y)$ are isomorphic, but the converse isn't true, as K_3 and $K_{1,3}$ have the same line graphs.

Lemma. *If X and Y are graphs with minimum valency at least 4, then $X \cong Y$ if and only if $L(X) \cong L(Y)$.*

Proof. Let C be a clique in $L(X)$ with $|C| = c < 4$. The vertices in C correspond to a set of c edges in X , all of which are incident to a common vertex x . Thus, there is a bijection between vertices of X and maximal cliques in $L(X)$ which maps adjacent vertices in X to pairs of cliques in $L(X)$ which share exactly one vertex. We can similarly construct an analogous bijection between Y and $L(Y)$. Let $f : X \rightarrow L(X)$ and $g : Y \rightarrow L(Y)$ be these functions.

If we assume $X \cong Y$ by ϕ , then we want to show that $L(X) \cong L(Y)$ by demonstrating that $g \circ \phi \circ f^{-1} : L(X) \rightarrow L(Y)$ is an isomorphism. It suffices to show that the image of a k -clique under this composite function is a k -clique in $L(Y)$. But this is obvious. f^{-1} takes a maximal k -clique to

a set of k edges in X incident to some vertex x , which has valency k . Then $\phi(x) = y$ is some vertex in Y with valency k , so g sends this neighborhood to a maximal k -clique.

The other direction has an identical proof, except that we show that vertices in X and Y with equal valency are mapped to each other. \square

Theorem. *A graph is a line graph if and only if each induced graph on at most six vertices is also a line graph.*

Proof. This is an alternative phrasing of Beineke's Theorem. I'll fill in a proof later. \square

Corollary. *The set of graphs which are not line graphs but every induced subgraph is a line graph is finite and, in fact, of size nine.*

Definition. A bipartite graph is **semiregular** if it has a proper 2-coloring such that all vertices of the same color have the same valency. As an example, the complete bipartite graphs $K_{m,n}$ (a set of m vertices connected to each of a set of n vertices) are semiregular.

Lemma. *If the line graph of a graph is regular, then the graph itself is regular or a semiregular bipartite graph.*

Proof. Suppose $L(X)$ is k -regular. If u and v are adjacent in X , then their valencies sum to $k + 2$, so all neighbors of u have the same valency, so if two vertices share a neighbor, they have identical valencies. This only occurs in graphs which are regular or bipartite and semiregular, as if it contains an odd cycle, it must have two adjacent vertices with the same valencies, and bipartite graphs have no odd cycles. \square

Planar Graphs

Definition. A graph is called **planar** if it can be drawn (in the plane) without crossing edges. More precisely, a graph is planar if there exists a function which maps each vertex to a unique point in \mathbb{R}^2 and each edge to a non-self-intersecting curve with endpoints equal to the image of the vertices it's incident to such that no two such curves intersect. Such a function is called a **planar embedding**.

Definition. A **plane graph** is a planar graph together with a planar embedding.

The edges of a plane graph divide the plane into disjoint regions called *faces*. All but one (the *external* or *infinite*) face is bounded. The *length* of a face is the number of edges bounding it.

Theorem (Euler). *If $v - e + f = 2$, where v, e, f are the number of vertices, edges, and faces of a plane graph, respectively.*

Proof. The proof proceeds by strong induction on the number of edges. Observe that a tree on v vertices is a planar graph with $v - 1$ edges and 1 face. If a planar graph is not a tree, it contains a cycle. Removing an edge in this cycle (which does not disconnect the graph) merges two faces, which preserves the quantity $v - e + f$. Since a tree is a graph without cycles, and this process eventually transforms a graph into a tree, but since a tree satisfies $v - e + f = 2$, this quantity must be preserved at all steps of the process, hence it is true for the original graph. \square

Definition. A **maximal planar graph** is one in which adding an edge between any two vertices which are not already adjacent makes the graph non-planar. If a planar graph has an embedding where the length of some face is greater than 3, we can add edges interior to this face in without violating planarity. Thus any maximal planar graph must have every face be of length 3, called a **planar triangulation**.

In a triangulation, each edge is incident to two faces, so we have $3f = 2e$. Then by Euler's theorem, $e = 3n - 6$. Any planar graph with $3n - 6$ edges must be maximal and a planar triangulation.

A planar graph may have multiple distinct embeddings, and they don't necessarily preserve the lengths of the faces (although it must preserve the *number* of faces). It is a result in topological graph theory that a 3-connected planar graph has a (topologically) unique planar embedding.

Given a plane graph X , we can construct its dual X^* , where each face of X becomes a vertex of X^* with edges between vertices in X^* if and only if there is an edge separating the corresponding faces in X . Sometimes this gives rise to multiple edges between vertices, but we'll be sure to only worry about that if we have to.

The dual of a planar graph is connected, so if X is not connected, $(X^*)^*$ is not isomorphic to X , but this is true if X is connected.

We can generalize the notion of planar embeddings to embeddings in any surface. The dual is defined analogously in these topological spaces. The real projective plane \mathbb{RP}^2 is a non-orientable surface which looks like the closed disk with an antipodal identification along the boundary. The graph K_6 is not planar, but it does have an embedding in \mathbb{RP}^2 (which is triangular!), and its dual in this space is cubic, and turns out to be the Petersen graph.

The torus is an orientable surface, which looks like the surface of a donut. We can represent it as a rectangle with opposite edges identified. The graph K_7 is not planar, but there is an embedding on the torus (which is also triangular!), and its dual is the Heawood graph.

Chapter 2 : Groups

Permutation Groups

Given a set V of size n , we denote the set of all permutations of V as $Sym(V)$ or $Sym(n)$. A *permutation group* on V is some subgroup of $Sym(V)$, and for a graph X , we can think of $Aut(X)$ as some permutation group on its vertex set.

By Cayley's Theorem, *any* finite group G can be thought of as a permutation group on the set of its elements.

Definition. A **permutation representation** of a group G is a (group) homomorphism from G into $Sym(V)$ for some set V . Such a representation is called **faithful** if this homomorphism is injective².

A permutation representation is sometimes called a *group action*, in which case we say that G *acts (faithfully) on V* . A group acting on a set induces a whole bunch of other actions. For example, if $S \subset V$, then for any $g \in G$, S^g is also a subset of V (realized by applying the action of g to each element of S), called the *translate of S by g* . We can note that $|S| = |S^g|$, so G can be thought of as permuting *subsets* of V , so for any fixed k , G induces a group action on the k -subsets of V , or on ordered k -tuples in V .

Definition. A subset $S \subset V$ is **G -invariant** with respect to a permutation group on V if $s^g \in S$ for all $s \in S$ and $g \in G$. That is, any group action sends an element of S to another element of S . We sometimes say that S is *invariant under G* .

If S is G -invariant, each group element g permutes the elements of S . Write $g|_S$ to denote the restriction of g to S . Then the map $g \mapsto g|_S$ is a group homomorphism from G into $Sym(S)$, and the image is a permutation group in S , which we write $G|_S$ or G^S .

Definition. A permutation group on V is called **transitive** if given any $x, y \in V$, there is a group element $g \in G$ such that $x^g = y$.

Definition. If S is a G -invariant subset of V and $G|_S$ is transitive, then S is an **orbit** of G . For any $x \in V$, the set $x^G = \{x^g | g \in G\}$ is an orbit of G .

It's easy to see that the orbits of G form equivalence classes (if $y = x^g$, then $y^{g^{-1}} = x$, so they belong to the same orbit) and therefore partition V . Any G -invariant subset of V is therefore the union of some collection of orbits. In fact, an orbit is, in a sense, a *minimal* G -invariant subset containing a particular element.

Counting

Definition. If G is a permutation group on V , the **stabilizer** G_x of an element $x \in V$ is the set of group elements g such that $x^g = x$.

It's not too hard to see that the stabilizer of an element forms a subgroup. Clearly the identity is in G_x . For any $h \in G_x$, $h^{-1} \in G_x$ as applying the group actions in order should be the same as applying the product of the group actions. A similar argument shows closure and associativity.

We can generalize the idea to sets. If x_1, x_2, \dots, x_r are distinct elements of V , then the stabilizer

²equivalently, the kernel is trivial, or each element of G maps to a unique permutation

$$G_{x_1, x_2, \dots, x_r} = \bigcap_{i=1}^r G_{x_i}$$

is also a subgroup of G , formed by the pointwise intersection of the stabilizers of the elements we looked at, and is called the *pointwise stabilizer* of $\{x_1, x_2, \dots, x_r\}$. If S is a subset of V , then the stabilizer G_S of S is the subset of G formed by all group elements $g \in G$ such that $S^g = S$. Since we only insist that elements of S are permuted, rather than fixed, this is called the *setwise stabilizer* of S .

Lemma. *If V is a set, G a group acting on V , and S an orbit of G . If x and y are elements of S , the set of group elements which map x to y is a right coset of G_x . Conversely, all elements of a right coset of G_x map to the same element of S .*

Proof. Since G is transitive on S , there is some g such that $x^g = y$. If $h \in G$ and $x^h = y$, then $x^g = x^h$ (as both equal y), and $x^{hg^{-1}} = x$, so $hg^{-1} \in G_x$, and $h \in G_x g$, which is thus the coset containing all elements which map x to y .

For the converse, we need to show that every element of $G_x g$ maps x to the same element. Every element of this coset looks like hg for some $h \in G_x$. Since $x^{hg} = (x^h)^g = x^g$, all elements of $G_x g$ map x to x^g , and we are done.

□

A consequence of this is the famed Orbit-Stabilizer Theorem:

Theorem (Orbit-Stabilizer). *If G is a group acting on V and x is an element of V , then $|G_x||x^G| = |G|$.*

Proof. The proof follows almost immediately from the previous lemma. The points of x^G are in bijection with the cosets of G_x , so by Lagrange's Theorem, the product of the size of a coset with the number of cosets is equal to the order of the group. □

If x and y are distinct points in some orbit of G , how are G_x and G_y related?

Definition. If a group element can be written as $g^{-1}hg$, it is said to be **conjugate** to h (by g). The set of all elements conjugate to h is called the **conjugacy class** of h . Given any group element g , the map $\tau_g : h \mapsto g^{-1}hg$, called **conjugation by g** is a permutation of G .

The set of all such maps forms a group isomorphic to G which has orbits coinciding with conjugacy classes. If $H \subset G$ and $g \in G$, we write $g^{-1}Hg = \{g^{-1}hg | h \in H\}$. If H is a subgroup, then $g^{-1}Hg$ is also a subgroup, and is isomorphic to H . In this case, we say $g^{-1}Hg$ is *conjugate to H* .

Lemma. *Let G be a group acting on V and x an element of V . If $g \in G$, then $g^{-1}G_x g = G_{x^g}$. That is, the stabilizers of two points in the same orbit are conjugate.*

Proof. Let $x^g = y$. First, we need to show that every element of $g^{-1}G_x g$ fixes y . Take $h \in G_x$. Then $y^{g^{-1}hg} = x^{hg} = x^g = y$, so $g^{-1}hg \in G_y$, but if $h \in G_y$, then $ghg^{-1} \in G_x$, so in fact $g^{-1}G_x g = G_y$.

□

If g is a permutation of V , denote $\text{fix}(g)$ the set of points in V fixed by g . That is, $\text{fix}(g) = \{v \in V | v^g = v\}$.

Lemma (Burnside³). *Let G be a group acting on V . Then the number of orbits of G is equal to the average number of elements of V fixed by a group element.*

Proof. Let the pair (g, x) be a group element and an element of V , respectively. We'll count these in two ways. First, summing the number of fixed elements $fix(g)$ over all elements $g \in G$, we get $\sum_{g \in G} |fix(g)|$ is one representation of the total number of such pairs, and is equal to the size of G times the average number of fixed points. Alternatively, if we sum over elements of V , we note that the number of elements of G which fix an $x \in V$ is the size of the orbit G_x . Thus the number of such pairs can also be written $\sum_{x \in V} |G_x|$.

Since $|G_x|$ is constant as x goes over an orbit, the contribution of each orbit is $|x^G||G_x|$, which equals $|G|$. Thus the total sum is $|G|$ times the number of orbits, which is what we wanted to show. \square

Asymmetric Graphs

Definition. A graph is **asymmetric** if its automorphism group is trivial. It turns out that, asymptotically, almost all graphs are asymmetric. That is, as the number of vertices grows, the fraction of total possible graphs which are asymmetric approaches 1.

Let V be a set of size n and consider all distinct graphs on a vertex set of size n . Let K_n denote a fixed copy of the complete graph on n vertices. Clearly there is a one-to-one correspondence between these graphs and subsets of $E(K_n)$ (the edge set of K_n), as we can identify a graph uniquely by listing which edges are (or are not) present. Thus there are $2^{\binom{n}{2}}$ graphs on n vertices.

Definition. If X is a graph, the set of graphs isomorphic to X is called the **isomorphism class** of X . These classes partition the set of graphs with vertex set V (as isomorphism is an equivalence relation). Two graphs X and Y belong to the same class if (and only if!) there exists a permutation in $Sym(V)$ such that the edge set of X to the edge set of Y . In this way, an isomorphism class is an orbit of $Sym(V)$ as an action on $E(K_n)$.

Lemma. *If the line graph of a graph is regular, then the graph itself is regular or a semiregular bipartite graph.*

Proof. This follows from the Orbit-Stabilizer Theorem. An isomorphism class is an orbit, $Aut(X)$ is a stabilizer of X , and $n!$ is the order of $Sym(V)$. \square

We want to count the number of isomorphism classes, to do which we will use Burnside's Lemma by finding the average number of subsets of $E(K_n)$ fixed by an element of $Sym(V)$. We can see that if a group element g has r orbits, it fixes 2^r subsets as an action on the power set of $E(K_n)$ (permuting subsets). For any such g , let $orb_2(g)$ denote the number of orbits of g as an action on $E(K_n)$. Then Burnside's Lemma tells us that the number of isomorphism classes of graphs on vertex set V is equal to

$$\frac{1}{n!} \sum_{g \in Sym(V)} 2^{orb_2(g)}$$

³This goes by 'Burnside's Lemma' (not to be confused with Burnside's $p^a q^b$ theorem), but proper attribution is to Cauchy and Frobenius.

If every graph were to be asymmetric (we know this isn't the case), we would have that each isomorphism class has exactly $n!$ members and $\frac{2^{\binom{n}{2}}}{n!}$ classes. Even though this isn't true, we'll show next that it's pretty close, and asymptotically, this is the limit.

Lemma. *The number of isomorphism classes of graphs on n vertices is at most $(1 + o(1))\frac{2^{\binom{n}{2}}}{n!}$.*

Proof. The support of a permutation is the set of elements *not* fixed by it. We first claim that over all permutations g with support size $2r$, the one which maximizes $\text{orb}_2(g)$ is one which is composed of the product of r 2-cycles. To see this, let g be such an element. We have that g fixes $n - 2r$ elements and that $g^2 = e$, so the size of the orbit of any pair of elements is one or two. There are two ways that an edge can not be fixed by g . Either x and y are both in the support of g but $x^g \neq y$ or x is in the support but y is not, or vice versa. There are $2r(r - 1)$ edges in the former category and $2r(n - 2r)$ in the latter. Thus the number of orbits of length 2 is $r(n - r - 1)$ and the total number of orbits $\text{orb}_2(g) = \binom{n}{2} - r(n - r - 1)$.

Now, we're going to partition the permutations in $\text{Sym}(n)$ into three classes and estimate the contribution of each to the sum in the statement of the lemma.

Fix $m \leq n - 2$ an even integer, and split the permutations in $\text{Sym}(n)$ into three classes as follows. $\mathcal{C}_1 = \{e\}$, \mathcal{C}_2 is the set of permutations with support at most m , and \mathcal{C}_3 is everything else. We can approximate the sizes of these by saying that $|\mathcal{C}_1| = 1$, $|\mathcal{C}_2| \leq \binom{m}{n} n! \leq n^m$, and $|\mathcal{C}_3| \leq n! \leq n^n$.

An element $g \in \mathcal{C}_2$ has the maximum number of orbits on pairs if it is a single 2-cycle, in which case the number of orbits is $\binom{n}{2} - (n - 2)$. An element $g \in \mathcal{C}_3$ has a maximum number of orbits when it is the composition of $\frac{m}{2}$ 2-cycles, in which case it has

$$\binom{n}{2} - \frac{m}{2}(n - \frac{m}{2} - 1) \leq \binom{n}{2} - \frac{nm}{4}$$

such orbits.

Thus (taking $m = \lfloor c \log n \rfloor$ for $c > 4$)

$$\begin{aligned} \sum_{g \in \text{Sym}(V)} 2^{\text{orb}_2(g)} &\leq 2^{\binom{n}{2}} + n^m 2^{\binom{n}{2} - (n-2)} + n^n 2^{\binom{n}{2} - \frac{nm}{4}} \\ &= 2^{\binom{n}{2}} \left(1 + n^m 2^{-(n-2)} + n^n 2^{-\frac{nm}{4}} \right) \\ &= 2^{\binom{n}{2}} \left(1 + 2^{m \log n - n + 2} + 2^{n \log n - nm/4} \right) \\ &= 2^{\binom{n}{2}} (1 + o(1)) \end{aligned}$$

□

Lemma. *Almost all graphs are asymmetric.*

Proof. Suppose the proportion of isomorphism classes of graphs which are asymmetric is μ . Each class which is *not* asymmetric contains at most $\frac{n!}{2}$ elements, whereas the average size of a class is

$$n! \left(\mu + \frac{1 - \mu}{2} \right) = \frac{n!}{2} (1 + \mu)$$

So,

$$\frac{n!}{2}(1+\mu)(1+o(1))\frac{2^{\binom{n}{2}}}{n!} > 2^{\binom{n}{2}}$$

and thus as n goes to ∞ , μ goes to 1. Since the proportion of isomorphism classes which are asymmetric is at least as large as the proportion of isomorphism classes (an isomorphism class of an asymmetric graph is a singleton), the proportion of graphs which are asymmetric goes to 1 as n goes to ∞ . □

Although most graphs are asymmetric, it is surprisingly hard to actually cook up a graph which is certainly asymmetric. Here is one such construction. Let T be a tree such that no vertices have valency 2 and at least one vertex has valency strictly greater than two. Assume that it has exactly m leaves. We can construct a *Halin graph* by drawing T in the plane, then constructing an m -cycle by connecting each of the m leaves in a cycle. This graph is still planar and is asymmetric. Halin graphs have some interesting properties. It's not too hard to construct a cubic (3-regular) Halin graph which is asymmetric which also has the property that it is strongly 3-connected, but any proper subgraph is at most 2-connected.

Orbits on Pairs

Let G be a transitive permutation group acting on the set V (that is, G induces a single orbit on V). Then we can think of G as acting on $V \times V$, the set of ordered pairs of elements of V .

Definition. The orbits of G on $V \times V$ are called **orbitals**.

Since G is transitive, the set $\{(x, x) | x \in V\}$ is certainly an orbital of G , called the *diagonal orbital*. If $\Omega \subset V \times V$, we denote the *transpose* of Ω as Ω^T , which is the set $\{(y, x) | (x, y) \in \Omega\}$.

Claim. Ω is G -invariant if and only if Ω^T is G -invariant.

Proof. Since transposition is an involution, we only need to show one direction, as without loss of generality, we can show the other direction by exchanging the roles of Ω and Ω^T .

Suppose Ω is G -invariant. Then any element of G sends something in Ω to something else in Ω . Thus $(x, y) \in \Omega$ implies $(x^g, y^g) \in \Omega$ for any g . But if (x, y) and (x^g, y^g) are both in Ω , then (y, x) and (y^g, x^g) are in Ω^T , so Ω^T is G -invariant as well. □

It follows from this fact that if Ω is an orbital, then $\Omega^T = \Omega$ or $\Omega^T \cap \Omega = \emptyset$. That is, an orbital either contains all of the diagonal or none of it. If $\Omega = \Omega^T$, we call Ω a *symmetric orbital*.

Lemma. Let G be a group acting on a set V and let $x \in V$. There exists a bijection between the orbits of G on $V \times V$ and the orbits of G_x on V .

Proof. Let Ω be an orbit of G on $V \times V$ and denote Y_Ω the set $\{y | (x, y) \in \Omega\}$. We will show that Y_Ω is an orbit of G_x acting on V . If y and y' are in Y_Ω , then (x, y) and (x, y') are in Ω , so there is a $g \in G$ such that $(x, y)^g = (x, y')$. Thus $g \in G_x$ and $y^g = y'$, so y and y' are in the orbit of G_x . Conversely, if $(x, y) \in \Omega$ and $y' = y^g$ for some $g \in G_x$, then $(x, y') \in \Omega$. Thus Y_Ω is an orbit of G_x . Since V is partitioned by the sets Y_Ω as we let Ω range over all the orbits of $V \times V$, we are done. □

This tells us that for any $x \in V$, each orbit Ω of G on $V \times V$ is associated with a *unique* orbit of G_x . The number of orbits of G_x on V is called the *rank* of the group G . If Ω is a symmetric orbit, the corresponding G_x is called *self-paired*. Each orbit Ω can be thought of as a directed graph with vertices V and arcs Ω . When Ω is symmetric, the graph is undirected. By the claim above, if this graph is directed, at most one arc exists between any pair of vertices. Such a directed graph is called an *oriented graph*, and we will see these again later.

Lemma. *Let G be a transitive permutation group acting on V and let Ω be an orbit of G on $V \times V$, and let $(x, y) \in \Omega$. Then Ω is symmetric if and only if there is a $g \in G$ such that $x^g = y$ and $y^g = x$.*

Proof. If (x, y) and (y, x) are in Ω , then there exists a g such that $(x, y)^g = (x^g, y^g) = (y, x)$.

If there exists a g such that $x^g = y$ and $y^g = x$, then g swaps x and y . Since $(x, y)^g = (y, x)$ and both are in Ω , it follows that $\Omega = \Omega^T$, as we know $\Omega \cap \Omega^T \neq \emptyset$. \square

Note that if there is a permutation g which swaps x and y , then (xy) is a cycle in g (in canonical form). Thus g must have even order, so the whole group G must also have even order.

Definition. A permutation group G acting on a set V is **generously transitive** if for any two distinct $x, y \in V$, there is a group element $g \in G$ which swaps them. Generous transitivity is equivalent to all orbits of $V \times V$ being symmetric.

Each orbital of a transitive permutation group G on V gives rise to a graph which is either undirected or oriented. Clearly, G acts as a transitive group of automorphisms on each of these graphs, and the union of any set of orbitals is a directed graph (or not) on which G acts transitively.

Example. Let V be the set of 35 triples from a fixed set of seven elements. The symmetric group $G = \text{Sym}(7)$ acts transitively on V , and it is clear that G is generously transitive. Let x be a fixed triple, and we will consider the orbits of G_x on V . There are four such orbits: x itself, the set of things which intersect x in 2 points, 1 point, and are disjoint. The first is the diagonal orbital and the remaining three correspond to the (undirected!) graphs $J(7, 3, 2)$, $J(7, 3, 1)$, and $J(7, 3, 0)$, respectively. Clearly G is a subgroup of the automorphism groups of these three graphs. Interestingly, G is the automorphism group of $J(7, 3, 2)$ and $J(7, 2, 0)$, but is a proper subgroup of $J(7, 3, 1)$.

Lemma. *The automorphism group of $J(7, 3, 1)$ contains a group isomorphic to $\text{Sym}(8)$ (and therefore $\text{Sym}(7)$, properly).*

Proof. There are 35 partitions of the set $\{0, 1, \dots, 7\}$ into two sets of size 4 ($35 = \frac{1}{2} \binom{8}{4}$). Let X be the graph with vertices corresponding to these partitions with an edge if and only if the intersection from one piece of the first with one piece of the second has size 2 (i.e. there would be an edge between $(1, 2, 3, 4), (5, 6, 7, 8)$ and $(1, 2, 5, 6), (3, 4, 7, 8)$). It is obvious that $\text{Aut}(X)$ contains a subgroup isomorphic to $\text{Sym}(8)$, as swapping the elements in the underlying set preserves adjacency and non-adjacency. We can also see that X is isomorphic to $J(7, 3, 1)$ because a partition of a set of 8 elements into two sets of size 4 is determined by identifying which 4-set contains zero and specifying the three other elements in that 4-set. Hence such a partition can be uniquely matched with a triple from a set of size 7, and two partitions are adjacent in X if and only if the triples share one element in common. As X is isomorphic to $J(7, 3, 1)$ and $\text{Aut}(X)$ contains $\text{Sym}(8)$ as a subgroup, $J(7, 3, 1)$ does as well, and we are done. \square

Primitivity

Definition. Let G be a transitive group acting on a set V . A nonempty subset $S \subset V$ is called a **block of imprimitivity** for G if for any element $g \in G$, either $S^g = S$ or $S \cap S^g = \emptyset$. As G is transitive, the translates of S form a partition of V . This set of translates is called a **system of imprimitivity** for G .

Example. One example of a system of imprimitivity is the cube graph on 8 vertices Q . We can see that $\text{Aut}(Q)$ acts transitively on Q (pick any two vertices to swap and reflect over the axis of symmetry between them). For each vertex x there is a unique vertex x' at distance 3 from x , and all other vertices are at distance 1 or 2. If we take $S = \{x, x'\}$ and let $g \in \text{Aut}(Q)$ be any group element, then either $S^g = S$ or $S \cap S^g = \emptyset$, as automorphisms preserve distances, so these vertices must either be swapped or fixed, or $x \mapsto y$ and $x' \mapsto y'$, and since $x \neq y$, it must be that $x' \neq y'$, because the vertex at distance 3 is unique.

There are four disjoint sets of the form S^g (each of the 8 vertices has a unique match), so as g ranges over all of $\text{Aut}(Q)$, these sets are permuted.

The partition of V into singletons is also a system of imprimitivity, as is the partition of V into a single component. These are said to be the *trivial* systems of imprimitivity.

Definition. A group with no nontrivial systems of imprimitivity is **primitive**. Otherwise, if there is a nontrivial system of imprimitivity, we call the group **imprimitive**.

There are two characterizations of primitive permutation groups. Here is the first:

Lemma. Let G be a transitive permutation group acting on a set V and let x be an element of V . Then G is primitive if and only if G_x is a maximal subgroup of G . That is, G_x is a subgroup of G and there is no nontrivial subgroup of G containing G_x .

Proof. We will prove this by contraposition, showing that G has a nontrivial system of imprimitivity if and only if G_x is not a maximal subgroup. For convenience of notation, we'll write $H \leq G$ if H is a subgroup of G and $H < G$ if H is a *proper* subgroup of G .

First, suppose that G has a nontrivial system of imprimitivity and let B be the block of imprimitivity containing our point x . We'll show that $G_x < G_B < G$, and thus that G_x is not maximal. If $g \in G_x$, then $B \cap B^g$ is not empty, as it surely contains x , so by definition, $B = B^g$, so $G_x \leq G_B$. To show the inclusion is proper, we need to find an element of G_B not in G_x . Let $y \neq x$ be some other element of B . Since G is transitive, there is a group element $h \in G$ such that $y = x^h$, but then $B = B^h$, but $h \notin G_x$, so $G_x < G_B$.

For the other direction, suppose that H is a subgroup of G such that $G_x < H < G$ (G_x is not maximal). We will show that the orbits of H form a nontrivial system of imprimitivity. Let B be the orbit of H containing x and let $g \in G$. We need to show that B and B^g are either equal or disjoint. Suppose that $y \in B \cap B^g$. Since $y \in B$, there is an element $h \in H$ such that $y = x^h$, and since $y \in B^g$, there is an $h' \in H$ such that $y = x^{h'g}$. But then $x = x^{h'gh^{-1}}$ so $h'gh^{-1} \in G_x < H$. Thus $g \in H$, and because B is an orbit of H , we have that $B = B^g$. Since $G_x < H$, B contains something that is not x , and since $H < G$, it cannot be all of V , so it is a nontrivial block of imprimitivity.

□

Primitivity and Connectivity

The second characterization of primitivity will require us to build a little machinery for dealing with directed graphs. We will then look at the orbits of G on $V \times V$.

Definition. A **path** in a directed graph is a sequence of vertices such that there is an arc from each vertex in the sequence to the next. A **weak path** is a sequence of vertices such that there is an arc either from a vertex to the next *or* from a vertex to the previous.

Definition. A directed graph is **strongly connected** if any pair of vertices can be joined by a path, and **weakly connected** if any pair of vertices can be joined by a weak path.

It is clear that a directed graph is weakly connected if and only if the underlying undirected graph is connected.

Definition. A **strong component** is a maximal induced subgraph (with respect to inclusion) which is strongly connected. Since each vertex alone is a strong component, it follows that the strong components of a directed graph form a partition of the vertices.

Definition. The **in-valency** and **out-valency** of a vertex in a directed graph are the number of arcs into and out of the vertex, respectively.

Lemma. *Let D be a directed graph such that every vertex in D has in-valency equal to its out-valency. Then D is strongly connected if and only if it is weakly connected.*

Proof. Strong connectivity obviously implies weak connectivity, so we focus on proving the other direction. Suppose, for the sake of contradiction, that D is weakly connected but not strongly connected, and let D_1, D_2, \dots, D_r be the strong components of D . If there is an arc starting in D_1 and ending in D_2 , then there cannot be one from D_2 to D_1 , so all such arcs between these components must be from D_1 into D_2 . In this way, we can construct a directed graph D' whose r vertices are D_1, D_2, \dots, D_r where there is an arc from one vertex to another if and only if there is an arc from the component of D corresponding to the first into that of the second. This directed graph is connected and must be acyclic, otherwise the components corresponding to the vertices in a cycle would be a strong component, contradicting the maximality of the D_i . Then there must be a component (let's say D_1 , without loss of generality) such that any arc ending in that component must start at another vertex in that component, as we have a directed acyclic graph D' which must have at least one vertex with in-valency zero. Thus the total out-valency of the vertices of D_1 must be less than the total in-valencies, which is a contradiction. \square

Who cares, right? Let G be a group acting transitively on V and let Ω be an orbit of G on $V \times V$ which is not symmetric. Then Ω corresponds to an oriented graph, and G acts transitively on its vertices. Thus, every vertex in Ω has the same in-valency and out-valency, and since the sum of the total in-valencies must equal the sum of the total out-valencies, the in- and out-valencies of any vertex are equal to each other. Then by the previous lemma, Ω is weakly connected if and only if it is strongly connected, so there is no need to differentiate between weakly and strongly connected orbits. We just call them *connected orbits*.

Lemma. *Let G be a transitive permutation group acting on V . Then G is primitive if and only if each nondiagonal orbit is connected.*

Proof. Suppose that G is imprimitive and that B_1, B_2, \dots, B_r is a system of imprimitivity. Let x, y be distinct points in B_1 . and let Ω be the orbit containing (x, y) . If $g \in G$, then x^g and y^g have to be in the same block (else B^g contains points from two distinct blocks, contradicting that it is a

block of imprimitivity). Thus each arc in the graph of Ω joins vertices corresponding to points in the same block, so Ω is not connected.

Conversely, let Ω be a nondiagonal orbit which is not connected, and let B be the point set of some component. If $g \in G$, then B and B^g must be equal or disjoint, so B is a nontrivial block of imprimitivity, and thus G is imprimitive.

□

Chapter 3 : Transitive Graphs

Now we can really start bringing together groups and graphs. We'll study graphs whose automorphism group acts transitively on the vertices. That is, for any pair of vertices x and y , there is some group element which sends x to y . Such graphs are necessarily regular, and one challenge is finding properties of vertex transitive graphs which do not hold for all regular graphs. We'll see that, in general, transitive graphs are more strongly connected than regular graphs. Cayley graphs are an important class of vertex transitive graphs, and we'll see a bit of them in this chapter.

Vertex-Transitive Graphs

Definition. A graph X is **vertex-transitive** (or just **transitive**) if its automorphism group acts transitively on its vertex set $V(X)$.

One family of transitive graphs are the k -cubes Q_k . We can think about these combinatorially by thinking of each vertex as one of the 2^k binary strings (or tuples) and two vertices are adjacent if and only if their corresponding strings differ in exactly one position. The cube Q_3 is usually just called 'the cube', and we have seen this object already, when looking at systems of imprimitivity.

Lemma. *The k -cube, Q_k , is vertex transitive.*

Proof. If v is a fixed binary tuple, then the mapping $\rho_v : x \mapsto x + v$ where we do binary addition placewise permutes the vertices of Q_k . This is an automorphism because the tuples x and y differ in exactly one position if and only if $x + v$ and $y + v$ differ in exactly one position (we flip the same bits in each). This group H acts transitively on the vertices because for any two vertices x and y , we can send x to y with ρ_{y-x} . There are 2^k such permutations.

Note that H is *not* the full automorphism group. Any permutation of the k coordinate positions is also an automorphism of Q_k , and there are $k!$ of these, and they form a subgroup K isomorphic to $Sym(k)$. By standard results in group theory, the group HK is a subgroup of $Aut(Q_k)$ and the size of HK is

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

It is clear that the intersection of these groups is the identity permutation, so we have that $|Aut(Q_k)|$ is at least $2^k k!$. \square

Another family of vertex transitive graphs are the circulants, as any vertex can be sent to any other by using the appropriate element of the cyclic subgroup of its automorphism group. Both the cubes and the circulants are part of a construction which produces many (not all) vertex-transitive graphs.

Definition. Let G be a group and C a subset of G which is closed under taking inverses and does not contain the identity. Then the **Cayley graph** $X(G, C)$ is the graph with vertex set G and edge set $E(X(G, C)) = \{(g, h) | hg^{-1} \in C\}$. That is, there is an edge between group elements g and h if there is an element a of C such that $h = ag$. If C is an arbitrary subset of G , then we can create a directed graph in this way, but if C is inverse-closed, then this directed graph has arcs in both directions and reduces to the previous construction.

Many results for Cayley graphs hold for this general directed case, but we will be explicit when we are using this construction rather than the canonical one.

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

Proof. For each $g \in G$, the mapping $\rho_g : x \mapsto xg$ is a permutation of the elements of G , and it is an automorphism of $X(G, C)$, as

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

so xg is adjacent to yg if and only if x is adjacent to y . The permutations ρ_g are a subgroup of the automorphism group of $X(G, C)$ which acts transitively because for any vertices g and h , $\rho_{g^{-1}h}$ sends g to h . □

The k -cube is a Cayley graph for the group $(\mathbb{Z}_2)^k$ and the circulant on n vertices is a Cayley graph for \mathbb{Z}_n . Most small vertex-transitive families of graphs are Cayley graphs, but there are many such families which are not Cayley graphs. In particular, the graphs $J(v, k, i)$ are vertex transitive because we can pick an element of $\text{Sym}(v)$ to map any k -set to any other, but they are not Cayley graphs in general. We can prove this for one counterexample and move on from there:

Lemma. *The Petersen graph is not a Cayley graph.*

Proof. The Petersen graph has 10 vertices and is 3-regular. There are two groups with 10 elements: \mathbb{Z}_{10} and D_{10} , the dihedral group with 10 elements. If we pick $|C| = 3$ for either of these, we get a graph which contains cycles of order 4, but the Petersen graph only contains cycles of order 5, so there is no isomorphism. □

Edge-Transitive Graphs

Definition. A graph X is **edge-transitive** if its automorphism group acts transitively on its edge set $E(X)$. That is, for any pair of edges (u, v) and (x, y) , there is a group element which sends (u, v) to (x, y) , i.e. it sends u to x and v to y or the other way around. An edge-transitive graph is vertex transitive.

It's clear that the graphs $J(v, k, i)$ are edge-transitive, but the circulants are, in general, not.

Definition. Recall that an *arc* is an ordered pair of adjacent vertices. A graph X is **arc transitive** if $\text{Aut}(X)$ acts transitively on the arcs. That is, for any pair of arcs (u, v) and (x, y) , there is a group element which sends (u, v) to (x, y) , i.e. it sends u to x and v to y but *not* the other way around. It is often useful to view an undirected graph as a directed graph with arcs in both directions. As such, an arc-transitive graph is necessarily edge-transitive (and vertex-transitive).

The complete bipartite graphs $K_{m,n}$ are edge-, but not vertex-transitive (unless $m = n$) because there is no automorphism which maps a vertex with valency m to one with valency n (or vice versa).

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

Proof. Suppose that X is edge- but not vertex-transitive and that (x, y) is an edge of X where x and y are vertices such that there exists no automorphism mapping x to y . If w is a vertex of X , then w lies on some edge and there is an element of $\text{Aut}(X)$ which maps this edge incident to w to the one between x and y , so any vertex either lies in the orbit of x or the orbit of y . These orbits are disjoint, as we know that x and y are in different orbits. Thus there are exactly two orbits of $\text{Aut}(X)$. An edge which connects two vertices in one orbit cannot be mapped by an automorphism to an edge which is incident to a vertex in the other orbit, so no such edge can exist. Therefore,

all edges in X are incident to one vertex from the orbit of x and one from the orbit of y , so X is bipartite. □

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

Proof. Let $G = \text{Aut}(X)$ and suppose that x and y are adjacent vertices in X . Let Ω be the orbit of G on $V \times V$ which contains (x, y) . Since X is edge-transitive, there is an automorphism which maps any arc in X to either (x, y) or (y, x) . But since X is not arc-transitive, we can choose x and y such that (y, x) is not in Ω , so Ω is not symmetric. Thus, X is the graph with edges $\Omega \cup \Omega^T$. Because the out-valency of x is the same in Ω and Ω^T , the valency of X must be even. □

Corollary. *A vertex- and edge-transitive graph of odd valency must be arc-transitive as well.*

Edge Connectivity

Definition. An **edge cutset** in a graph X is a collection of edges such that deleting these edges from X separates X into a strictly greater number of connected components. For a connected graph, the **edge connectivity** is the minimum number of edges in any cutset. That is, the size of the smallest set of edges which, if deleted, disconnects X . We will denote this quantity $\kappa_1(X)$. If a single edge e is a cutset, then we call e a **bridge** or **cut-edge**.

The edge connectivity of a graph clearly cannot be greater than its minimum valency, so the edge connectivity of a vertex-transitive graph is at most its valency. We're about to prove that the edge connectivity of a vertex-transitive graph is exactly equal to its valency. If $A \subset V(X)$, we'll denote ∂A to be the set of vertices with one end in A and one end not in A . If $A = \emptyset$ or $A = V(X)$, then $\partial A = \emptyset$. The edge connectivity of X is the minimum size of ∂A as A ranges over all possible proper subsets of $V(X)$.

Lemma. *Let X be a graph and A and B be subsets of $V(X)$. Then $|\partial(A \cup B)| + |\partial(A \cap B)| \leq |\partial A| + |\partial B|$.*

Proof. The right-hand side counts the number of edges leaving A or B . The left-hand side counts the number of edges leaving A or B except those between A and B plus the edges leaving those vertices in both A and B . Thus the difference between the right- and left-hand sides is twice the number of edges crossing the symmetric difference of A and B . Since this is at least zero, the inequality holds. □

Definition. An **edge atom** of a graph X is a subset $S \subset V(X)$ such that $|\partial S| = \kappa_1(X)$ and, given that this holds, $|S|$ is minimal. Since $\partial S = \partial(V \setminus S)$, if S is an edge atom, then $2|S| \leq |V(X)|$.

Corollary. *Any two distinct edge atoms are vertex disjoint.*

Proof. Assume $\kappa = \kappa_1(X)$ and let A and B be distinct edge atoms in X . If $A \cup B = V(X)$, then since neither A nor B can contain more than half of the vertices, it must be that $|A| = |B| = \frac{1}{2}|V(X)|$, so $A \cap B = \emptyset$. Thus $A \cup B \subsetneq V(X)$. The previous lemma tells us that $|\partial(A \cup B)| + |\partial(A \cap B)| \leq 2\kappa$. But since $A \cup B \neq V(X)$ and $A \cap B \neq \emptyset$, we have that $|\partial(A \cup B)| = |\partial(A \cap B)| = \kappa$. Since $A \cap B$ is a nonempty proper subset of A , this cannot happen, as A is an edge atom. Thus A and B must be disjoint. □

Lemma. *If X is a connected vertex-transitive graph, then its edge connectivity is equal to its valency.*

Proof. Suppose that X is vertex-transitive and has valency k . Let A be an edge atom of X . If A is a single vertex, then $|\partial A| = k$ and we are done. Otherwise, suppose that $|A| \geq 2$. If g is an automorphism of X and $B = A^g$ (the image of the vertices in A under g), then $|B| = |A|$ and $|\partial B| = |\partial A|$. From the previous lemma, we have that A is either equal to or disjoint from B . Thus A is a block of imprimitivity for $\text{Aut}(X)$, and by Exercise 2.13, it follows that the subgraph of X induced by A is regular, so let its valency be ℓ .

Each vertex in A has $k - \ell$ neighbors not in A , so $|\partial A| = |A|(k - \ell)$. Since X is connected, $\ell < k$, so if $|A| \geq k$, then $|\partial A| \geq k$. So we assume $|A| < k$. Since $\ell \leq |A| - 1$, it follows that $|\partial A| \geq |A|(k + 1 - |A|)$. The minimum value of the right-hand side occurs when $|A| = 1$ or $|A| = k$. Thus $|\partial A| \geq k$ for all cases. \square

Vertex Connectivity

Definition. A **vertex cutset** in a graph is a set of vertices whose deletion increases the number of connected components of X . The **vertex connectivity** is the size of the smallest vertex cutset, which we denote $\kappa_0(X)$. For any $k \leq \kappa_0(X)$, we say that X is **k -connected**.

Complete graphs have no vertex cutsets, but it is conventional to let $\kappa_0(K_n) = n - 1$. The central result in this topic is Menger's theorem, which we are about to prove.

Definition. If u and v are distinct vertices of X , then two paths P and Q are **openly disjoint** if, aside from u and v , the vertex sets of P and Q are disjoint.

Theorem (Menger). *Let u and v be distinct vertices in X . Then the maximum number of openly disjoint paths from u to v is equal to the minimum size of a set of vertices $S \subset V(X)$ such that u and v lie in distinct connected components of $X \setminus S$. That is, the maximum number of such paths is equal to the smallest vertex cutset which separates u from v .*

Proof. If we have a collection of m openly disjoint u - v paths, then we must remove at least one vertex from each path in order to disconnect u from v . \square

This theorem tells us that two vertices that can't be separated by fewer than m vertices must be joined by m openly disjoint paths. A basic corollary is that two vertices which cannot be separated by a single vertex must lie on a cycle. We'll make use of the corollary that a pair of vertices that cannot be separated by a set of size two must be joined by three openly disjoint paths. There are lots of variations of Menger's theorem. In particular, two subsets A and B of $V(X)$ cannot be separated by fewer than m vertices if and only if there are m disjoint paths which start in A and end in B .

We are about to prove a lower bound on the vertex connectivity of a vertex-transitive graph.

If A is a set of vertices in X , let $N(A)$ denote the vertices in $V(X) \setminus A$ with a neighbor in A and let \overline{A} be the complement of $A \cup N(A)$ in $V(X)$. That is, \overline{A} is a collection of vertices, $N(A)$ (the 'neighborhood of A ') is the collection of vertices just outside of A , and \overline{A} is everything else.

Definition. A **fragment** of X is a subset A such that \overline{A} is nonempty and $|N(A)| = \kappa_0(X)$. We have \overline{A} empty when every vertex in $V(X)$ is either in A or adjacent to a vertex in A , and $|N(A)| = \kappa_0(X)$ when $N(A)$ is a minimum vertex cutset.

An *atom* of X is a fragment which contains the minimum possible number of vertices. An atom must be connected and if X is k -regular with an atom consisting of a single vertex, then $\kappa_0(X) = k$.

We can also see that if A is a fragment, then $N(A) = N(\overline{A})$ and $\overline{\overline{A}} = A$. The following lemma gives us some useful properties of fragments.

Lemma. *Let A and B be fragments in X . Then:*

- a) $N(A \cap B) \subset (A \cap N(B)) \cup (N(A) \cap B) \cup (N(A) \cap N(B))$
- b) $N(A \cup B) = (\overline{A} \cap N(B)) \cup (N(A) \cap \overline{B}) \cup (N(A) \cap N(B))$
- c) $\overline{A} \cup \overline{B} \subset \overline{A \cap B}$
- d) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Proof. Suppose first that $x \in N(A \cap B)$. Since $A \cap B$ and $N(A \cap B)$ are disjoint, if $x \in A$ then $x \notin B$, so $x \in N(A)$ (or vice versa). If x isn't in either A or B , then it is in $N(A) \cap N(B)$, and we have proved (a).

Similarly, we can show $N(A \cup B) \subset (\overline{A} \cap N(B)) \cup (N(A) \cap \overline{B}) \cup (N(A) \cap N(B))$. To show inclusion in the other direction (and therefore equality), note that if $x \in \overline{A} \cap N(B)$, then x is in neither A nor B . Since $x \in N(B)$ and $x \notin A$, $x \in N(A \cup B)$. Similarly, if $x \in N(A) \cap \overline{B}$ or $x \in N(A) \cap N(B)$, then $x \in N(A \cup B)$, and we have proved (b).

Next, if $x \in \overline{A}$, then x is not in A or $N(A)$, so it can't be in $A \cap B$ or $N(A \cap B)$, so $x \in \overline{A \cap B}$, which proves (c).

Finally, if $x \in \overline{A \cup B}$, then x is not in $A \cup B$ or $N(A \cup B)$. Thus x is not in A or B nor $N(A)$ or $N(B)$, thus it is in both \overline{A} and \overline{B} , and we have proved (d). □

Theorem. *Let X be a graph on n vertices with connectivity k . Suppose A and B are fragments of X and $A \cap B$ is nonempty. If $|A| \leq |\overline{B}|$, then $A \cap B$ is a fragment.*

Proof. Since A , $N(A)$, and \overline{A} (symmetrically for B) partition the set $V(X)$ into three disjoint parts, the pairwise intersections of one chunk from A with a chunk from B gives us a partition into nine disjoint parts. As some shorthand, we'll denote

$$a = |A \cap N(B)|, b = |N(A) \cap B|, c = |N(A) \cap N(B)|, d = |N(A) \cap \overline{B}|, e = |\overline{A} \cap N(B)|$$

. We proceed in steps.

a) $|A \cup B| < n - k$

Since $|F| + |\overline{F}| = n - k$ for any fragment F , $|A| \leq |\overline{B}| = n - k - |B|$, as A and B are fragments. Thus $|A| + |B| \leq n - k$, and since A and B share at least one element in common, the inequality is strict.

b) $|N(A \cup B)| \leq k$

From the previous lemma, $|N(A \cap B)| \leq a + b + c$ and $|N(A \cup B)| = c + d + e$. Thus, $2k = |N(A)| + |N(B)| = a + b + 2c + d + e \geq |N(A \cap B)| + |N(A \cup B)|$. Since $|N(A \cap B)| \geq k$, it must be that $|N(A \cup B)| \leq k$.

c) $\overline{A} \cap \overline{B} \neq \emptyset$.

From (a) and (b), we have that $|A \cup B| + |N(A \cup B)| < n$, so $\overline{A \cup B} \neq \emptyset$, and the claim follows from part (d) of the previous lemma.

d) $|N(A \cup B)| = k$

For any fragment F , $N(F) = N(\overline{F})$. By part (a) of the previous lemma, and step (b) above, we get

$$\begin{aligned} N(\overline{A} \cap \overline{B}) &\subset (\overline{A} \cap N(\overline{B})) \cup (\overline{B} \cap N(\overline{A})) \cup (N(\overline{A}) \cap N(\overline{B})) \\ &= (\overline{A} \cap N(B)) \cup (\overline{B} \cap N(A)) \cup (N(A) \cap N(B)) \\ &= N(A \cup B) \end{aligned}$$

Since $\overline{A} \cap \overline{B}$ is nonempty, $|N(\overline{A} \cap \overline{B})| \geq k$, so $|N(A \cup B)| \geq k$. Combining this with step (b), the claim follows.

e) $A \cap B$ is a fragment.

From step (b), we have that $|N(A \cap B)| + |N(A \cup B)| \leq 2k$, and (d) tells us that $|N(A \cap B)| \leq k$, so $N(A \cap B)$ is of size k , and we are done. □

Corollary. *If A is an atom and B a fragment of X , then A is entirely contained in one of B , $N(B)$, or \overline{B} .*

Proof. Since A is an atom, $|A| \leq |B|$ and $|A| \leq |\overline{B}|$. Thus the intersection of A with B or \overline{B} is a fragment (if nonempty). Since A is an atom, no proper subset can be a fragment. □

Now we are ready to prove the theorem mysteriously referenced earlier.

Theorem. *A vertex-transitive graph with valency k has vertex connectivity at least $\frac{2}{3}(k+1)$.*

Proof. Let X be a vertex-transitive graph with valency k , and let A be an atom in X . If A is a single vertex, then $|N(A)| = k$ and we are done. Suppose $|A| \geq 2$. If $g \in \text{Aut}(X)$, then A^g is an atom as well, so by the previous corollary, either $A = A^g$ or A and A^g are disjoint. Then A is a block of imprimitivity for $\text{Aut}(X)$, and its translates partition $V(X)$. Then again by the corollary, we have that $N(A)$ is also partitioned by the translates of A , so $|N(A)| = t|A|$ for some positive integer t .

Let u be a vertex in A . Then the valency of u is at most $|A| - 1 + |N(A)| = (t+1)|A| - 1$. Thus it follows that $k+1 \leq (t+1)|A|$ and $\kappa_0(X) \geq \frac{t}{t+1}k$. To complete the proof, we only need to show $t \geq 2$.

Suppose for the sake of contradiction that $t = 1$. By the corollary above, $N(A)$ is a union of atoms, so $N(A)$ is also an atom. Since $\text{Aut}(X)$ acts transitively on the atoms of X , it follows that $|N(N(A))| = |A|$, so since $A \cap N(N(A))$ is nonempty, $A = N(N(A))$. This implies $\overline{A} = \emptyset$, contradicting the assumption that A is a fragment. □

Matchings

Definition. A **matching** M in a graph X is a set of edges such that no two edges are incident to the same vertex. Equivalently, a matching is a subset of the vertices of X such that M can be partitioned into disjoint sets of size 2 such that there is an edge in X connecting each pair. A matching M is called **perfect** or a **1-factor** if every vertex in X belongs to M . A **maximum matching** is a matching M such that no other edges can be added to M without violating the definition of a matching.

Our treatment of matchings will largely be from the perspective of edge sets rather than vertex sets. That is, when we talk about a matching M , we formally mean that M is the set of edges in the matching, but we will be sloppy and talk about a vertex being ‘in’ the matching when what we really mean is that the vertex is incident to some edge in M .

Obviously any graph which has a perfect matching has an even number of vertices. We can also induce a partial ordering on matchings by inclusions. A maximum matching is therefore an element of this poset which has nothing sitting above it.

The following result tells us that a connected vertex-transitive graph on an even number of vertices *must* have a perfect matching, and that such a graph on an odd number of vertices has a maximum matching which misses exactly one vertex. To prove this, we first need two lemmas and a few definitions. Throughout, we will assume X is connected and vertex-transitive.

Definition. If M is a matching, in X and P is a path in X such that every second edge of P is in M , then we call P an **alternating path** with respect to M . Similarly, an *alternating cycle* is a cycle with every second edge in M .

Suppose that M and N are matchings in X , and consider their symmetric difference $(M \cup N) \setminus (M \cap N)$, which we will write $M \oplus N$, for ease of notation. Since M and N are regular subgraphs with valency 1, $M \oplus N$ is a subgraph with valency at most 2. Thus each component of it must either be a path or a cycle. Since no vertex of $M \oplus N$ has two incident edges in either M or N , these paths or cycles are alternating with respect to both M and N , and each cycle must have even length. Suppose P is a path in $M \oplus N$ with odd length. Without loss of generality, suppose that P contains more edges from M than N , so $N \oplus P$ is also a matching which contains more edges than N . Thus P must contain an equal number of edges from M and N , so its length is even.

Lemma. *Let u and v be vertices in X such that no maximum matching misses both of them. Suppose then that M_u is a maximum matching which misses u but not v and M_v a maximum matching which misses v but not u . Then there is a path of even length in $M_u \oplus M_v$ with u and v as its endpoints.*

Proof. Since M_u and M_v miss u and v , respectively, their valencies in $M_u \oplus M_v$ must be 1, so both are end vertices of some path. We need to show that they are in the same connected component of $M_u \oplus M_v$. As M_u and M_v have maximum size, all paths (including those with endpoints u and v) have even length. Suppose, for the sake of contradiction, that u and v lie on distinct paths. Let P be the path on u . Then P is alternating with respect to M_v , has even length, and $M_v \oplus P$ is a matching in X which misses u and v and has the same size as M_v , which contradicts how we chose u and v . \square

We have to prove one more lemma before our theorem.

Definition. We call a vertex u in X **critical** if it is in every maximum matching. If X is vertex transitive and one vertex is critical, then every vertex is critical, so X has a perfect matching.

Lemma. Let u and v be distinct vertices in X , and let P be a path from u to v . If no vertex of $V(P) \setminus \{u, v\}$ is critical, then no maximum matching misses both u and v .

Proof. We proceed by induction on the length of P . If u and v are adjacent, then no maximum matching can miss both u and v , as we can always add the edge (u, v) to some matching which misses both to increase the size.

Suppose P has length at least 2, and let x be some vertex on P distinct from u and v . Then u and x are joined by a path which has no critical vertices, and this path is shorter than P , so by induction, no maximum matching misses both u and x and no maximum matching misses both v and x . Since x is not critical, there is a maximum matching M_x which misses x . Assume, for the sake of contradiction, that N is a maximum matching which misses both u and v . Then by the previous lemma, there is a path from u to x in $M_x \oplus N$ and similarly there is a path from x to v , so there is a u - v path, which implies that $u = v$, contradicting the assumption that they are distinct. □

We can now wrap this up into a proof of our big theorem:

Theorem. Let X be a connected vertex-transitive graph. Then X has a matching which misses at most one vertex, and for any edge there exists a maximum matching containing that edge.

Proof. We noted that a vertex-transitive graph which contains a critical vertex must contain a perfect matching, and by the previous lemma, if X is vertex-transitive and does not contain a critical vertex, then no two vertices are both missed by any maximum matching, so a maximum matching covers all but one vertex of the graph.

We now only need to show that any edge is contained in some maximum matching. We proceed inductively, supposing it holds for vertex-transitive graphs smaller than X (base cases of graphs on one, two, or three vertices are trivial). If X is edge-transitive, the claim is trivial, so we assume that X is not edge-transitive. Suppose, for the sake of contradiction, that e is an edge not in any maximum matching. Let Y be the subgraph of X induced by the edge set consisting of the orbit of e under $\text{Aut}(X)$. Since X is not edge-transitive, Y is a strict subgraph of X on the same vertex set. We will show that X has a matching containing an edge of Y which misses at most one vertex. Thus under some $g \in \text{Aut}(X)$, this matching maps to one containing e missing at most one vertex.

If Y is connected, then by induction each edge lies in a matching which misses at most one vertex, and we are done. Suppose then that Y is not connected. The components of Y form a system of imprimitivity for $\text{Aut}(X)$ and are pairwise isomorphic vertex-transitive graphs. If the number of vertices in each component is even, then by induction we can find a perfect matching on each component whose union is a perfect matching in Y . Assume then that there is some component of Y which has an odd number of vertices. Let Y_1, Y_2, \dots, Y_r be the components of Y . Consider the graph Z which has a vertex for each Y_i and an edge between Y_i and Y_j if and only if there is an edge in the original graph X joining some vertex of Y_i to Y_j . Then Z is vertex-transitive, so by induction contains a matching N which misses at most one vertex. Suppose $(Y_i, Y_j) \in N$ is an edge, and since Y_i is adjacent to Y_j in Z , there are vertices y_i, y_j in X which are adjacent. Since Y_i and Y_j are vertex-transitive and have an odd number of vertices, there is a matching in Y_i missing only y_i and similarly for y_j , but then we can include the edge (y_i, y_j) to get a matching in X which misses nothing in either component. If the number of components Y_i is even, this construction gets

us a perfect matching. Otherwise, we have a matching which is perfect on all but one component, and then a matching within that last component which misses exactly one vertex. This concludes the proof. \square

Hamiltonian Paths and Cycles

Definition. A **Hamilton path** in a graph X is a path which meets every vertex. A **Hamilton cycle** is a path which meets every vertex and starts and ends at the same vertex. A graph is called **hamiltonian** if it contains a Hamilton cycle. All known vertex-transitive graphs have Hamilton paths and only five are known which do not contain Hamilton cycles. Let's take a look at these.

Clearly K_2 is vertex transitive and has a Hamilton path but no Hamilton cycle (no nontrivial cycles at all!). More interestingly, the Petersen graph doesn't have a Hamilton cycle. The graph has enough symmetry that a case argument is tedious, rather than unmanageable, but we'll see an algebraic proof in a later chapter. The Coxeter graph, which is arc-transitive and on 28 vertices, is also not hamiltonian. the other two graphs are realized by replacing the vertices of the Petersen and Coxeter graphs with triangles.

Definition. The **subdivision graph** $S(X)$ of a graph X is obtained by placing a new vertex in the middle of each edge of X . That is, the vertex set of $S(X)$ is $V(X) \cup E(X)$, and two vertices v, e in $S(X)$ are adjacent if and only if v corresponds to a vertex in $V(X)$ and e to an edge in $E(X)$ such that e is incident to v . This graph is bipartite, with the vertices from $V(X)$ and $E(X)$ forming the bipartition. The vertices in the 'edge class' all have valency 2. If X is regular with valency k , then the vertices in the 'vertex class' are also all of valency k . In this case, $S(X)$ is semiregular bipartite.

Lemma. *Let X be a cubic graph. Then $L(S(X))$ has a Hamilton cycle if and only if X does.*

Proof. A Hamilton cycle in a line graph $L(X)$ corresponds to an ordered enumeration of the edges of X such that each edge in the enumeration is incident to a vertex in common with the preceding and succeeding edge, and the first and last edge in the enumeration is the same. Since $S(X)$ for a cubic graph is a semiregular bipartite graph, a Hamilton cycle in $L(S(X))$ uniquely corresponds to an ordering of the valency 2 vertices of $S(X)$ such that any two successive vertices in the ordering are at distance two from each other. But this induces an ordering of the vertices of valency 3, which corresponds to a sequence of vertices in X itself. It is clear that if there is a Hamilton cycle in $L(S(X))$, the induced ordering on the valency 3 vertices corresponds to a Hamilton cycle in X . But the same goes the other way. If we have a Hamilton cycle in X , this corresponds to an ordering of the valency 3 vertices such that successive vertices are at distance 2, which means we have to visit each vertex of valency 2 once, hence we use every edge (one to enter, one to leave). \square

If X is arc-transitive and cubic, then $L(S(X))$ is vertex-transitive. Thus we get the last two of the known vertex-transitive graphs which are not hamiltonian. Of these five graphs, only K_2 is a Cayley graph (for the group \mathbb{Z}_2 , of course), and it is conjectured that all other Cayley graphs are hamiltonian and, even more strongly, that all other vertex-transitive graphs are hamiltonian. This conjecture is essentially a totally open problem, but it is known to be false for directed graphs.

A natural question is to find a lower bound on the length of a longest cycle in a vertex-transitive graph X . The best known bound is $O(\sqrt{|V(X)|})$, which isn't great, but we'll derive it anyway.

Lemma. *Let G be a transitive permutation group acting on a set V , let S be a subset of V , and set c equal to the minimum value of $|S \cap S^g|$ as g ranges over G . Then $|S| \geq \sqrt{c|V|}$.*

Proof. We'll count pairs (g, x) where $g \in G$ and $x \in S \cap S^g$. For each $g \in G$, there are at least c such points in S , so there are at least $c|G|$ such pairs. On the other hand, the elements of G which maps x to y form a coset of G_x , so there are exactly $|S||G_x|$ elements $g^{-1} \in G$ such that $x^{g^{-1}} \in S$, (equivalently, $x \in S^g$). Thus $c|G| \leq |S|^2|G_x|$ and since G is transitive, $\frac{|G|}{|G_x|} = |V|$ by the Orbit-Stabilizer theorem. The claim follows from basic algebraic manipulation. \square

The next theorem depends on the fact that in a 3-connected graph, any two cycles of maximum length have at least three vertices in common, which follows from Menger's theorem.

Theorem. *A connected vertex-transitive graph on n vertices contains a cycle of length at least $\sqrt{3n}$.*

Proof. Let X be a graph and $G = \text{Aut}(X)$. First, a connected vertex transitive graph with valency at least 3 is 3-connected (the theorem is trivial for graphs with valency 2), so let C be a maximum-length cycle in X . Then, $|C \cap C^g| \geq 3$ for any automorphism of X (there are at least three vertices in common between any two maximum-length cycles), so the result follows from the bound in the previous lemma. \square

In fact, the Petersen graph has cycles which pass through nine of the ten vertices.

Cayley Graphs

An important class of objects in algebraic graph theory, we are now ready to develop some theory about Cayley graphs.

Definition. A permutation group G acting on a set V is **semiregular** if no nonidentity element of G fixes a point of V . From the Orbit-Stabilizer theorem, it follows that every orbit of a semiregular group has length $|G|$. A group G is **regular** if it is semiregular and transitive. If G is regular on V , then $|G| = |V|$.

Any group G acts regularly on itself. Recall that ρ_g for $g \in G$ is the permutation of the elements of G such that $x \mapsto xg$. The mapping $g \mapsto \rho_g$ is called the *right regular representation* of G . This group is isomorphic to G , hence G acts transitively (and regularly) on it.

Lemma. *Let G be a group and C an inverse-closed subset of G which does not include e . Then $\text{Aut}(X(G, C))$ contains a regular subgroup isomorphic to G .*

Proof. This follows immediately from the proof of the earlier theorem that the Cayley graph $X(G, C)$ is vertex-transitive. \square

There is a converse of this lemma, which we will prove.

Lemma. *If a group G acts regularly on the vertices of the graph X , then X is a Cayley graph relative to some inverse-closed set $C \subset G \setminus \{e\}$.*

Proof. Fix a vertex u of X . If v is any vertex of X , there is a unique group element, say g_v , such that $u^{g_v} = v$, since G acts regularly on $V(X)$. Let $C = \{g_v \mid (u, v) \in E(X)\}$. If x and y are vertices of X , since $g_x \in \text{Aut}(X)$, x is adjacent to y if and only if $x^{g_x^{-1}}$ is adjacent to $y^{g_x^{-1}}$. But $x^{g_x^{-1}} = u$ and $y^{g_x^{-1}} = u^{g_y g_x^{-1}}$ so x and y are adjacent if and only if $g_y g_x^{-1} \in C$. But this looks like the construction of a Cayley graph. If we identify each vertex x with the group element g_x , then X is isomorphic to $X(G, C)$. Since X is undirected and has no self-loops, the set C must be an inverse-closed subset of $G \setminus \{e\}$. \square

One thing we've been sweeping under the rug is that there are many Cayley graphs for any given group. It's natural to ask under what conditions two Cayley graphs for the same group are isomorphic, and the next lemma gets towards an answer to this question. An *automorphism of a group* is a bijection $\theta : G \rightarrow G$ such that $\theta(gh) = \theta(g)\theta(h)$ for all $g, h \in G$. That is, an isomorphism from a group to itself.

Lemma. *If θ is an automorphism of the group G , then $X(G, C)$ and $X(G, \theta(C))$ are isomorphic as graphs.*

Proof. For any two vertices x and y in $X(G, C)$, it must be that $\theta(y)\theta(x)^{-1} = \theta(yx^{-1})$ (thinking of x and y as group elements). Thus $\theta(y)\theta(x)^{-1} \in \theta(C)$ if and only if $yx^{-1} \in C$. Thus θ preserves adjacency and non-adjacency between $X(G, C)$ and $X(G, \theta(C))$. □

The converse of this is not true; two Cayley graphs for a group can be isomorphic even if there is no automorphism relating their connection sets.

Definition. A **generating set** C of a group G is a subset such that any element of G can be written as the product of elements of C . Equivalently, the only subgroup of G which contains C is G itself.

Lemma. *The Cayley graph $X(G, C)$ is connected if and only if C is a generating set for G .*

Proof. It is clear that if C generates G , the Cayley graph is connected, as x and y are adjacent if and only if there is a $g \in C$ such that $xg = y$.

For the other direction, suppose that $X(G, C)$ is connected. Since two vertices are adjacent if and only if they belong to the subgroup generated by C , it follows that C generates G . □

Directed Cayley Graphs With No Hamiltonian Cycles

It turns out that it's pretty simple to find vertex-transitive directed graphs which are not hamiltonian, and the examples will even be directed Cayley graphs.

Theorem. *Suppose that distinct group elements α and β generate a finite group G , and that the graph X is the directed Cayley graph $X(G, \{\alpha, \beta\})$ with connection set $\{\alpha, \beta\}$. Furthermore, assume that, in their actions by left multiplication on G that α and β have k and ℓ cycles, respectively. If the element $\beta^{-1}\alpha$ has odd order and $V(X)$ has a partition into r disjoint directed cycles, then r , k , and ℓ all have the same parity.*

Proof. Suppose $V(X)$ has a partition into r directed cycles, and define the permutation π of G to be $x^\pi = y$ if the arc (x, y) is in one of the directed cycles, that is, π 'pushes' every vertex forward along its directed cycle. If we let $P = \{x \in V(X) | x^\pi = \alpha x\}$ and $Q = \{x \in V(X) | x^\pi = \beta x\}$, then P and Q partition $V(X)$, because α and β were chosen to be distinct.

Let τ be the permutation in G such that $x^\tau = \beta^{-1}x^\pi$. Clearly τ fixes every element of Q , and it maps elements of P to other elements of P , and for any $x \in P$, $x^\tau = \beta^{-1}\alpha x$, and since $\beta^{-1}\alpha$ has odd order, τ must as well. This is because odd permutations have even order, as an element of odd order is the square of some element in the cyclic group it generates, thus it is even.

It is a fact about symmetric groups that the parity of a permutation on n elements with r disjoint cycles is the parity of $r + n$. Since left multiplication by $\pi\beta^{-1}$ is an even permutation, $\ell + r$ is even. A symmetric argument for $\pi\alpha^{-1}$ tells us that $k + r$ is even. Thus ℓ, k, r all have the same parity.

□

The symmetric group on n elements can be generated by two permutations: (12) and $(123 \dots n)$. For example, $Sym(4)$ is generated by $\alpha = (12)$ and $\beta = (1234)$. The Cayley graph $X = X(Sym(4), \{(12), (1234)\})$ is shown below (maybe later). Now, $\beta^{-1}\alpha = (143)$, which has odd order (order 3), and since $|Sym(4)| = 24$, α and β have 12 and 6 cycles in $Sym(4)$, respectively, under the action of left multiplication. Thus $V(X)$ can be partitioned into an even number of directed cycles, so, in particular, does not have a directed Hamilton cycle.

This can generalize to an infinite family of directed Cayley graphs $X(n) = X(Sym(n), \{(12), (123 \dots n)\})$.

Corollary. *If $n \geq 4$ is even, then the directed Cayley graph $X(n)$ is not hamiltonian.*

Proof. Performing the same construction above shows us that α has $\frac{n!}{2}$ cycles in its action by left multiplication and $(123 \dots n)$ has $(n-1)!$, but $(123 \dots n)^{-1}(12)$ has order $n-1$, so since we can only partition $V(X)$ into an even number of directed cycles, we are done. □

We know that $X(3)$ and $X(5)$ are hamiltonian, but we don't know about odd $n \geq 7$.

Retracts

Recall that a *retract* is a subgraph Y of X such that there exists a homomorphism f from X to Y such that the restriction $f|_Y$ of f to Y is the identity map on the vertices in Y . It's even enough to only require that $f|_Y$ is a bijection, i.e. an automorphism of Y . We're about to prove that every vertex-transitive graph is the retract of some Cayley graph. If G is our group acting transitively on $V(X)$ and x and y vertices of X , then by a lemma in Chapter 2, the set of group elements in G which map x to y is a right coset of G_x . Thus there is a bijection from $V(X)$ to the right cosets of G_x . The action of G on $V(X)$ coincides with the action of right multiplication on the cosets of G_x .

Theorem. *Any connected vertex-transitive graph is a retract of some Cayley graph.*

Proof. Let X be a connected vertex-transitive graph and let $x \in V(X)$. Define the set $C = \{g \in G \mid (x, x^g) \in E(X)\}$, the set of group elements which send x to one of its neighbors. We have that C is the union of right cosets of G_x , and since x is not adjacent to itself, $C \cap G_x$ is empty. Furthermore, since x^a is adjacent to x^b if and only if x is adjacent to $x^{ba^{-1}}$, this is true if and only if $ba^{-1} \in C$.

If $g \in C$ and $h, h' \in G_x$, then $x = x^h$, x^h is adjacent to x^{gh} , and $x^{gh} = x^{h'gh}$, so $h'gh \in C$. Thus $G_x C G_x \subset C$, and since $e \in G_x$, $C \subset G_x C G_x$, so $C = G_x C G_x$.

Let H be the subgroup of $Aut(X)$ generated by C . By induction on the diameter of X , we can see that H acts transitively on the vertices of X . Now let Y be the Cayley graph $X(H, C)$. The right cosets of H_x partition $V(Y)$, so we can express any group element of H as ga for some $g \in H_x$. If g and h are both in H_x , then ga and hb are adjacent if and only if $hb(ga)^{-1} = hba^{-1}g^{-1} \in C$, which happens if and only if $ba^{-1} \in C$. Thus any two distinct right cosets have no edges between them or are completely connected, and since $e \notin C$, the subgraph of Y induced by each right coset is empty.

Therefore, the subgraph of Y induced by any complete set of coset representatives of H_x is isomorphic to X . The map sending the vertices of Y in some right coset of H_x to the corresponding right coset, viewed as a vertex of X , is a homomorphism from Y to X , and its restriction to a complete set of coset representatives is a bijection, thus X is a retraction of the Cayley graph Y . □

Some dissection of the proof tells us that, given X , we can get the Cayley graph Y by replacing each vertex of X with an independent set of size $|G_x|$. The graph induced by a pair of these independent sets is empty when the vertices in X are not adjacent, or is a complete bipartite subgraph if they are adjacent. Then

$$\frac{|V(X)|}{\alpha(X)} = \frac{|V(Y)|}{\alpha(Y)}$$

where $\alpha(\cdot)$ is the size of the largest independent set in the respective graph. This will come back later.

Transpositions

We will look at some special Cayley graphs for the symmetric groups. A set of transpositions (2-cycles) from $Sym(n)$ can be thought of as the edge set of a graph on n vertices with (ij) as a transposition corresponding to the edge (i, j) . It is (also) a fact about symmetric groups that they are generated by the complete set of 2-cycles.

Definition. Call a generating set C for a group **minimal** G if for any $g \in C$, $C \setminus \{g\}$ is not a generating set.

Lemma. *Let \mathcal{T} be a set of transpositions in $Sym(n)$. Then \mathcal{T} is a generating set for $Sym(n)$ if and only if its graph is connected.*

Proof. Let T be the graph of \mathcal{T} . The vertex set of this graph is $\{1, 2, 3, \dots, n\}$. Let G be the group generated by \mathcal{T} . If $(1i)$ and (ij) are elements of \mathcal{T} , then $(1j)$ is in G , as $(1j) = (ij)(1i)(ij)$. By induction, if there is a path from 1 to i in T , then $(1i) \in G$. Thus if k and ℓ are in the same connected component, then $(k\ell) \in G$, by the same argument using k instead of 1. Thus the transpositions belonging to some connected component generate the symmetric group on the vertices of that component. Since no transposition can map between elements in different connected components, the entire graph must be connected if and only if our set of transpositions generate all of $Sym(n)$. \square

Lemma. *Let \mathcal{T} be a set of transpositions in $Sym(n)$. Then the following are equivalent:*

- a) \mathcal{T} is a minimal generating set for $Sym(n)$.
- b) The graph of \mathcal{T} is a tree.
- c) The product of the elements of \mathcal{T} in any order is an n -cycle in $Sym(n)$.

Proof. A connected graph on n vertices must have at least $n - 1$ edges with equality if and only if it is a tree. Thus (a) and (b) are equivalent, as removal of an element of \mathcal{T} disconnects the graph, so by the previous lemma does not generate all of $Sym(n)$.

To see that (b) and (c) are equivalent, observe that an n -cycle can be written as the product of no fewer than $n - 1$ transpositions, and since all of the n -cycles are conjugate to each other, we can see that if *any* ordering of the transpositions in \mathcal{T} has a product which is not an n -cycle, all of them do, and \mathcal{T} cannot generate the n -cycles, contradicting the equivalence of (a) and (b). \square

There are $(n - 1)!$ possible products of $n - 1$ transpositions, and if (c) in the previous lemma holds, each of these will be distinct, i.e. we see every n -cycle exactly once, written as the product of a unique ordering of elements of \mathcal{T} .

If \mathcal{T} is a transposition, then the Cayley graph $X(\text{Sym}(n), \mathcal{T})$ has no triangles or any odd cycles, as the product of any odd number of transpositions cannot be another transposition. This graph is bipartite, with classes corresponding to the parity of the elements of $\text{Sym}(n)$.

From (b) in the previous lemma, we can see that each tree on n vertices determines a Cayley graph of $\text{Sym}(n)$.

Lemma. *Let \mathcal{T} be a set of transpositions in $\text{Sym}(n)$, and let $g, h \in \mathcal{T}$. If the graph of \mathcal{T} contains no triangles, then g and h have exactly one common neighbor in the Cayley graph $X(\text{Sym}(n), \mathcal{T})$ if $gh \neq hg$ and exactly two common neighbors otherwise.*

Lemma. *The neighbors of a vertex g in $X(\text{Sym}(n), \mathcal{T})$ are those of the form xg , where $x \in \mathcal{T}$. If $xg = yh$ is a common neighbor of g and h , then $yx = hg$ and any solution to this yields a common neighbor. If h and g commute, then $yx = hg$ has two solutions, one of which is the identity and the other is hg .*

If h and g do not commute, then they have overlapping support, but there are three ways to factor hg into transpositions: as hg , as ah and as gb , for specific a and b . But because there are no triangles in the graph of \mathcal{T} , a and b cannot be in \mathcal{T} , hence the identity is the only common neighbor of g and h .

Theorem. *Let \mathcal{T} be a minimal generating set of transpositions for $\text{Sym}(n)$. If the graph of \mathcal{T} is asymmetric, the groups $\text{Aut}(X(\text{Sym}(n), \mathcal{T}))$ and $\text{Sym}(n)$ are isomorphic.*

Proof. Let T be the graph of \mathcal{T} . Since \mathcal{T} is a minimal generating set, T is a tree and is thus acyclic. Then by the previous lemma, we can determine the set of non-commuting transpositions in \mathcal{T} from the graph $X(\text{Sym}(n), \mathcal{T})$, or equivalently those transpositions in \mathcal{T} which have overlapping support. Thus $X(\text{Sym}(n), \mathcal{T})$ determines the line graph of T . Since T is a tree, it is determined by its line graph.

Any (non-identity) element $g \in \text{Aut}(X(\text{Sym}(n), \mathcal{T}))$ induces a permutation of \mathcal{T} . Since automorphisms preserve paths of length two, the restriction of g to \mathcal{T} is an automorphism of T , which, by the assumption on T , is trivial.

Suppose now that $g \in \text{Aut}(X(\text{Sym}(n), \mathcal{T}))$ fixes at least one vertex. We want to show that g is the identity, and thus that this automorphism group acts regularly. Suppose, for the sake of contradiction, that g is not the identity. Then since $X(\text{Sym}(n), \mathcal{T})$ is connected, there is a vertex v fixed by g adjacent to a vertex w which is not fixed. Then $\rho_v g \rho_v^{-1}$ fixes the vertex e corresponding to the identity and moves the adjacent vertex wv^{-1} , which is impossible. Thus g must be the identity, so the automorphism group acts regularly. Since the group acts regularly and every automorphism of T is trivial, the automorphism group of $X(\text{Sym}(n), \mathcal{T})$ must be exactly $\text{Sym}(n)$. \square

It is often difficult to determine the full automorphism group of a Cayley graph, so this theorem is actually kind of interesting.

Chapter 4 : Arc-Transitive Graphs

Recall that an *arc* in a graph is an ordered pair of adjacent vertices. Thus a graph is *arc-transitive* if its automorphism group acts transitively on the set of arcs. This is stronger than vertex- or edge-transitivity, so we can prove some interesting things in this setting which apply to these weaker notions. We begin by building up to Tutte's results on cubic arc-transitive graphs. Then, we consider some famous examples of arc-transitive graphs.

Arc-Transitive Graphs

Definition. An ***s*-arc** in a graph is a sequence of s vertices such that consecutive vertices are adjacent and $v_{n-1} \neq v_{n+1}$. We are permitted to use the same vertex twice in general, just not in second-adjacent positions. A graph is ***s*-arc-transitive** if its automorphism group acts transitively on s -arcs. This property is inductive, in that if a graph is s -arc-transitive, it is also $(s-1)$ -arc-transitive. A 0-arc-transitive graph is vertex-transitive. A 1-arc-transitive graph is sometimes called **symmetric**.

A cycle on n vertices is s arc-transitive for all s .⁴ More interestingly, the cube Q is 2-arc-transitive but not 3-arc-transitive, as the three arcs which form three sides of a 4-cycle can't be mapped to three arcs which do not form three sides of a 4-cycle.

A graph X is s -arc transitive if it has a group G of automorphisms such that G is transitive, and the stabilizer G_u of a vertex u acts transitively on s -arcs starting at u .

Lemma. *The graphs $J(v, k, i)$ are at least arc transitive.*

Proof. Consider the vertex $\{1, 2, 3, \dots, k\}$. The stabilizer of this vertex contains $\text{Sym}(k) \times \text{Sym}(v-k)$. Clearly any two k -sets meeting this initial vertex in an i -set can be mapped to each other by this group. \square

Lemma. *The graphs $J(2k+1, k, 0)$ are at least 2-arc transitive.*

Proof. Each edge in this graph can be labeled by the single element not in either of the sets it is incident to. Thus a 2-arc is an ordered pair of distinct elements. Suppose we want to map the arc $[a, b]$ onto an arc $[x, y]$. Then the permutation $(ax)(by)$ does the job. \square

Definition. The **girth** of a graph is the length of the shortest cycle in it.

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

Proof. Let's assume $s \geq 3$, otherwise the conclusion is meaningless. By our assumption, X contains a cycle of length g as well as a path of length g whose endpoints are not adjacent. This is a g -arc with adjacent end vertices and a g -arc with nonadjacent end vertices. No automorphism can map one to the other, so $s < g$. Since X contains cycles of length g , and since these contain s -arcs, any s -arc must lie in some cycle of length g . Let $\alpha = v_1, v_2, \dots, v_s$ be an s -arc. Since v_{s-1} has valency at least 3, it is adjacent to some vertex $w \neq v_s, v_{s-2}$, and since the girth of X is at least s , w doesn't lie in α , otherwise we could have constructed a shorter cycle. Thus if we replace v_s with w , we get a second s -arc β which intersects α in an $(s-1)$ -arc. Since β lies in a g -cycle as well, we get a pair of cycles of length g which share at least $s-1$ edges in common.

⁴The comment in the book is one of the best things I've ever read in a math book: "...which only goes to show that truth and utility are different concepts."

Deleting these $s - 1$ edges from the graph, the graph must still contain a cycle of length at most $2g - 2s + 2$, so $2g - s2 + 2 \geq g$, and the result follows from algebraic manipulation. \square

A natural question to ask is what we can say about the s -arc transitive graphs with girth equal to $2s - 2$. It follows from the next lemma that these graphs are what we will later refer to as *generalized polygons*.

Lemma (Tutte). *If X is s -arc transitive with girth $2s - 2$, it is bipartite with diameter $s - 1$.*

Proof. First, if X has girth $2s - 2$, then any s -arc lies in at most one cycle of length $2s - 2$, and so if X is s -arc transitive, every s -arc lies in a unique cycle of length $2s - 2$. Thus X has diameter at least $s - 1$, which is the distance between opposite points in such a cycle. Let u be a vertex of X and suppose, for the sake of contradiction, that v is a vertex at distance s from u . Then there is an s -arc joining u and v , which lies in a cycle of length $2s - 2$. Since the diameter of such a cycle is $s - 1$, we have a contradiction. Thus the diameter of X is at most $s - 1$, so it is equal to this quantity.

If X is not bipartite, it contains an odd cycle of minimal length C . Because the diameter of X is $s - 1$, the cycle must have length $2s - 1$. Let u be a vertex in C and let v, v' be the two vertices at distance $s - 1$ from u . Then we can form an s -arc u, \dots, v, v' which must lie in a cycle C' of length $2s - 2$. The vertices of C and C' not internal to this s -arc form a cycle of length less than $2s - 2$, which contradicts our earlier result. \square

In a little bit, we'll use this result to show that s -arc transitive graphs with girth $2s - 2$ are distance transitive.

Arc Graphs

Definition. If $s \geq 1$ and $\alpha = (x_0, x_1, \dots, x_s)$ is an arc in X , the **head** $head(\alpha)$ is the $(s - 1)$ -arc (x_1, x_2, \dots, x_s) and the **tail** $tail(\alpha)$ is the $(s - 1)$ -arc $(x_0, x_1, \dots, x_{s-1})$. If α and β are s -arcs, then we say **α follows β** if there is an $(s + 1)$ -arc γ such that $head(\gamma) = \beta$ and $tail(\gamma) = \alpha$. Sometimes we say that α can be **shunted** onto β .

Let s be a non-negative integer. We let $X^{(s)}$ denote the directed graph with the s -arcs of X as its vertices, such that (α, β) is an arc in $X^{(s)}$ if and only if α can be shunted onto β . Automorphisms of X extend to automorphisms of $X^{(s)}$, so if X is s -arc transitive, $X^{(s)}$ is vertex transitive.

Lemma. *Let X and Y be directed graphs and let f be a homomorphism from X onto Y such that every edge in Y is the image of an edge in X (i.e. f is edge-surjective). Suppose y_0, y_1, \dots, y_r is a path in Y . Then for each vertex x_0 in X such that $f(x_0) = y_0$, there is a path x_0, x_1, \dots, x_r such that $f(x_i) = y_i$. That is, if f is edge-surjective, then the preimages of r -arcs in Y are r -arcs in X in the natural way.*

Proof. Any vertex which is the preimage of y_0 must be adjacent to some vertex which is the preimage of y_1 , as f preserves adjacency. Since homomorphisms map edges onto edges, we can proceed inductively. \square

Definition. A **spindle** in X is a subgraph of X consisting of two given vertices u and v joined by three paths, with any two of these having only the endpoints in common. A **bicylce** is a subgraph consisting of either two cycles with exactly one vertex in common or two vertex-disjoint cycles

with a path connecting them such that the only sharing of vertices is that each cycle contains an endpoint of the path.

Lemma. *If X is a spindle or a bicycle, then $X^{(1)}$ is strongly connected.*

Proof. Recall that $X^{(1)}$ is the directed graph whose vertices are edges in X with an arc (x, z) if and only if x, y, z is a 2-arc in X . This graph is vertex-transitive, so by an earlier theorem which states that if every vertex has in-valency equal to its out-valency, then it is weakly connected if and only if it is strongly connected. Since X is connected, $X^{(1)}$ is weakly connected, thus it is strongly connected. \square

Theorem. *If X is a connected graph with minimum valency two which is not a cycle, then $X^{(s)}$ is strongly connected for all $s \geq 0$.*

Proof. First we prove this for $s = 0, 1$ then for all s by induction. If $s = 0$, then $X^{(0)}$ is the graph where we replace each edge in X with a pair of opposite directed arcs, so this case is obviously true. For $s = 1$, we need to show that any 1 arc can be shunted onto any other 1-arc. Since X is connected, we can shunt any 1-arc onto an edge of X , but not necessarily in the correct direction. We therefore need to show that any 1-arc can be reversed, that is the arc (x, y) can be shunted onto the arc (y, x) .

Since X has minimum valency at least two and is finite, it contains a cycle C . If C does not contain x and y , then we can find a path in X joining y to C . We can then shunt (x, y) along the path and around the cycle then back along the path to get a $y-x$ arc.

If x and y are both in C but they are not adjacent in the cycle, then adding the edge (x, y) to C forms a spindle, so by the lemma above, we are done.

Finally, we need to consider that (x, y) is an edge in C . Since X is not a cycle and is connected, there is a vertex z in X which is not in C adjacent to some vertex w in C . Let P be a maximal-length path in X such that w and z are the first two vertices in P . The last vertex in P is adjacent to a vertex in P and possibly a vertex in C . If it is adjacent to a vertex in C which is not w , then (x, y) is an edge in a spindle formed by adding this edge to P . If it is adjacent to a vertex in P which is not in C , then we can add this edge to form a bicycle. In either case, by the above lemma, we are done.

Finally, we induct. Suppose that $X^{(s)}$ is strongly connected for some $s \geq 1$. The operation of taking the head of an $(s+1)$ -arc is a homomorphism from $X^{(s+1)}$ to $X^{(s)}$. Since X has minimum valency at least two, each s -arc is the head of some $(s+1)$ -arc, so every edge in $X^{(s)}$ is the image under the homomorphism of some edge in $X^{(s+1)}$. Let α, β be any two $(s+1)$ -arcs in X . Since $X^{(s)}$ is strongly connected, there is a path in it joining $head(\alpha)$ to $tail(\beta)$. By the earlier lemma, this path lifts to a path in $X^{(s+1)}$ from α to a vertex γ such that $head(\gamma) = tail(\beta)$. Since X has minimum valency at least two and $s \geq 1$, γ can be shunted onto β , so α can be shunted onto β by γ , so there is a path in $X^{(s+1)}$ from α to β . Since these were chosen arbitrarily, it follows that $X^{(s+1)}$ is strongly connected. \square

We're about to use this to prove that an arc-transitive cubic graph is s -arc regular for some s .

Cubic Arc-Transitive Graphs

A result of Tutte shows that for any s -arc transitive cubic graph, $s \leq 5$. This led to a result of Weiss that for any s -arc transitive graph, $s \leq 7$. This result relies on the classification of the finite simple groups.

Lemma. *Let X be a strongly connected directed graph, let G be a transitive subgroup of its automorphism group, and, if u is a vertex of X , let $N(u)$ be the set of vertices such that (u, v) is an arc of X . If there is a vertex u such that $G_u \upharpoonright N(u)$ is the identity, then G is regular.*

Proof. Suppose that u is a vertex of X and that $G_u \upharpoonright N(u)$ is the identity group. By an earlier lemma, if v is any vertex in X , then G_u is conjugate to G_v in G , as $v = u^g$ for some g by transitivity, and $g^{-1}G_u g = G_{x^g} = G_v$. Hence $G_v \upharpoonright N(v)$ must be the identity for all vertices v .

Assume, for the sake of contradiction, that G_u is not the identity group. Since X is strongly connected, we can pick a path from u to some vertex w which is not fixed by G_u , and we can, without loss of generality, pick the w corresponding with the shortest such path. Then if v is the second-last vertex along this path, and $u \neq v$ as $N(u)$ is fixed by G_u , and $N(v)$ is not fixed here. Since G_u fixes v it fixes $N(v)$, but acts nontrivially on it, because it doesn't fix w . Hence $G_v \upharpoonright N(v)$ is not the identity group. This is our contradiction, hence G_u is the identity group.

Thus the group acts regularly as the only group element with fixed points is the identity. □

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

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

Proof. If X is cubic, then $X^{(s)}$ has out-valency two. Let $G = \text{Aut}(X)$, let α be an s -arc in X , and let H be the subgroup of G which fixes each vertex in α . Then G acts vertex transitively on $X^{(s)}$ and H is the stabilizer in G of the vertex α in $X^{(s)}$. If the restriction of H to the out-neighbors of α isn't trivial, then H must swap the two s -arcs which follow α . Any two $(s+1)$ -arcs in X can be mapped by elements of G to $(s+1)$ -arcs which have α as the initial s -arc portion. In this case, G acts transitively on the $(s+1)$ -arcs of X , which contradicts the assumption. Thus the restriction of H to the out-neighbors of α must be trivial, so by the previous lemma, the whole group H must be trivial. This $G_\alpha = \{e\}$, so G acts regularly on the s -arcs of X . □

If X is a regular graph on n vertices with valency k and $s \geq 1$, then there are exactly $nk(k-1)^{s-1}$ s -arcs. It follows that if X is s -arc transitive, then $|\text{Aut}(X)|$ must be divisible by $nk(k-1)^{s-1}$ and if X is s -arc regular, then $|\text{Aut}(X)| = nk(k-1)^{s-1}$. In particular, a cubic arc-transitive graph X is s -arc regular if and only if $|\text{Aut}(X)| = (3n)2^{s-1}$. For example consider the cube Q on 8 vertices. The stabilizer of a vertex must contain $\text{Sym}(3)$, so $|\text{Aut}(Q)| \geq 48$. We saw earlier that Q is not 3-arc transitive, so it must be 2-arc regular, hence $|\text{Aut}(Q)| = 48$.

Finally, we get to Tutte's theorem:

Theorem (Tutte). *If X is s -arc regular and cubic, then $s \leq 5$.*

The smallest 5-arc regular cubic graph is Tutte's 8-cage on 30 vertices.

Corollary. *If X is arc-transitive and cubic, v is a vertex of X and $G = \text{Aut}(X)$, then $|G_v|$ divides 48 and is divisible by 3.*

The Petersen Graph

The Petersen graph is really cool. It's small (10 vertices, 15 edges) but it plays a central role in many different aspects of graph theory, as it is a frequent example and counterexample. We have already proven some things about the Petersen graph under a different name, such as $J(5, 2, 0)$ or $L(K_5)$, the dual of K_6 in \mathbb{RP}^2 , and as one of the five nonhamiltonian vertex-transitive graphs.

The Petersen graph can also be constructed from the dodecahedron. Every vertex in the dodecahedron has a unique vertex at distance five from it. Consider the graph where vertices correspond to pairs $\{v, v'\}$ of such vertices, where $\{u, u'\}$ is adjacent to $\{v, v'\}$ if and only if there is a perfect matching between them in the dodecahedron. The resulting graph is the Petersen graph, and we say that the dodecahedron is a *two-fold cover* of the Petersen graph. Covers will come back later, but they are of importance in algebraic topology.

Since $\text{Sym}(5)$ acts on $J(5, 2, 0)$, the automorphism group of the Petersen graph has order at least 120, so it is at least 3-arc transitive. Because its girth is five, it cannot be 4-arc transitive. Thus it is 3-arc regular and its automorphism group has exactly 120 elements. Thus $\text{Sym}(5)$ in its action on the 2-element subsets of a set of five elements is the entire automorphism group of the Petersen graph.

The Petersen graph is important in one of the most famous graph theory problems, the Four Color Theorem. This theorem asks whether (and answers in the affirmative) any plane graph can be properly face-colored with at most four colors such that any two adjacent faces are a different color. It can be shown that this is equivalent to asking whether a cubic planar graph with edge connectivity at least two can be properly edge-colored with three colors such that any two edges incident to the same vertex are colored differently. The Petersen graph was the first cubic graph to be shown to not have a proper 3-edge coloring.

Theorem. *The Petersen graph cannot be 3-edge-colored.*

Proof. Let P be the Petersen graph and suppose, for the sake of contradiction, that P can be properly 3-edge-colored. Since P is cubic, each color class is a 1-factor (a perfect matching). Exploring a case argument shows that each edge belongs to exactly two 1-factors. For each of these 1-factors, the remaining edges form a graph isomorphic to a pair of C_5 cycles, which cannot be partitioned into two 1-factors. Since P is edge-transitive, this must hold for all 1-factors of P , so P cannot be properly 3-edge-colored. \square

Since the Petersen graph is not planar, it is not a counterexample to the Four Color Theorem.

We have seen that there is a cycle through any nine, but not all ten, vertices of the Petersen graph. Let $X \setminus v$ denote the induced subgraph realized by deleting the vertex v from the graph. A nonhamiltonian X for which $X \setminus v$ is hamiltonian for all vertices v is called *hypohamiltonian*. The Petersen graph is the unique smallest hypohamiltonian graph, and the next smallest have 13 and 15 vertices, respectively, and these are closely related to the Petersen graph. These will come back later.

We have only just begun to see the special properties of the Petersen graph, and it will show up again and again. In particular, the Petersen graph is *distance-transitive*, a *Moore graph*, and

strongly regular.

Distance-Transitive Graphs

Definition. 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 g of X such that $(v, v') = (u, u')^g$. A distance-transitive graph is always at least 1-arc transitive. The complete graphs, the complete bipartite graphs with equal sized classes, and the circuits are all distance transitive.

The Petersen graph is distance transitive, since it and its complement are both arc transitive. Another family of examples are the k -cubes Q_k from Chapter 3. If $d(u, u') = d(v, v') = i$, then by adding u (realized as a bit string) to the first pair and v to the second pair lets us assume, without loss of generality, that $u = v = \vec{0}$. Then u' and v' are different strings with i ones which can obviously be mapped to each other by an element of $Sym(k)$ which acts by permuting indices.

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

Proof. We want to show that u and v have distance i in $J(v, k, k - 1)$ if and only if $|u \cap v| = k - i$, realizing u and v as k -sets. To see this, observe that the definition of the graph is that u and v are at distance one if and only if their intersection has $k - 1$ elements. Vertices u and v are at distance 2 if and only if there is some vertex w such that $|u \cap w| = |w \cap v| = k - 1$ and $|u \cap v| \neq k - 1$. Since u, v, w are all k -sets, this can only happen if u and v share exactly $k - 2$ elements. We can proceed further inductively. \square

Lemma. *The graph $J(2k + 1, k + 1, 0)$ is distance transitive.*

Proof. This follows immediately from the proof that it is k -arc transitive. \square

There is an equivalent characterization of distance transitivity which is often easier to work with, but we need to develop a bit of notation first. If u is a vertex of X , then let $X_i(u)$ denote the set of vertices at distance i from u . The partition $\{u, X_1(u), \dots, X_d(u)\}$ is called the *distance partition* with respect to u ⁵ this thing should look very familiar to anyone who's seen breadth first search algorithms before. If G acts distance transitively on X , u is a vertex of X , and v, v' are two vertices at distance i from u , there is an element of G which maps (u, v) to (u, v') , that is there is some $g \in G_u$ which maps v to v' , and thus G_u acts transitively on $X_i(u)$. Thus the cells of the distance partition with respect to u are the orbits of G_u . If the diameter of X is d , then for any vertex u in X , the vertex stabilizer G_u has exactly $d + 1$ orbits, so G is transitive with rank $d + 1$.

Since the cells of the distance partition are orbits of G_u , every vertex in $X_i(u)$ is adjacent to a_i vertices in $X_i(u)$, b_i vertices in $X_{i+1}(u)$ and c_i vertices in $X_{i-1}(u)$. Another way to say this is that the graph induced by the cell $X_i(u)$ is a_i -regular, and the graph induced by any pair of cells is semiregular. The whole graph X is regular, and its valency is b_0 , the number of edges from u to any vertex in $X_1(u)$. If d is the diameter of X , then $c_i + a_i + b_i = b_0$ for $i = 1, 2, \dots, d$.

These are called the *parameters* of the distance transitive graph X and determine lots of properties of X . We can write these numbers in a $3 \times (d + 1)$ array called the *intersection array*:

⁵.

$$\begin{pmatrix} - & c_1 & \dots & c_{d-1} & c_d \\ a_0 & a_1 & \dots & a_{d-1} & a_d \\ b_0 & b_1 & \dots & b_{d-1} & - \end{pmatrix}$$

Each column sums to the valency of the graph, so we only need to give only two rows to determine the third and thus the whole graph. It is customary to use the following abbreviation:

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

As an example, think of the dodecahedron. A quick examination lets us construct the following intersection array:

$$\begin{pmatrix} - & 1 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 1 & - \end{pmatrix}$$

Lemma. *A connected s -arc transitive graph with girth $2s - 2$ is distance transitive with diameter $s - 1$.*

Proof. Let X be connected, s -arc transitive, and have girth $2s - 2$, and let (u, u') and (v, v') be pairs of vertices at distance i . Since X has diameter $s - 1$, we know that $i \leq s - 1$. These two pairs of vertices are joined by paths of length i , and since X is transitive on s -arcs, it must be transitive on i arcs as well. Thus there is an automorphism mapping (u, u') to (v, v') , so X is distance transitive. \square

Distance transitivity is a *symmetry property* of graphs in that it is defined in terms of the existence of certain automorphisms, namely that the a_i, b_i, c_i are well-defined. There is a combinatorial analogue which simply asks that these numerical properties of the a_i, b_i, c_i hold, without making mention of automorphisms and whether or not they exist. Given any X , we can compute the distance partition, and it may occur by accident that every vertex in $X_i(u)$ is adjacent to some constant number of vertices in its own and the adjacent cells, regardless of whether there are automorphisms which force this to happen.

Definition. If the intersection array is well-defined and is the same regardless of which vertex u we pick as the initial vertex, then X is called **distance regular**. Any distance transitive graph must be distance regular, but the converse is not at all true.

One class of distance regular graphs, many of which are not distance transitive are the *Latin squares*. A Latin square of order n is an $n \times n$ matrix with entries from $\{1, 2, \dots, n\}$ such that each row and column has each element exactly once. Given an $n \times n$ Latin square L , we can get the set of n^2 triples (i, j, L_{ij}) , which correspond to a row index, a column index, and the entry at that position. Let $X(L)$ be the graph with these triples as vertices and edges between two triples if and only if they agree on at one coordinate (by the definition of Latin squares, they can agree on at most one coordinate). Alternatively, $X(L)$ is the graph whose vertices are the n^2 positions in L and two ‘positions’ are adjacent if they lie in the same row, the same column, or have the same entry. This graph has n^2 vertices, diameter 2, and is $3(n - 1)$ -regular. It is distance regular but not, in general, distance transitive.

Lemma. *The order n Latin square L is distance regular*

Proof. Each vertex has the same valency and L has diameter 2, so every distance partition will have one vertex in $X_0(u)$, $3(n-1)$ vertices in $X_1(u)$, and the remainder in $X_2(u)$, and by symmetry, the intersection arrays must be the same for all choices of u . \square

The Coxeter Graph

The Coxeter graph is a 28-vertex cubic graph with girth 7. One way to construct it is to take Cayley graphs on the cycles $X(\mathbb{Z}_7, \{1, -1\})$, $X(\mathbb{Z}_7, \{2, -2\})$ and $X(\mathbb{Z}_7, \{3, -3\})$ and add seven new vertices, each of which connects to the same element in each cycle.

Another way to construct it is as an induced subgraph of $J(7, 3, 0)$. The vertices of $J(7, 3, 0)$ are the 35 triples from $\Omega = \{1, 2, \dots, 7\}$, two vertices are adjacent if they correspond to disjoint triples, distance 2 if they have 2 points in common, and distance 3 if they share one point. Call a *heptad* a set of seven triples such that each pair share exactly one point and there is no point in all of them. Graph theoretically, a heptad is a set of seven vertices such that each pair is at distance 3. As an example, the set $\{(124), (235), (346), (457), (561), (672), (713)\}$ form a heptad. This set of triples is invariant under the 7-cycle $\sigma = (1234567) \in \text{Sym}(7)$. It's easy to see that the four triples $\{(357), (367), (567), (356)\}$ lie in distinct orbits of σ . The orbit of (356) is another heptad. The orbits of the first three are isomorphic, in the order presented, to $X(\mathbb{Z}_7, \{1, -1\})$, $X(\mathbb{Z}_7, \{2, -2\})$ and $X(\mathbb{Z}_7, \{3, -3\})$, respectively. It's simple to see that these three triples are the unique triples in their orbits which are disjoint from (124) , and a little harder to see that no triple from one of these orbits is disjoint from any triple in one of the other two. Thus, the orbits of the triples $\{(124), (357), (367), (567)\}$ induce a subgraph isomorphic to the Coxeter graph, and the seven vertices excluded from this subgraph are a heptad. We can use this embedding to show that its girth is seven.

Lemma. *The diameter of $J(7, 3, 0)$ is three and its girth is six.*

Proof. Let $Y = J(7, 3, 0)$. $Y_1(u)$ is the set of triples disjoint from u , $Y_2(u)$ is the set of triples which meet u in two points, and $Y_3(u)$ the set of triples which meet u in one point. Thus there are no edges internal to $Y_1(u)$ or $Y_2(u)$, so the girth of Y is at least six. Since it is easy to find a 6-cycle, the girth is also at most six, and we are done. \square

A quick argument shows that each triple in Ω not in a heptad is disjoint from exactly one triple of the heptad. Thus deleting a heptad from $J(7, 3, 0)$ gives us a 28-vertex cubic graph X . To show that X has girth seven, we need to show that every heptad meets every 6-cycle on $J(7, 3, 0)$, so we characterize the 6-cycles of $J(7, 3, 0)$.

Lemma. *There is a bijection between 6-cycles in $J(7, 3, 0)$ and partitions of Ω of the form $\{abc, de, fg\}$.*

Proof. The partition $\{abc, de, fg\}$ corresponds to the 6-cycle $ade, bfg, cde, afg, bde, cfg$. To show that every 6-cycle has this form, we just need to look at 6-cycles through 123. Without loss of generality, assume that the neighbors of 123 are 456 and 457. The vertex at distance three from 123 has one point in common with 123, say 1, and two in common with 456 and 457, so it must be 145. This then determines the partition $\{167, 23, 45\}$, and the 6-cycle must be of the type described above. \square

Lemma. *Every heptad meets every 6-cycle in $J(7, 3, 0)$.*

Proof. The seven triples in a heptad contain 21 pairs of points. As two distinct triples have only one point in common, these pairs must be distinct. Thus each pair of points in Ω lies in exactly one triple in the heptad. If the point i lies in r triples, then it lies in $2r$ pairs. Thus each point must lie in exactly three triples. Without loss of generality, consider the 6-cycle corresponding to $\{123, 45, 67\}$. Each heptad has a triple of the form $a45$ and one of the form $b67$. At least one of a, b must be one of 1, 2, 3, otherwise the two triples would meet in two points. Thus the 6-cycle has a point in common with any heptad. \square

We'll see later that all of the heptads in $J(7, 3, 0)$ are equivalent under $Sym(7)$. The automorphism group of the Coxeter graph is at least the size of the stabilizer in $Sym(7)$ of the heptad we removed from $J(7, 3, 0)$. The heptad described earlier is fixed by the permutations $(23)(47), (2347)(56), (235)(476), (1234567) \subset Sym(7)$. The first two generate a group of order 8, so the group generated by these has order divisible by 8, 3, and 7, and is therefore of order at least 168. This implies the Coxeter graph is at least 2-arc transitive. In fact, there is an additional automorphism of order two, so its full automorphism group has order 336 and acts 3-arc regularly.

Tutte's 8-Cage

Another cubic arc-transitive graph is Tutte's 8-cage on 30 vertices. Tutte, in 1947, gave the following description of the construction of the graph. Take the cube Q and an additional vertex ∞ . In each set of four parallel edges, join the midpoint of each pair of opposite edges with an edge, then join the midpoint of the two new edges by an edge, then join the midpoint of this edge to ∞ . The resulting graph is cubic and on 30 vertices. Alternatively, we can use the edges and 1-factors of K_6 . There are 15 edges in K_6 , and each lies in three 1-factors (perfect matchings), so there are 15 1-factors. Construct a bipartite graph T with the 15 edges as one color class and the 15 1-factors as the other, with an edge in T corresponds with an edge in the first class being part of a 1-factor in the second. This graph is cubic and on 30 vertices, and is isomorphic to the 8-cage. One advantage here is that it is clear that $Sym(6)$ acts as an automorphism group with the two partitions as its orbits.

We should still think about why these two descriptions are equivalent. It turns out that the cubic graph on 30 vertices with girth 8 is unique. We'll first show that this bipartite graph T has girth 8.

Lemma. *Let F be a 1-factor of K_6 and let e be an edge of K_6 which is not in F . Then there is a unique 1-factor on e which contains an edge of F .*

Proof. Two edges of K_6 lie in a 1-factor if and only if they are disjoint, and two disjoint edges lie in a unique 1-factor. Since $e \notin F$, it meets two distinct edges of F , so it is disjoint from exactly one edge in F , and e plus this edge thus lie in a unique 1-factor. \square

Since T is bipartite, if its girth is less than 8, it must be four or six, as bipartite graphs do not contain odd cycles. The girth can't be four, as otherwise e_1, F_1, e_2, F_2 is a cycle where e_2 belongs to disjoint 1-factors F_1, F_2 , but both of these contain e_1 , which obviously can't happen. Similarly, the girth can't be six, as then $e_1, F_1, e_2, F_2, e_3, F_3$ is a cycle in which F_2 and F_3 are distinct 1-factors on e_3 which contain e_2 and e_1 , respectively, contradicting the previous lemma. Thus T has girth at least eight. To see that it is exactly eight, we can construct an 8-cycle. There are lots of them, but one example is $(1, 2), (1, 2-3, 4-5, 6), (34), (1, 5-2, 6-3, 4), (2, 6), (1, 4-2, 6-3, 5), (3, 5), (1, 2-3, 5-4, 6)$ (the edge $(1, 2)$, then the 1-factor matching 1 to 2, 3 to 4, and 5 to 6, and so on).

Finally, we need to show that there is an automorphism which swaps the classes of vertices, which we need to build up to a little bit.

Definition. A **1-factorization** of a graph is a partition of its edge set into 1-factors. Given a 1-factor F of K_6 , there are six 1-factors which share an edge with F , so eight are edge-disjoint from F . The union of two disjoint 1-factors in K_6 forms a 6-cycle, so the remaining edges form a 3-prism. The 3-prism has four 1-factors and a unique 1-factorization, so any disjoint one factors lie in a unique 1-factorization. Counting the triples (F, G, \mathcal{F}) where F and G are 1-factors in the 1-factorization \mathcal{F} , we see there are six 1-factorizations of K_6 . Since each 1-factor lies in the same number of 1-factorizations, this implies that each 1-factor lies in two 1-factorizations. There are fifteen pairs of distinct 1-factorizations, so any two distinct 1-factorizations have a unique 1-factor in common.

We will use these six 1-factorizations to construct a bijection between the edges and the 1-factors of K_6 and then show that this bijection is an automorphism of T . Arbitrarily label the 1-factorizations of K_6 as $\mathcal{F}_1, \dots, \mathcal{F}_6$. Define a map ψ by doing the following. If $e = (i, j)$ is an edge in K_6 , then $\psi(e)$ is the 1-factor that \mathcal{F}_i and \mathcal{F}_j have in common. The five edges in K_6 incident to vertex i are mapped by ψ to the five 1-factors contained in \mathcal{F}_i . If e and f are edges in K_6 incident to the same vertex, then $\psi(e)$ and $\psi(f)$ are edge-disjoint 1-factors. Since there are only eight 1-factors disjoint from any given one, this tells us that if e and f are not incident, then $\psi(e)$ and $\psi(f)$ must share an edge. Thus three independent edges in K_6 are mapped by ψ to three 1-factors, any two of which share an edge. Any such set must therefore consist of the three 1-factors on a single edge. Thus if $F = \{e, f, g\}$ is a 1-factor, then define $\psi(F)$ to be the edge of K_6 common to $\psi(e), \psi(f), \psi(g)$.

This is definitely a bijection, and all we need to show now is that it is also an automorphism of T . Suppose that e is an edge adjacent to the 1-factor $F = \{e, f, g\}$. Then $\psi(F)$ is the edge that $\psi(e), \psi(f), \psi(g)$ share. In particular, $\psi(F)$ is an edge in $\psi(e)$, so $\psi(e)$ is adjacent to $\psi(f)$ in T . Thus ψ is an automorphism of T which swaps the two color classes. Hence T is vertex transitive and thus arc transitive with an automorphism group of order at least $2 \times 6! = 1440$. If T is s -arc transitive, then $s \geq 5$, so by previous results, we know $s = 5$. Thus we know that T is distance transitive with diameter 4.

Finally we'll sketch a proof that this graph is the unique bipartite cubic graph on 30 vertices with girth 8. Let X be such a graph and v any vertex in X , and consider the graph induced by $X_3(v) \cup X_4(v)$, the set of vertices at distance 3 and 4 from v . The eight vertices in $X_4(v)$ all have valency three and the twelve vertices of $X_3(v)$ all have valency two and are adjacent to two vertices in $X_4(v)$. This graph is thus a subdivision of a cubic graph Y which has girth four. That X has girth eight implies that there is a partition of the edges of Y into pairs at distance three. The cube is the unique graph on eight vertices with this property, so $X_3(v) \cup X_4(v)$ is the subdivision graph of the cube, but this is exactly the first step in Tutte's construction, and the only extension to a bipartite cubic graph on 30 vertices with girth eight is Tutte's procedure.

Chapter 5 : Generalized Polygons and Moore Graphs

A general graph with diameter d has girth at most $2d + 1$, and a bipartite graph with diameter d has girth at most $2d$. These bounds are simple, but the graphs for which these are tight are actually kind of interesting. Graphs with diameter d and girth $2d + 1$ are called *Moore graphs*.⁶ The tools in this theory have led to a proof that a Moore graph has diameter at most two, and such a graph with diameter equal to two must be regular with valency 2, 3, 7, or 57, and the machinery to prove this will come later, in Chapter 10.

Bipartite graphs with diameter d and girth $2d$ are called *generalized polygons*⁷ and complete bipartite graphs, which have diameter two and girth four, are generalized polygons we've already seen a bit about. Generalized polygons are related to classical geometry, and a generalized polygon with diameter three is related to the projective planes. When $d = 4$, these are called generalized quadrangles and many examples are related to quadrics in projective space.

We're going to look closely at Moore graphs and generalized polygons.

Incidence Graphs

Definition. An *incidence structure* is a set \mathcal{P} of points, a set \mathcal{L} of lines (disjoint from \mathcal{P}), and a relation $I \subseteq \mathcal{P} \times \mathcal{L}$ called *incidence*. If $(p, L) \in I$, then we say that the point p and the line L are **incident**. If $\mathcal{J} = (\mathcal{P}, \mathcal{L}, I)$ is an incidence structure, then its **dual incidence structure** $\mathcal{J}^* = (\mathcal{L}, \mathcal{P}, I^*)$, where $I^* = \{(L, p) | (p, L \in I)\}$. This can be thought of as exchanging the roles of the points and lines.

Definition. The **incidence graph** $X(\mathcal{J})$ of an incidence structure \mathcal{J} is the graph with vertices $\mathcal{P} \cup \mathcal{L}$ where two vertices are adjacent if and only if the corresponding (p, L) is in \mathcal{J} .

The incidence graph for any incidence structure is obviously bipartite. More interestingly, the converse holds as well. For any bipartite graph, we can define an incidence structure just by declaring one class to be the points and the other the lines and using adjacency to define incidence. In this way, it is clear that any bipartite graph identifies an incidence structure and its dual, and the graphs $X(\mathcal{J})$ and $X(\mathcal{J}^*)$ are isomorphic. This suggests that the definition of incidence structures isn't terribly strong, so we need to do some more work and impose some conditions before we can prove interesting things.

Definition. A **partial linear space** is an incidence structure in which any two points are incident with at most one line. This also implies that any two lines are incident with at most one common point.

Lemma. *The incidence graph $X(\mathcal{J})$ of a partial linear space has girth at least six.*

Proof. If $X(\mathcal{J})$ contains a 4-cycle p, L, q, M for points p and q and lines L and M , then p and q are distinct points shared by two lines, which violates the definition of partial linear space. Since bipartite graphs do not contain odd cycles, the shortest cycle must be of length at least six. \square

In talking about partial linear spaces, we will use geometric terminology. Two points are *collinear* or *joined by a line* if they are incident to the same line. Two lines are *concurrent* if they are incident to a common point. Three pairwise non-collinear points are called a *triangle*.

⁶introduced by Hoffman and Singleton in a seminal paper in AGT

⁷introduced by Tits in work relating to the classification of finite simple groups, of all places

An automorphism of an incidence structure $\mathcal{J} = (\mathcal{P}, \mathcal{L}, I)$ is a permutation σ of $\mathcal{P} \cup \mathcal{L}$ such that $\mathcal{P}^\sigma = \mathcal{P}$, $\mathcal{L}^\sigma = \mathcal{L}$, and $(p^\sigma, L^\sigma) \in I$ if and only if $(p, L) \in I$. This gives an automorphism of the incidence graph which preserves the two classes of the bipartition. An incidence-preserving permutation π of $\mathcal{P} \cup \mathcal{L}$ such that $\mathcal{P}^\pi = \mathcal{L}$ and $\mathcal{L}^\pi = \mathcal{P}$ is called a *duality*. An incidence structure with a duality isomorphic to its dual is called *self-dual*.

Projective Planes

Definition. A **projective plane** is a partial linear space satisfying:

- 1) Any two lines meet in a unique point.
- 2) Any two points meet in a unique line.
- 3) There is at least one triangle.

The first two conditions are dual to each other and the third is self-dual, so the dual of a projective plane is a projective plane. The first two conditions are actually the interesting one, and the third just rules out the 1-dimensional degenerate cases. Sometimes in finite geometry we stipulate a stronger condition, that there is a *quadrangle*, a set of four points, no three of which are collinear and consider the triangle setting degenerate.

Theorem. *Let \mathcal{J} be a partial linear space which contains a triangle. Then \mathcal{J} is a (possibly degenerate) projective plane if and only if its incidence graph $X(\mathcal{J})$ has diameter three and girth six.*

Proof. Let \mathcal{J} be a projective plane containing a triangle. Any two points are at distance two in $X(\mathcal{J})$, and the same for any two lines. Pick a line L and a point p not on L . Any line M through p must meet L at some point p' , and thus L, p', M, p is a path of length three from L to p . Thus any two vertices are at distance at most three, and the existence of a triangle guarantees at least one pair at distance exactly three, so the diameter of $X(\mathcal{J})$ is three. Since \mathcal{J} is a partial linear space, the existence of the triangle also guarantees that the girth is exactly six.

For the other direction, let $X(\mathcal{J})$ of an incidence structure, and suppose that $X(\mathcal{J})$ has diameter three and girth six. One piece of the bipartition corresponds to the points of \mathcal{J} and the other to the lines of \mathcal{J} . Any two points must be at an even distance from each other, and since this distance is at most three, it must be two. There must be a unique path of length two between these two points, otherwise there would be a 4-cycle in $X(\mathcal{J})$, contradicting the assumption on the girth. Hence there is a unique line between any two points, and by duality, any two lines meet at a unique point. Hence we have a projective plane with a triangle. \square

A Family of Projective Planes

Let V be the 3-dimensional vector space over the field \mathbb{F} with q elements. We can define the incidence structure $PG(2, q)$ as follows: the points are the 1-dimensional subspaces of V and the lines are the 2-dimensional subspaces of V . A point p is incident to a line L if and only if the 1-dimensional subspace p is contained in the 2-dimensional subspace L . A k -dimensional subspace of V contains $q^k - 1$ non-zero vectors, so each 2-dimensional subspace contains $q^2 - 1$ non-zero vectors and each 1-dimensional subspace contains $q - 1$ non-zero vectors. Thus each line contains $(q^2 - 1)/(q - 1) = (q + 1)$ distinct points. Similarly, the entire projective plane contains $(q^3 - 1)/(q - 1) = (q^2 + q + 1)$ points. There are $q^2 + q + 1$ lines with $q + 1$ lines passing through each point.

Each point can be represented by a vector $a \in V$, where a and λa represent the same point if $\lambda \neq 0$. A line can be represented by a pair of linear independent vectors, or by a vector a^T . We understand here that a line is a 2-dimensional subspace formed by the vectors x such that $a^T x = 0$. Of course if $\lambda \neq 0$, then λa^T and a^T determine the same line. Then the point represented by a vector b lies on the line represented by a^T if and only if $a^T b = 0$.

Two 1-dimensional subspaces of V lie in a unique 2-dimensional subspace of V (determined by their direct sum), so there is a unique line which joins two points. Two 2-dimensional subspaces intersect in a 1-dimensional subspace (as $\dim(V) = 3$), so any two lines meet in a unique point. Thus $PG(2, q)$ is a projective plane.

By the theorem in the previous section, the incidence graph X of $PG(2, q)$ is bipartite with diameter three and girth six. It has $2(q^2 + q + 1)$ vertices and is $(q + 1)$ -regular. We can also show that it is 4-arc transitive. First we need to find some automorphisms of it.

Let $GL(3, q)$ denote the group of 3×3 invertible matrices over \mathbb{F} . Each element permutes the non-zero vectors in V and maps subspaces to other subspaces, preserving dimension, thus giving rise to an automorphism of X . Recalling that for any pair of ordered bases, there exists an invertible linear map from one to the other, we can say that $GL(3, q)$ acts transitively on the set of ordered bases of V .

Let $p \vee q$ denote the unique line joining the points p and q . If p, q, r are three non-collinear points, then $p, p \vee q, q, q \vee r, r, r \vee p$ is a 6-cycle (hexagon) in X . The sequence $(p, p \vee q, q, q \vee r, r)$ is thus a 4-arc in X , so $\text{Aut}(X)$ acts transitively on the 4-arcs which begin at a point vertex of X . A symmetric argument shows the same for 4-arcs beginning at line vertices. Thus to show that $\text{Aut}(X)$ acts transitively on 4-arcs, we just need to show there is an automorphism which exchanges points and lines in X . This automorphism is pretty simple. For each vector a , swap the point a with the line a^T . Since $a^T b = 0$ if and only if $b^T a = 0$, this maps adjacent vertices to adjacent vertices and swaps points and lines (i.e. is a duality). Therefore, we can see that X is 4-arc transitive. Additionally, by a lemma in the previous chapter, we know that X is distance transitive as well.

Generalized Quadrangles

A second interesting class of incidence structures is the *generalized quadrangles*, which is a partial linear space satisfying the additional conditions that:

- 1) Given any line L and a point p not on L , there is a unique point p' on L such that p and p' are collinear.
- 2) There are points which are not collinear and lines which are not concurrent.

Each of these conditions is self-dual, so the dual of a generalized quadrangle is still a generalized quadrangle. Again we have that the first condition is the interesting one while the second excludes non-interesting degenerate cases where all of the lines intersect at a point or all of the points are on the same line. One generalized quadrangle we've seen before is the incidence structure on the edges and 1-factors of K_6 . This is a generalized quadrangle with incidence graph isomorphic to the Tutte 8-cage.

Two very simple generalized quadrangles are the *grid* and its dual. In a grid, every point is on two lines and in the dual, every line contains two points. We'll see soon why finite geometers think of these as degenerate cases.

Theorem. Let \mathcal{J} be a partial linear space which contains non-collinear points and non-concurrent lines. Then \mathcal{J} is a generalized quadrangle if and only if its incidence graph $X(\mathcal{J})$ has diameter four and girth eight.

Proof. Let \mathcal{J} be a generalized quadrangle and consider the distances in $X(\mathcal{J})$ from some point p . A line is distance one from p if it contains p , and distance three otherwise (as \mathcal{J} is a generalized quadrangle). A point is at distance two from p if it is collinear with p and distance four otherwise. The existence of non-collinear points guarantees that there is a pair of points at distance four. By duality, the same is true for some pair of lines, so the diameter of $X(\mathcal{J})$ is at least four. The girth is at least six. If it were exactly six, then the point and line opposite each other on the 6-cycle violate the condition that there is a unique point on the line not collinear with the point. To show that there is an 8-cycle, let p and q be non-collinear points. Then there is a line L_p containing p but not q and a line L_q containing q but not p . But then there is a unique point on L_p collinear with q and a unique point on L_q collinear with p , and these eight objects in the correct order form an 8-cycle, hence the girth of $X(\mathcal{J})$ is eight.

For the other direction, let $X(\mathcal{J})$ be the incidence graph of some partial linear space \mathcal{J} , and suppose its diameter is four and girth is eight. One part of the partition is the points of \mathcal{J} and the other is the lines. Consider a point p and a line L at distance three from p . Since the girth is eight, there is a unique path L, p', L', p from L to p . This provides the unique point p' on L not collinear with p . \square

A Family of Generalized Quadrangles

We can describe an infinite class of generalized quadrangles, of which the Tutte 8-cage is the incidence graph of the smallest member.

Let V be the vector space of dimension four over a field \mathbb{F} with order q . The *projective space* $PG(3, q)$ is the system of 1- 2- and 3-dimensional subspaces of V . We'll call these points, lines, and planes, respectively. There are $q^4 - 1$ non-zero vectors in V , and each 1-dimensional subspace contains $q - 1$ of them, so there are $(q^4 - 1)/(q - 1) = (q + 1)(q^2 + 1)$ points. We'll construct an incidence structure using all of these points, but only some of the lines, in $PG(3, q)$.

Let H be the matrix⁸

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Call a subspace S of V *totally isotropic* if $u^T H v = 0$ for all u and v in S . It's easy to see that $u^T H u = 0$ for all u , so every 1-dimensional subspace of V is trivially totally isotropic. For the 2-dimensional setting, we need to count the number of u, v pairs such that $\langle u, v \rangle$ is a 2-dimensional totally isotropic subspace. There are $q^4 - 1$ choices for u , and then $q^3 - q$ choices for a vector v orthogonal to u but not in the span of u . Thus there are $(q^4 - 1)(q^3 - q)$ such pairs, and the number of 2-dimensional totally isotropic subspaces of V is $(q^2 + 1)(q + 1)$.

Geometrically, we say that $PG(3, q)$ contains $(q^2 + 1)(q + 1)$ totally isotropic points and $(q^2 + 1)(q + 1)$ totally isotropic lines. A 2-dimensional subspace contains $q + 1$ subspaces of dimension one, so each

⁸if the field has characteristic 2 (i.e. if q is even), then $1 = -1$ in \mathbb{F}

totally isotropic line contains $q + 1$ totally isotropic points. Because the numbers of points and lines are equal, this implies that each totally isotropic point is contained in $q + 1$ totally isotropic lines. Let $W(q)$ be the incidence structure whose points and lines are the totally isotropic points and lines of $PG(3, q)$.

Lemma. *This incidence structure $W(q)$ is a generalized quadrangle.*

Proof. We need to prove that given a point p and a line L not containing p there is a unique point on L collinear with p . Suppose that the point p is spanned by the vector u . Any point collinear with p is spanned by a vector in u^\perp , which is a 3-dimensional subspace which intersects the 2-dimensional subspace L at a 1-dimensional subspace, which is the unique point p' on L collinear with p .

□

If X is the incidence graph of $W(q)$, then it is bipartite on $2(q^2 + 1)(q + 1)$ vertices and $(q + 1)$ -regular. By the earlier theorem, its girth is eight and diameter is four. We will see soon that it is also distance regular. Applying this construction to \mathbb{F}_2 , we get a generalized quadrangle with fifteen points and fifteen lines. This is the same as the generalized quadrangle on the 1-factors of K_6 and is isomorphic to the Tutte 8-cage.

We can use any invertible 4×4 matrix over \mathbb{F} with zeros along the diagonal such that $H^T = -H$, but any such matrix realizes the same generalized quadrangle.

Note that not every generalized quadrangle is regular even though the ones we construct with this process are. We'll see an example in a bit.

Generalized Polygons

We've seen two classes of incidence structures equivalent to bipartite graphs with diameter d and girth $2d$ ($d = 3$ for the triangles, $d = 4$ for the quadrangles).

Definition. We can generalize this by defining a **generalized polygon** to be a finite bipartite graph with diameter d and girth $2d$, and we call this a **generalized d-gon**, and we use the canonical names for these (pentagon, hexagon, etc.).

Definition. A vertex in a generalized polygon is **thick** if its valency is at least three and **thin** otherwise. The whole polygon is thick if all its vertices are thick.

We can show that the thick generalized polygons are regular or semiregular and the ones which are not thick are subdivisions of generalized polygons. We will prove a series of lemmas on the way to this theorem.

Lemma. *If v, w are vertices in a generalized polygon and the distance $d(v, w) = m$ is strictly less than the diameter of the graph, then there is a unique path of length m from v to w .*

Proof. If not, then there is a cycle of length less than $2m$, contradicting the assumption that the girth of the graph is $2d$. □

Lemma. *If v, w are vertices in a generalized polygon X and $d(v, w)$ is equal to the diameter d , then v and w have the same valency.*

Proof. Since X is bipartite with diameter d , any v' adjacent to v has distance $d - 1$ from w . Thus by the previous lemma, there is a unique path of distance $d - 1$ from v' to w which must contain exactly one neighbor w' of w . Each such path contains a different neighbor of w , so w contains at

least as many neighbors as v , and a symmetric argument shows the inequality in the other direction, so the valencies are equal. \square

Lemma. *Every vertex in a generalized polygon X has valency at least two.*

Proof. Let C be a cycle of length $2d$ in X , which must exist as the girth of X is $2d$. Every vertex in C must have valency at least two. Let x be a vertex not on the cycle, P the shortest path joining x to C , and i the length of P . Then starting at x , traveling i steps along P , then $d - i$ steps along C is a vertex on C at distance d from x . By the previous lemma, these two vertices must have the same valency, hence x has valency at least two. \square

The next series of lemmas tells us that generalized polygons which are not thick are, for the most part, trivial modifications of thick ones.

Lemma. *Let C be a cycle of length $2d$ in a generalized polygon X . Then any two vertices at the same distance in C from a thick vertex in C have the same valency.*

Proof. Let v be a thick vertex in C and let w be its antipode in C . Since v is thick, it has at least one neighbor not in the cycle v' , so there is a path P from v' to w disjoint from C except at w , as a path using the cycle has length $d + 1$, and we know there must be a shorter path. Thus C with P forms three internally vertex-disjoint paths of length d from v to w . Consider now two vertices v_1, v_2 in C at distance h from v . Let x be the unique vertex in P at distance $d - h$ from v . Then x is at distance d from v_1 and v_2 , so these both have the same valency as x and thus each other. \square

Lemma. *The minimum distance k between any pair of thick vertices in X is a divisor of d . If d/k is odd, then all the thick vertices have the same valency. If d/k is even, then the thick vertices share at most two valencies. Further, any vertex at distance k from a thick vertex is itself a thick vertex.*

Proof. Let v and w be thick vertices of X at distance k and let x be any other thick vertex of X . Without loss of generality, suppose v closer to x than w . Then we can find a cycle C of length $2d$ which extends the path from x to v to include w and then returns to x . We can repeatedly apply the previous lemma to the thick vertices of C starting at v , which tells us that every k th vertex must be thick, hence k divides d . Further, since the antipode v' of v is thick as well, every second thick vertex in C has the same valency, again by the previous lemma every thick vertex has the same valency as either v or w , including our arbitrarily chosen thick vertex x .

If d/k is odd, then v' and w have the same valency, so transitively v and w have the same valency and every thick vertex has that valency as well. On the other hand, if d/k is even, then v and w might not have the same valency. Let x' be a vertex at distance k from x . If $x' \in C$, then it is thick for sure. Otherwise, we can form a new cycle C' of length $2d$ which includes x, x' , and one of the vertices in C at distance k from x . By the previous argument, x' must be thick in this case, too. \square

Recall the subdivision graph $S(X)$ is the one formed by adding a vertex in the middle of each edge of X . Equivalently, we can think of this as replacing each edge in X with a path of length two. In this way, we can define the k -fold subdivision graph as the one in which we replace each edge of X with a path of length k .

Theorem. *A generalized polygon which is not thick is either a cycle, the k -fold subdivision of a multiple edge (a bundle of disjoint k -paths with common endpoints), or the k -fold subdivision of a thick generalized polygon.*

Proof. If X has no thick vertices, then every vertex has valency two, hence it is a cycle.

If not, then the previous lemma tells us that any path between two thick vertices in X has length a multiple of k with every k th vertex being thick and all the others thin. Define a graph X' to be the one whose vertices are the thick vertices of X and two vertices are adjacent in X' if and only if they are joined by a path of length k in X . Clearly X is the k -fold subdivision of X' . If k is equal to the diameter of X , then two thick vertices of maximum distance are joined by a collection of k -paths of thin vertices. This collection must contain all vertices of X , so X has only two thick vertices and is thus a bundle of k -paths with common (thick) endpoints.

If $k < d$, then X' has diameter $d' = d/k$ because a path of length d between two thick vertices in X must be a k -fold subdivision of a path of length d' in X' , and a cycle of length $2d$ in X is a k -fold subdivision of a cycle of length $2d/k$ in X' . Thus X' must have diameter d' and girth $2d'$. Clearly X' must also be bipartite, as if it contained an odd cycle, any k -fold subdivision of this cycle would have a thin vertex at distance at least $kd' + 1$ from some thick vertex in X , contradicting the assumption that X has diameter d . Hence X' is a thick generalized polygon and X is its k -fold subdivision. \square

In this sense, we can restrict our study of generalized polygons to the thick ones and consider the rest as degenerate cases. The degenerate projective plane on five vertices is a 3-fold subdivision of a multiple edge. The grids and dual grids are 2-fold subdivisions of the complete bipartite graphs, which are generalized 2-gons. Although many of the proofs about generalized polygons are beyond the scope of this subject, we can state many results. The following is a famous theorem about the diameter of a generalized polygon.

Theorem (Feit and Higman). *If a generalized d -gon is thick, then d must be 3, 4, 6, or 8.*

We've already seen some thick generalized triangles and quadrangles, and there are actually a lot of these. Generalized hexagons and octagons exist, but only a few families are known, and even the simplest are hard to describe.

Since a projective plane is a generalized thick triangle, it's regular. If all vertices have valency $s + 1$, then we say the projective plane has order s . The other thick generalized polygons are either regular or semiregular. If the valencies in a thick generalized polygon X are $s + 1$ or $t + 1$, then we say it has order (s, t) . These may be equal.

Lemma. *If a generalized polygon is regular, it is distance regular.*

The order of a thick generalized polygon satisfies a few inequalities:

Theorem (Higman and Haemers). *Let X be a thick generalized d -gon of order (s, t) .*

- a) *If $d = 4$, then $s \leq t^2$ and $t \leq s^2$.*
- b) *If $d = 6$, then st is a square and $s \leq t^3$ and $t \leq s^3$.*
- c) *If $d = 8$, then $2st$ is a square and $s \leq t^2$ and $t \leq s^2$.*

It is possible to take a generalized polygon of order (s, s) and subdivide each edge to create a generalized polygon of order $(1, s)$. Hence we can create a generalized 12-gon which is neither a cycle nor thick.

Two Generalized Hexagons

Although we know there is an infinite family of generalized hexagons, it's not actually that easy to cook one up. We'll show the construction of a (the smallest!) thick generalized hexagon.

The smallest thick generalized hexagon has order $(2, 2)$ and is cubic with girth six and diameter 12. It is distance regular with intersection array $\{3, 2, 2, 2, 2, 2; 1, 1, 1, 1, 1, 3\}$. Given this array, we can count the vertices in each cell of the distance partition for any starting vertex u . We know that $|X_1(u)| = 3$ so there are six edges between $X_1(u)$ and $X_2(u)$, and since each vertex of $X_2(u)$ is adjacent to one vertex in $X_1(u)$, we can see that $|X_2(u)| = 6$. Continuing, we get that the sizes of the cells starting at $X_0(u)$ are 1, 3, 6, 12, 24, 48, and 32.

Theorem. *If X is a generalized hexagon of order $(2, 2)$, then the graph $X_5(u) \cup X_6(u)$ is the subdivision $S(Y)$ of a cubic graph Y on 32 vertices.*

Proof. The 48 vertices in $X_5(u)$ are each adjacent to two of the 32 vertices in $X_6(u)$, and each vertex of $X_6(u)$ is adjacent to three from $X_5(u)$. From here it is clear that we can construct a cubic graph Y using the vertices of $X_6(u)$ as vertices and the vertices from $X_5(u)$ as the edges. Subdividing Y completes the construction. \square

Given this cubic graph Y on 32 vertices, we can construct a generalized hexagon by specifying which vertex of $X_5(u)$ subdivides which edge of Y . First, we encode the vertices of $X_5(u)$. Let the three vertices adjacent to u be labeled r, g, b , respectively. Each of these has two neighbors in $X_2(u)$, call them $r0, r1, b0, b1, g0, g1$. Then the two neighbors of $r0$ in $X_3(u)$ are $r00, r01$. Continuing like this, we can identify each vertex in $X_5(u)$ with one of r, g, b followed by a 4-bit binary string.

Lemma. *For $c \in \{r, g, b\}$, the 16 edges of Y subdivided by the 16 vertices of $X_5(u)$ with first entry c form a 1-factor in Y .*

Proof. The distance from $c \in \{r, g, b\}$ to any vertex of $X_5(u)$ with first entry c is exactly four, so there is a path of length at most eight between any two vertices in $X_5(u)$ with first entry c . Since X has girth 12, there is no cycle of length 10, so two such vertices cannot subdivide incident edges of Y , hence they form a 1-factor. \square

The figure shows a bipartite cubic graph on 32 vertices with the 1-factorization given by the three colors r, g, b . We draw this graph on a torus with opposite sides of the hexagon identified.

For the moment, let's define the distance between two edges of a graph to be the distance that the corresponding vertices have in the subdivision graph. Thus incident edges have distance two, and an edge has distance zero from itself.

Theorem. *Let Y be the graph above and let R be the set of edges in one color class. Then for every edge $e \in R$, there is a unique edge $e' \in R$ at distance 10 from e . Furthermore:*

- a) *There is a unique partition of the eight pairs $\{e, e'\}$ into four quartets of edges with pairwise distance at least eight.*
- b) *There is a unique partition of these four pairings into two octets with pairwise distance at least six.*

Proof. The rare proof-by-picture! (I'll include this later when I come back with the figures...) \square

We can subdivide the edges of Y to form a generalized hexagon in a way that is clear now. The edges in each color class R are assigned to the vertices of $X_5(u)$ with the corresponding first element in their identifier string. The two octets of edges are assigned to the two octets of vertices whose strings agree in the first two positions, the four quartets to the vertices whose strings agree in the first three positions, and the eight pairs to those whose strings agree in the first four positions. Then the two edges of a pair are subdivided arbitrarily by the two vertices to which the pair is assigned. We repeat for each color class.

The resulting graph is bipartite and has no cycle of length less than 12, and its diameter is six.

The automorphism group of this generalized hexagon does not act transitively on the vertices, but rather has two orbits which correspond to the bipartition. The distance partition from a vertex v in the opposite class as u has $X_5(v) \cup X_6(v)$ a subdivision of a different graph than the one induced by u . In fact, it is the subdivision of a disconnected graph, each of which has a component which looks like the following:

These components together are the dual of our generalized hexagon. It turns out that there are only two possibilities for the graph constructed this way, and we have now seen both of them. These are the unique dual pair of generalized hexagons of order $(2, 2)$.

Moore Graphs

Definition. A **Moore graph** is a graph with diameter d and girth $d + 1$. The graphs C_5 (all the odd cycles), the Petersen graph, and the complete graphs on at least three vertices are all Moore graphs. A major result of algebraic graph theory is that there are at most two more Moore graphs, one of which we'll see soon and one which may or may not exist.

Lemma. *Let X be a Moore graph. Then X is regular.*

Proof. First we'll show that any vertices at distance d have the same valency then use this to show that the graph is regular. Let v and w be vertices of X at distance d and let P be the path of length d joining them. Let v' be any neighbor of v not on P . Then the distance from v' to w must be at least d and at most d , so there is a unique path P' of length d from v' to w which must meet a neighbor w' of w not on P . Each such neighbor of v thus corresponds to a different neighbor of w , and going in the other direction, v and w must have the same number of neighbors.

Let C be a cycle of length $2d + 1$. If we take two walks of d steps around C from some vertex v , we arrive at a neighbor v' of v , which by the first part has the same valency as v , and taking our two walks in the other direction tells us that the other neighbor of v on C does as well. transitively, we can see that every vertex on C has the same valency. Given any vertex x not on C , we can form some path of length $i < d$ to C . Then there is a vertex $d - i$ steps along C which is at distance d from x , so x also has the same valency as every vertex on the cycle. Hence X is regular. \square

Theorem. *Moore graphs are distance regular.*

Proof. Let X be a Moore graph of diameter d . By the previous lemma, X is regular, so let k be its valency. To show X is distance regular, it is sufficient to show that the distance numbers a_i, b_i, c_i are well-defined.

Let v be a vertex of X and let $X_1(v), \dots, X_d(v)$ be the cells of the distance partition. Since for each vertex $w \in X_i(v)$ there is a unique path of length i from v to w , the proof is fairly straightforward.

For any i such that $1 \leq i < d$, a vertex $w \in X_i(v)$ cannot have two neighbors in the preceding cell, because otherwise we could find a cycle of length $2i$ through v and w , but since X is regular, w must have at least one neighbor in the preceding cell, hence $c_i = 1$ for all $1 \leq i \leq d$. Similarly, w cannot have a neighbor in the same cell, otherwise we could find a cycle of length $2i + 1$ through v , w , and this neighbor. Hence $a_i = 0$ for $1 \leq i < d$. Since X is regular, we get that $b_0 = k$ and $b_i = k - 1$ for $1 \leq i \leq d$. Hence these values are all well-defined and X is distance regular. \square

The theory of distance regular graphs can be used to show that Moore graphs of diameter greater

than two do not exist, and that if one does, it must have valency 2, 3, 7, or 57. A lot of this comes from the theory of strongly regular graphs, which is the topic of Chapter 10. The odd cycles have valency two, the Peterson graph has valency three, and we are about to construct a Moore graph with valency seven. The existence of the one of valency 57 is an open question.⁹

The Hoffman-Singleton Graph

The *Hoffman-Singleton graph* is the Moore graph with valency seven. Here we provide a construction. It has 50 vertices, as we can count the vertices at distance one and two from a fixed vertex to get cell sizes $1 + 7 + 42 = 50$.

Lemma. *An independent set C in a Moore graph of diameter two and valency seven contains at most 15 vertices, and if it contains exactly 15, then every vertex not in C has exactly three neighbors in C .*

Proof. Let X be such a Moore graph. Let C be an independent set of size c . Without loss of generality, we can label the vertices of X such that $\{1, 2, 3, \dots, 50 - c\}$ are the vertices not in C . If i is a vertex not in C , let k_i denote the number of its neighbors in C . Since no two vertices in C are adjacent in X , we know that $7c = \sum_{i=1}^{50-c} k_i$.

Now consider the paths of length two joining two vertices in C . Since every pair of non-adjacent vertices in X has exactly one common neighbor, combinatorially, we can see that $\binom{c}{2} = \sum_{i=1}^{50-c} \binom{k_i}{2}$.

From these two equations, we can see that for any real number μ ,

$$\sum_{i=1}^{50-c} (k_i - \mu)^2 = (50 - c)\mu^2 - 14c\mu + c^2 + 6c$$

and as the right side must be non-negative for all values of μ , so as a quadratic in μ , it has at most one real root. Thus the discriminant

$$196c^2 - 4(50 - c)(c^2 + 6c) = 4c(c - 15)(c + 20)$$

of the quadratic must be less than or equal to zero. Therefore we need for $c \leq 15$, which proves the first part of the theorem.

If $c = 15$, then the right side of our quadratic becomes

$$35\mu^2 - 210\mu + 315 = 35(\mu - 3)^3$$

so setting $\mu = 3$ on the left side gives us $\sum_{i=1}^3 5(k_i - 3)^2 = 0$, which happens exactly when all the k_i are equal to three, and we are done. \square

Now we can describe the construction, using the idea of heptads from Chapter 4. Recall that there are 35 triples from the set $\Omega = \{1, 2, \dots, 7\}$. A *heptad* is a set of seven triples such that each pair meet in exactly one point and there is no point in every triple. We call a set of triples *concurrent* if there is a point common to all and that the intersection of any two is only this point. A *triad* is a set of three concurrent triples.

⁹From Wikipedia, we know that it has 3250 vertices and its automorphism group has order at most 375.

Claim. No two distinct heptads have three nonconcurrent triples in common.

Proof. For each set of nonconcurrent triples, we can check that there is a unique heptad containing it. \square

Claim. Each triad is contained in exactly two heptads.

Proof. Without loss of generality, let 123, 145, 167 be our triad. There are two heptads containing this triad: 123, 145, 167, 246, 257, 347, 356 and 123, 145, 167, 247, 256, 346, 357. Applying the permutation (67) to the first yields the second. \square

Claim. There are exactly 30 heptads

Proof. There are 15 triads for each point, so there are 210 pairs consisting of a triad and a heptad which contains it. Since each heptad contains exactly seven triads, there must be 30 heptads. \square

Claim. Any pair of heptads must have 0, 1, or 3 triples in common.

Proof. If two heptads share four or more triples, then they have three nonconcurrent triples in common, so 3 is an upper bound on the number of shared triples. If two triples meet in exactly one point, there is a third triple which is concurrent with them, and this third triple is unique. Thus any heptad containing the first two must contain the third. \square

Claim. The automorphism group of a heptad has order 168 and is a subgroup of the alternating group on seven elements.

Proof. Since $Sym(7)$ acts transitively on the set of heptads and there are 30 heptads, the subgroup of $Sym(7)$ which fixes a heptad has order $168 = 7!/30$. We previously exhibited a subset of the even permutations which satisfies this. \square

Claim. The heptads form two orbits of length 15 under the action of the alternating group $Alt(7)$. Any two heptads in the same orbit have exactly one triple in common.

Proof. Since the subgroup of $Alt(7)$ fixing a heptad has order 168, the number of heptads in an orbit must be 15. Let Π be the first of the two heptads in the above claim about each triad being in exactly two heptads. The permutations (123) and (132) are both in $Alt(7)$ and map Π onto two distinct heptads which have exactly one triple in common with Π (the triple 123). From each triple in Π , we can find two 3-cycles in $Alt(7)$ which preserves exactly this triple. Since there are 15 heptads in an orbit and since all heptads in an orbit are equivalent, any two heptads in the orbit must share exactly one triple. \square

Claim. Each triple in Ω lies in exactly six heptads, three from each orbit.

Proof. Just count them. \square

Now we can construct the Hoffman-Singleton graph. Choose an orbit of heptads. The vertices of the graph are the heptads with the 35 triples in Ω . A heptad is joined to a triple if and only if it contains the triple. Two triples are adjacent if and only if they are disjoint. The heptads form an independent set of size 15, the diameter of the graph is two, it contains a 5-cycle, and 50 vertices.

Designs

Returning to incidence structures, another interesting class is the collection of t -designs. In general, these are not partial linear spaces, and the term ‘block’ is often used in place of ‘line’.

Definition. A t – (v, k, λ_t) **design** is a set \mathcal{P} of v points with a collection \mathcal{B} of k -subsets of points, called blocks, such that every t -set of points lies in exactly λ_t blocks. The projective planes $PG(2, q)$ have the property that every pair of points lie in a unique block, so these are examples of $2 - (q^2 + q + 1, q + 1, 1)$ designs.

Suppose that \mathcal{D} is a t – (v, k, λ_t) design and let S be a set of s points for $s < t$. We can count the number of blocks λ_s of \mathcal{D} containing S . We will do this combinatorially, by counting in two ways the pairs of (T, B) such that T is a t -set containing S and B is a block containing T .

First, S lies in $\binom{v-s}{t-s}$ t -subsets T , each of which lies in λ_t blocks. Also, for each block containing S , there are $\binom{k-s}{t-s}$ choices for T , so

$$\lambda_s \binom{k-s}{t-s} = \lambda_t \binom{v-s}{t-s}$$

and since the number of blocks doesn’t depend on the choice of S , we can see that \mathcal{D} is also an s – (v, k, λ_s) design. This also tells us that λ_s must be an integer for all $s \leq t$.

The value λ_0 is the total number of blocks in the design, and we typically denote it b . Plugging in $s = 0$ above gives us

$$b \binom{k}{t} = \lambda_t \binom{v}{t}$$

The value λ_1 is the number of blocks containing each point, and is typically called the *replication number* and denoted r . Plugging in $t = 1$ above gives us $bk = vr$.

If $\lambda_t = 1$, then the design is called a *Steiner system*, and a 2-design with $\lambda_2 = 1$ and $k = 3$ is called a *Steiner triple system*. The projective plane $PG(2, 2)$ is a 2– $(7, 3, 1)$ design, and is thus a Steiner triple system. This object is usually called the *Fano plane* and drawn as follows, where the blocks are the straight lines and curves on the central circle.

The *incidence matrix* of a design is the matrix N with rows and columns indexed by points and blocks, respectively. The entry $N_{ij} = 1$ if and only if the i th point lies in the j th block, and $N_{ij} = 0$ otherwise. The matrix N has fixed row and column sums, and satisfies

$$NN^T = (r - \lambda_2)I + \lambda_2 J$$

where I is the identity matrix and J is the matrix of all ones. Conversely, any binary matrix with constant row and column sums which satisfies this equation is the incidence matrix of some 2-design.

Lemma. In a 2-design with $k < v$, we have $b \geq v$.

Proof. Putting $t = 2$ and $s = 1$ into the equation relating λ_s and λ_t , we get $r(k - 1) = (v - 1)\lambda_2$. Thus $k < v$ implies $r - \lambda_2 > 0$. Since $(r - \lambda_2)I$ is positive definite and $\lambda_2 J$ is positive semidefinite, their sum is positive semidefinite, so NN^T is invertible. Thus the rows of N must be linearly independent, so $b \geq v$. \square

A 2-design in which $b = v$ is called *symmetric*. The dual of a 1-design is a 1-design, but in general the dual of a 2-design is not a 2-design.

Lemma. *The dual \mathcal{D}^* of a symmetric design \mathcal{D} is a symmetric design with the same parameters.*

Proof. If N is the incidence matrix of \mathcal{D} , then N^T is the incidence matrix of \mathcal{D}^* . Since \mathcal{D} is a 2-design, we have $NN^T = (r - \lambda_2)I + \lambda_2 J$, so $N^T = N^{-1}((r - \lambda_2)I + \lambda_2 J)$. Since \mathcal{D} is symmetric, $r = k$, so N commutes with both I and J . Thus $N^T N = (r - \lambda_2)I + \lambda_2 J$ and thus \mathcal{D}^* is a 2-design with the same parameters as \mathcal{D} . \square

Theorem. *A bipartite graph is the incidence graph of a symmetric 2-design if and only if it is distance regular with diameter three.*

Proof. Let \mathcal{D} be a symmetric $2-(v, k, \lambda_2)$ design with incidence graph X . Any two points lie at distance two in X , and the same is true of any two blocks. Thus any point is at distance three from a block it doesn't lie on, and a block is at distance three from a point not on it, so X has diameter three.

Now consider the distance partition from some point. It is clear that X is bipartite, so $a_1 = a_2 = a_3 = 0$. Since two points lie in λ_2 blocks, we have that $c_2 = \lambda_2$ and since $r = k$, we get that the intersection array for X looks like

$$\begin{Bmatrix} - & 1 & \lambda_2 & k \\ 0 & 0 & 0 & 0 \\ k & k-1 & k-\lambda_2 & - \end{Bmatrix}$$

Since we know that the dual \mathcal{D}^* of \mathcal{D} is a design with the same parameters, the distance partition from a block yields the same intersection numbers, thus X is distance regular.

For the other direction, let X be a bipartite distance regular graph with diameter three. Declare one class of vertices to be the points and the other the blocks. Considering the distance partition from some point, we can see that each point lies in b_0 blocks and every two points lie in c_2 blocks. Thus we have a 2-design with $r = b_0$ and $\lambda_2 = c_2$. Now looking at the distance partition from some block, we have that every block contains b_0 points and every two blocks meet at c_2 points. Thus we have a 2-design where $k = b_0 = r$, so $b = v$. \square

Since projective planes are symmetric designs, this is another proof of the lemma which tells us that regular generalized polygons are distance regular for the case of generalized polygons of diameter three. The incidence graph of the Fano plane is called the Heawood graph, which if we remember from way back when, is the dual of K_7 .

Another way to build a graph from a design is to consider the *block graph* in which the vertices are blocks of \mathcal{D} and two vertices are adjacent if the blocks intersect. In general, blocks can meet in different numbers of points, which gives rise to some interesting graphs.

Theorem. *The block graph of a Steiner triple system with $v > 7$ is distance regular with diameter two.*

Proof. Let \mathcal{D} be a $2-(v, 3, 1)$ design and let X be the block graph of \mathcal{D} . Every point lies in $(v-1)/2$ blocks, so X is regular with valency $3(v-1)/2$. If we consider two blocks which intersect, there are $(v-5)/2$ further blocks through that point of intersection, and four blocks containing a pair of points, one from each block, other than the point of intersection. Thus $a_1 = (v-5)/2 + 4 = (v+2)/2$.

If we look at two blocks which do not intersect, then there are nine blocks containing a pair of points, one from each block, and thus $c_2 = 9$. Thus the diameter of the graph is two. Computing the remainder of the intersection numbers completes the proof that X is regular. \square