# 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 $r^g_{n-1}$ 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 $\phi$. 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 $\phi$. 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 $\phi$ 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 $C_n = \{0, 1, 2, \ldots n-1\}$ 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 $\Omega$ be some fixed set of size $v$. The vertices of $J(v, k, i)$ are the subsets of $\Omega$ 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 $\Omega$ 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 $Aut(J(v, k, i))$ contains a subgroup isomorphic to $Sym(v)$.*

*Proof.* Let $g$ be a permutation of $\Omega$ 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 $Aut(J(v, k, i))$ 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 $2k - 2$. $\square$

**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 $S_1, S_2, \ldots, S_k$ 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.

$\square$

*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 $f : X \to L(X)$ and $g : Y \to L(Y)$ be these functions.

If we assume $X \cong Y$ by $\phi$, 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 $x_1, x_2, \ldots x_r$ are distinct elements of $V$, then the stabilizer

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

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

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 $\{x_1, x_2, \ldots, x_r\}$. 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 $\sum_{g \in G} |fix(g)|$ 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.

□

## 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 $Sym(V)$. □

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

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

[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.

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 $orb_2(g)$ 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 $|\mathcal{C}_3| \leq n! \leq n^n$

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 $c > 4$)

$$\begin{aligned}
\sum_{g \in Sym(V)} 2^{orb_2(g)} &\leq 2^{\binom{n}{2}} + n^m 2^{\binom{n}{2}-(n-2)} + n^n 2^{\binom{n}{2}-\frac{nm}{4}} \\
&= 2^{\binom{n}{2}} \left(1 + n^m 2^{-(n-2)} + n^n 2^{-\frac{nm}{4}}\right) \\
&= 2^{\binom{n}{2}} \left(1 + 2^{m \log n - n + 2} + 2^{n \log n - nm/4}\right) \\
&= 2^{\binom{n}{2}} (1 + o(1))
\end{aligned}$$

□

**Lemma.** *Almost all graphs are asymmetric.*

*Proof.* Suppose the proportion of isomorphism classes of graphs which are asymmetric is $\mu$. 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 $\infty$, $\mu$ 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 $\infty$.

$\square$

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 $\Omega$ as $\Omega^T$, which is the set $\{(y,x)|(x,y) \in \Omega\}$.

**Claim.** $\Omega$ is $G$-invariant if and only if $\Omega^T$ 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 $\Omega$ and $\Omega^T$.

Suppose $\Omega$ is $G$-invariant. Then any element of $G$ sends something in $\Omega$ to something else in $\Omega$. 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 $\Omega$, then $(y,x)$ and $(y^g,x^g)$ are in $\Omega^T$, so $\Omega^T$ is $G$-invariant as well. $\square$

It follows from this fact that if $\Omega$ is an orbital, then $\Omega^T = \Omega$ or $\Omega^T \cap \Omega = \varnothing$. That is, an orbital either contains all of the diagonal or none of it. If $\Omega = \Omega^T$, we call $\Omega$ 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 $\Omega$ be an orbit of $G$ on $V \times V$ and denote $Y_\Omega$ the set $\{y|(x,y) \in \Omega\}$. We will show that $Y_\Omega$ is an orbit of $G_x$ acting on $V$. If $y$ and $y'$ are in $Y_\Omega$, then $(x,y)$ and $(x,y')$ are in $\Omega$, 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 $Y_\Omega$ is an orbit of $G_x$. Since $V$ is partitioned by the sets $Y_\Omega$ as we let $\Omega$ range over all the orbits of $V \times V$, we are done.

$\square$

This tells us that for any $x \in V$, each orbit $\Omega$ 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 $\Omega$ is a symmetric orbit, the corresponding $G_x$ is called *self-paired*. Each orbit $\Omega$ can be thought of as a directed graph with vertices $V$ and arcs $\Omega$. When $\Omega$ 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 $\Omega$ be an orbit of $G$ on $V \times V$, and let $(x, y) \in \Omega$. Then $\Omega$ 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 $\Omega$, 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 $\Omega$, it follows that $\Omega = \Omega^T$, as we know $\Omega \cap \Omega^T \neq \varnothing$. □

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 $G = Sym(7)$ 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 $Sym(8)$ (and therefore $Sym(7)$, properly).*

*Proof.* There are 35 partitions of the set $\{0, 1, \ldots, 7\}$ 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 $Aut(X)$ contains a subgroup isomorphic to $Sym(8)$, 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 $Aut(X)$ contains $Sym(8)$ as a subgroup, $J(7, 3, 1)$ does as well, and we are done.

□

## 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 $S \cap S^g = \varnothing$. 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 $Aut(Q)$ 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 $g \in Aut(Q)$ be any group element, then either $S^g = S$ or $S \cap S^g = \varnothing$, 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 $Aut(Q)$, 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 **primitive**.

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 $D_1, D_2, \ldots, D_r$ 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 $D_1, D_2, \ldots, D_r$ 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 $\Omega$ be an orbit of $G$ on $V \times V$ which is not symmetric. Then $\Omega$ corresponds to an oriented graph, and $G$ acts transitively on its vertices. Thus, every vertex in $\Omega$ 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, $\Omega$ 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 $B_1, B_2, \ldots, B_r$ is a system of imprimitivity. Let $x, y$ be distinct points in $B_1$. and let $\Omega$ 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 $\Omega$ joins vertices corresponding to points in the same block, so $\Omega$ is not connected.

Conversely, let $\Omega$ 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.

$\square$

# 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 $\rho_{y-x}$. 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 $2^k k!$. □

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 $\rho_g$ 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 may 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 $Sym(v)$ 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 $Aut(X)$ 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 $Aut(X)$ 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 $Aut(X)$ 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 $Aut(X)$. 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 $G = Aut(X)$ and suppose that $x$ and $y$ are adjacent vertices in $X$. Let $\Omega$ 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 $\Omega$, so $\Omega$ is not symmetric. Thus, $X$ is the graph with edges $\Omega \cup \Omega^T$. Because the out-valency of $x$ is the same in $\Omega$ and $\Omega^T$, 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 $\partial A$ to be the set of vertices with one end in $A$ and one end not in $A$. If $A = \varnothing$ or $A = V(X)$, then $\partial A = \varnothing$. The edge connectivity of $X$ is the minimum size of $\partial A$ 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 $\kappa = \kappa_1 9X)$ and let $A$ and $B$ be distinct edge atoms in $X$. If $A \cup B = V(X)$, them 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 $A \cap B = 0$. 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 $A \cap B \neq \varnothing$, 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 $Aut(X)$, and by Exercise 2.13, it follows that the subgraph of $X$ induced by $A$ is regular, so let its valency be $\ell$.

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. □

## 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 $v$. □

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, $A$ 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).

$\square$

**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 deonte

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

. 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)** $\overline{A} \cap \overline{B} \neq \varnothing$.

From (a) and (b), we have that $|A \cup B| + |N(A \cup B)| < n$, so $\overline{A \cup B} \neq \varnothing$, 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.

$\square$

**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. $\square$

*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 singe vetex, then $|N(A)| = k$ and we are done. Suppose $|A| \geq 2$. If $g \in Aut(X)$, 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 $Aut(X)$, 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 $Aut(X)$ 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 $\overline{A} = \varnothing$, contradicting the assumption that $A$ is a fragment. $\square$

## 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, we 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 $M$ s 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 maximim 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 $v$. □

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 $Aut(X)$. 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 $g \in Aut(X)$, 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 $Aut(X)$ 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 $Y_1, Y_2, \ldots, Y_r$ 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. □

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 $G = Aut(X)$. 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. □

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 $\rho_g$ 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 $Aut(X(G, C))$ 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. □

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 $C = \{g_v | (u, v) \in E(X)\}$. If $x$ and $y$ are vertices of $X$, since $g_x \in Aut(X)$, $x$ 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 $G \setminus \{e\}$. □

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 $\theta : G \to G$ 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 $\theta$ 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 $\theta$ 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 $\alpha$ and $\beta$ 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 mulitplication on $G$ that $\alpha$ and $\beta$ have $k$ and $\ell$ 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 $\ell$ all have the same parity.*

*Proof.* Suppose $V(X)$ has a partition into $r$ directed cycles, and define the permutation $\pi$ of $G$ to be $x^\pi = y$ if the arc $(x, y)$ is in one of the directed cycles, that is, $\pi$ '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 $\alpha$ and $\beta$ were chosen to be distinct.

Let $\tau$ be the permutation in $G$ such that $x^\tau = \beta^{-1}x^\pi$. Clearly $\tau$ 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, $\tau$ 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 $\ell, k, r$ all have the same parity.

$\square$

The symmetric group on $n$ elements can be generated by two permutations: $(12)$ and $(123\ldots n)$. 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 $|Sym(4)| = 24$, $\alpha$ and $\beta$ 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 $X(n) = X(Sym(n), \{(12),(123\ldots n)\})$.

**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 $\alpha$ has $\frac{n!}{2}$ cycles in its action by left multiplication and $(123\ldots n)$ has $(n-1!)$, but $(123\ldots n)^{-1}(12)$ has order $n-1$, so since we can only partition $V(X)$ into an even number of directed cycles, we are done. $\square$

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 $f \restriction Y$ of $f$ to $Y$ is the identity map on the vertices in $Y$. It's even enough to only require that $f \restriction Y$ 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 $C = \{g \in G | (x, x^g) \in E(X)\}$, 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 $G_xCG_x \subset C$, and since $e \in G_x$, $C \subset G_xCG_x$, so $C = G_xCG_x$.

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 $Y$. $\square$

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 $\{1, 2, 3, \ldots, n\}$. 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 $\ell$ 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 $X(Sym(n), \mathcal{T})$ 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 $Sym(n)$.

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

**Lemma.** *Let $\mathcal{T}$ be a set of transpositions in $Sym(n)$, 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 $X(Sym(n), \mathcal{T})$ if $gh \neq hg$ and exactly two common neighbors otherwise.*

**Lemma.** *The neighbors of a vertex $g$ in $X(Sym(n), \mathcal{T})$ 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 $Sym(n)$. If the graph of $\mathcal{T}$ is asymmetric, the groups $Aut(X(Sym(n), \mathcal{T}))$ and $Sym(n)$ 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 $X(Sym(n), \mathcal{T})$, or equivalently those transpositions in $\mathcal{T}$ which have overlapping support. Thus $X(Sym(n), \mathcal{T})$ determines the line graph of $T$. Since $T$ is a tree, it is determined by its line graph.

Any (non-identity) element $g \in Aut(X(Sym(n), \mathcal{T}))$ 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 $g \in Aut(X(Sym(n), \mathcal{T}))$ 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 $X(Sym(n), \mathcal{T})$ 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 $X(Sym(n), \mathcal{T})$ must be exactly $Sym(n)$. □

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