Algebraic Graph Theory

Notes by Zach Schutzman

University of Pennsylvania, Fall 2017

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 $\phi : V(X) \to V(Y)$ 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 $X \to X$.

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

[1] Not 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 isomoprhic (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. □

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 $d(x, y) \lneq d(x^g, y^g)$. Then there is some path $x, r_2, r_3, \ldots r_{n-1}, y$ 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 $d(x, y) \gneq d(x^g, y^g)$.

□

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, $g \in Aut(\overline{X})$. □

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 $\phi : V(X) \to V(Y)$ 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 $X \to K_2$ 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 $\phi : V(X) \to V(Y)$ is a homomorphism. For $y \in V(Y)$, define $\phi^{-1}(y)$ to be $\phi^{-1}(y) = \{x \in V(X) | \phi(x) = y\}$, 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. □

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 $j - i \equiv \pm 1 \mod n$.

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 $Aut(C_n)$. 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 $-i \mod n$ is an element of $Aut(C_n)$. 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 $Aut(C_n)$ 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 $C \subset \mathbb{Z}_n \backslash 0$, 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 $X(\mathbb{Z}_m, C)$ 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 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 $v \leq k \leq i$, then $Aut(J(v,k,i))$ contains a subgroup isomorphic to $Sym(v)$.*

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 $J(v, k, i)$. □

We note that $Aut(J(v, k, i))$ acts on a set of size $\binom{v}{k}$, so when this quantity is not equal to v, it's not equal to $Sym(v)$, 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 $2k - 2$. □

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 $S_1, S_2, \ldots, S_k$ be the cliques, and let $v_1, v_2, \ldots, v_m$ be the vertices (if there are any) which are in exactly one S_i. The vertex set of our graph will be $S_1, \ldots, S_k, \{v_1\}, \ldots \{v_m\}$ 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.

□

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 $f : X \to L(X)$ and $g : Y \to L(Y)$ 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 $g \circ \phi \circ f^{-1} : L(X) \to L(Y)$ 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. □

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.

□

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. □

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.

□

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 $\mathbb{R}\mathrm{P}^2$ 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 $\mathbb{R}\mathrm{P}^2$ (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 injective[2].

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 $g \restriction S$ to denote the restriction of g to S. Then the map $g \mapsto g \restriction S$ is a group homomorphism from G into $Sym(S)$, and the image is a permutation group in S, which we write $G \restriction S$ 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 $G \restriction S$ 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

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

$$G_{x_1,x_2,\dots x_r} = \bigcap_1^r G_{x_i}$$

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

Lemma (Burnside[3])**.** *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 $\sum\limits_{g \in G} |fix(g)|$ 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 $\sum\limits_{x \in V} |G_x|$.

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.

□

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. *The size of the isomorphism class of a graph X on n vertices is $\frac{n!}{|Aut(X)|}$.*

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 $Sym(V)$. □

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

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

If every graph were to be asymmetric (we know this isn't the case), we would have that each

[3] This 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.

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 $orb_2(g)$ 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 $orb_2(g) = \binom{n}{2} - r(n-r-1)$.

Now, we're going to partition the permutations in $Sym(n)$ 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 $Sym(n)$ 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 $|\mathcal{C}_3| \leq n! \leq n^n$

□