2
Groups

The automorphism group of a graph is very naturally viewed as a group of permutations of its vertices, and so we now present some basic information about permutation groups. This includes some simple but very useful counting results, which we will use to show that the proportion of graphs on n vertices that have nontrivial automorphism group tends to zero as n tends to infinity. (This is often expressed by the expression "almost all graphs are asymmetric.") For a group theorist this result might be a disappointment, but we take its lesson to be that interesting interactions between groups and graphs should be looked for where the automorphism groups are large. Consequently, we also take the time here to develop some of the basic properties of transitive groups.

2.1 Permutation Groups

The set of all permutations of a set V is denoted by $\mathrm{Sym}(V)$, or just $\mathrm{Sym}(n)$ when $|V| = n$. A *permutation group* on V is a subgroup of $\mathrm{Sym}(V)$. If X is a graph with vertex set V, then we can view each automorphism as a permutation of V, and so $\mathrm{Aut}(X)$ is a permutation group.

A *permutation representation* of a group G is a homomorphism from G into $\mathrm{Sym}(V)$ for some set V. A permutation representation is also referred to as an *action* of G on the set V, in which case we say that G acts on V. A representation is *faithful* if its kernel is the identity group.

A group G acting on a set V induces a number of other actions. If S is a subset of V, then for any element $g \in G$, the translate S^g is again a subset of V. Thus each element of G determines a permutation of the subsets of V, and so we have an action of G on the power set 2^V. We can be more precise than this by noting that $|S^g| = |S|$. Thus for any fixed k, the action of G on V induces an action of G on the k-subsets of V. Similarly, the action of G on V induces an action of G on the ordered k-tuples of elements of V.

Suppose G is a permutation group on the set V. A subset S of V is G-*invariant* if $s^g \in S$ for all points s of S and elements g of G. If S is invariant under G, then each element $g \in G$ permutes the elements of S. Let $g \restriction S$ denote the *restriction* of the permutation g to S. Then the mapping

$$g \mapsto g \restriction S$$

is a homomorphism from G into $\mathrm{Sym}(S)$, and the image of G under this homomorphism is a permutation group on S, which we denote by $G \restriction S$. (It would be more usual to use G^S.)

A permutation group G on V is *transitive* if given any two points x and y from V there is an element $g \in G$ such that $x^g = y$. A G-invariant subset S of V is an *orbit* of G if $G \restriction S$ is transitive on S. For any $x \in V$, it is straightforward to check that the set

$$x^G := \{x^g : g \in G\}$$

is an orbit of G. Now, if $y \in x^G$, then $y^G = x^G$, and if $y \notin x^G$, then $y^G \cap x^G = \emptyset$, so each point lies in a unique orbit of G, and the orbits of G partition V. Any G-invariant subset of V is a union of orbits of G (and in fact, we could define an orbit to be a minimal G-invariant subset of V).

2.2 Counting

Let G be a permutation group on V. For any $x \in V$ the *stabilizer* G_x of x is the set of all permutations $g \in G$ such that $x^g = x$. It is easy to see that G_x is a subgroup of G. If $x_1, \dots, x_r$ are distinct elements of V, then

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

Thus this intersection is the subgroup of G formed by the elements that fix x_i for all i; to emphasize this it is called the *pointwise stabilizer* of $\{x_1, \dots, x_r\}$. If S is a subset of V, then the stabilizer G_S of S is the set of all permutations g such that $S^g = S$. Because here we are not insisting that every element of S be fixed this is sometimes called the *setwise stabilizer* of S. If $S = \{x_1, \dots, x_r\}$, then $G_{x_1,\dots,x_r}$ is a subgroup of G_S.

Lemma 2.2.1 *Let G be a permutation group acting on V and let S be an orbit of G. If x and y are elements of S, the set of permutations in G that* *map x to y is a right coset of G_x. Conversely, all elements in a right coset of G_x map x to the same point in S.*

Proof. Since G is transitive on S, it contains an element, g say, such that $x^g = y$. Now suppose that $h \in G$ and $x^h = y$. Then $x^g = x^h$, whence $x^{hg^{-1}} = x$. Therefore, $hg^{-1} \in G_x$ and $h \in G_x g$. Consequently, all elements mapping x to y belong to the coset $G_x g$.

For the converse we must show that every element of $G_x g$ maps x to the same point. Every element of $G_x g$ has the form hg for some element $h \in G_x$. Since $x^{hg} = (x^h)^g = x^g$, it follows that all the elements of $G_x g$ map x to x^g. □

There is a simple but very useful consequence of this, known as the orbit-stabilizer lemma.

Lemma 2.2.2 (Orbit-stabilizer) *Let G be a permutation group acting on V and let x be a point in V. Then*

$$|G_x| \left|x^G\right| = |G|$$

Proof. By the previous lemma, the points of the orbit x^G correspond bijectively with the right cosets of G_x. Hence the elements of G can be partitioned into $\left|x^G\right|$ cosets, each containing $|G_x|$ elements of G. □

In view of the above it is natural to wonder how G_x and G_y are related if x and y are distinct points in an orbit of G. To answer this we first need some more terminology. An element of the group G that can be written in the form $g^{-1}hg$ is said to be *conjugate* to h, and the set of all elements of G conjugate to h is the *conjugacy class* of h. Given any element $g \in G$, the mapping $\tau_g : h \mapsto g^{-1}hg$ is a permutation of the elements of G. The set of all such mappings forms a group isomorphic to G with the conjugacy classes of G as its orbits. If $H \subseteq G$ and $g \in G$, then $g^{-1}Hg$ is defined to be the subset

$$\{g^{-1}hg : h \in H\}.$$

If H is a subgroup of G, then $g^{-1}Hg$ is a subgroup of G isomorphic to H, and we say that $g^{-1}Hg$ is *conjugate* to H. Our next result shows that the stabilizers of two points in the same orbit of a group are conjugate.

Lemma 2.2.3 *Let G be a permutation group on the set V and let x be a point in V. If $g \in G$, then $g^{-1}G_x g = G_{x^g}$.*

Proof. Suppose that $x^g = y$. First we show that every element of $g^{-1}G_x g$ fixes y. Let $h \in G_x$. Then

$$y^{g^{-1}hg} = x^{hg} = x^g = y,$$

and therefore $g^{-1}hg \in G_y$. On the other hand, if $h \in G_y$, then ghg^{-1} fixes x, whence we see that $g^{-1}G_x g = G_y$. □

If g is a permutation of V, then $\mathrm{fix}(g)$ denotes the set of points in V fixed by g. The following lemma is traditionally (and wrongly) attributed to Burnside; in fact, it is due to Cauchy and Frobenius.

Lemma 2.2.4 ("Burnside") *Let G be a permutation group on the set V. Then the number of orbits of G on V is equal to the average number of points fixed by an element of G.*

Proof. We count in two ways the pairs (g, x) where $g \in G$ and x is a point in V fixed by g. Summing over the elements of G we find that the number of such pairs is

$$\sum_{g \in G} |\mathrm{fix}(g)|,$$

which, of course, is $|G|$ times the average number of points fixed by an element of G. Next we must sum over the points of V, and to do this we first note that the number of elements of G that fix x is $|G_x|$. Hence the number of pairs is

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

Now, $|G_x|$ is constant as x ranges over an orbit, so the contribution to this sum from the elements in the orbit x^G is $\left|x^G\right| |G_x| = |G|$. Hence the total sum is equal to $|G|$ times the number of orbits, and the result is proved. □

2.3 Asymmetric Graphs

A graph is *asymmetric* if its automorphism group is the identity group. In this section we will prove that almost all graphs are asymmetric, i.e., the proportion of graphs on n vertices that are asymmetric goes to 1 as $n \to \infty$. Our main tool will be Burnside's lemma.

Let V be a set of size n and consider all the distinct graphs with vertex set V. If we let K_V denote a fixed copy of the complete graph on the vertex set V, then there is a one-to-one correspondence between graphs with vertex set V and subsets of $E(K_V)$. Since K_V has $\binom{n}{2}$ edges, the total number of different graphs is

$$2^{\binom{n}{2}}.$$

Given a graph X, the set of graphs isomorphic to X is called the *isomorphism class* of X. The isomorphism classes partition the set of graphs with vertex set V. Two such graphs X and Y are isomorphic if there is a permutation of $\mathrm{Sym}(V)$ that maps the edge set of X onto the edge set of Y. Therefore, an isomorphism class is an orbit of $\mathrm{Sym}(V)$ in its action on subsets of $E(K_V)$.

Lemma 2.3.1 *The size of the isomorphism class containing X is*

$$\frac{n!}{|\mathrm{Aut}(X)|}.$$

Proof. This follows from the orbit-stabilizer lemma. We leave the details as an exercise. □

Now we will count the number of isomorphism classes, using Burnside's lemma. This means that we must find the average number of subsets of $E(K_V)$ fixed by the elements of $\mathrm{Sym}(V)$. Now, if a permutation g has r orbits in its action on $E(K_V)$, then it fixes 2^r subsets in its action on the power set of $E(K_V)$. For any $g \in \mathrm{Sym}(V)$, let $\mathrm{orb}_2(g)$ denote the number of orbits of g in its action on $E(K_V)$. Then Burnside's lemma yields that the number of isomorphism classes of graphs with vertex set V is equal to

$$\frac{1}{n!}\sum_{g\in\mathrm{Sym}(V)} 2^{\mathrm{orb}_2(g)}. \tag{2.1}$$

If all graphs were asymmetric, then every isomorphism class would contain $n!$ graphs and there would be exactly

$$\frac{2^{\binom{n}{2}}}{n!}$$

isomorphism classes. Our next result shows that in fact, the number of isomorphism classes of graphs on n vertices is quite close to this, and we will deduce from this that almost all graphs are asymmetric. Recall that $o(1)$ is shorthand for a function that tends to 0 as $n \to \infty$.

Lemma 2.3.2 *The number of isomorphism classes of graphs on n vertices is at most*

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

Proof. We will leave some details to the reader. The *support* of a permutation is the set of points that it does not fix. We claim that among all permutations $g \in \mathrm{Sym}(V)$ with support of size an even integer $2r$, the maximum value of $\mathrm{orb}_2(g)$ is realized by the permutation with exactly r cycles of length 2.

Suppose $g \in \mathrm{Sym}(V)$ is such a permutation with r cycles of length two and $n-2r$ fixed points. Since $g^2 = e$, all its orbits on pairs of elements from V have length one or two. There are two ways in which an edge $\{x, y\} \in E(K_V)$ can be not fixed by g. Either both x and y are in the support of g, but $x^g \neq y$, or x is in the support of g and y is a fixed point of g. There are $2r(r-1)$ edges in the former category, and $2r(n-2r)$ is the latter category. Therefore the number of orbits of length 2 is $r(r-1)+r(n-2r) = r(n-r-1)$, and the total number of orbits of g on $E(K_V)$ is

$$\mathrm{orb}_2(g) = \binom{n}{2} - r(n-r-1).$$

Now we are going to partition the permutations of $\mathrm{Sym}(V)$ into 3 classes and make rough estimates for the contribution that each class makes to the sum (2.1) above.

Fix an even integer $m \le n-2$, and divide the permutations into three classes as follows: $\mathcal{C}_1 = \{e\}$, $\mathcal{C}_2$ contains the nonidentity permutations with support of size at most m, and $\mathcal{C}_3$ contains the remaining permutations. We may estimate the sizes of these classes as follows:

$$|\mathcal{C}_1| = 1, \qquad |\mathcal{C}_2| \le \binom{n}{m} m! < n^m, \qquad |\mathcal{C}_3| < n! < n^n.$$

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 it has $\binom{n}{2} - (n-2)$ such orbits. An element $g \in \mathcal{C}_3$ has support of size at least m and so has the maximum number of orbits on pairs if it has $m/2$ 2-cycles, in which case it has

$$\binom{n}{2} - \frac{m}{2}\left(n - \frac{m}{2} - 1\right) \le \binom{n}{2} - \frac{nm}{4}$$

such orbits.

Therefore,

$$\begin{aligned} \sum_{g \in \mathrm{Sym}(V)} 2^{\mathrm{orb}_2(g)} &\le 2^{\binom{n}{2}} + n^m 2^{\binom{n}{2}-(n-2)} + n^n 2^{\binom{n}{2}-nm/4} \\ &= 2^{\binom{n}{2}} \left(1 + n^m 2^{-(n-2)} + n^n 2^{-nm/4}\right). \end{aligned}$$

The sum of the last two terms can be shown to be $o(1)$ by expressing it as

$$2^{m \log n - n + 2} + 2^{n \log n - nm/4}$$

and taking $m = \lfloor c \log n \rfloor$ for $c > 4$. $\square$

Corollary 2.3.3 *Almost all graphs are asymmetric.*

Proof. Suppose that the proportion of isomorphism classes of graphs on V that are asymmetric is μ. Each isomorphism class of a graph that is not asymmetric contains at most $n!/2$ graphs, whence the average size of an isomorphism class is at most

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

Consequently,

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

from which it follows that μ tends to 1 as n tends to infinity. Since the proportion of asymmetric graphs on V is at least as large as the proportion of isomorphism classes (why?), it follows that the proportion of graphs on n vertices that are asymmetric goes to 1 as n tends to ∞. $\square$

Although the last result assures us that most graphs are asymmetric, it is surprisingly difficult to find examples of graphs that are obviously asymmetric. We describe a construction that does yield such examples. Let T be a tree with no vertices of valency two, and with at least one vertex of valency greater than two. Assume that it has exactly m end-vertices. We construct a *Halin graph* by drawing T in the plane, and then drawing a cycle of length m through its end-vertices, so as to form a planar graph. An example is shown in Figure 2.1.

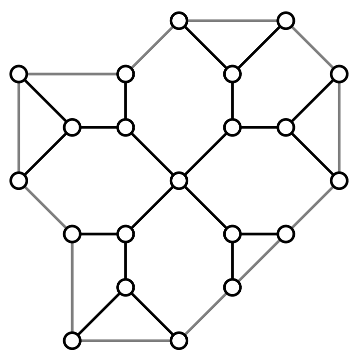

Figure 2.1. A Halin graph

Halin graphs have a number of interesting properties; in particular, it is comparatively easy to construct cubic Halin graphs with no nonidentity automorphisms. They all have the property that if we delete any two vertices, then the resulting graph is connected, but if we delete any edge, then we can find a pair of vertices whose deletion will disconnect the graph. (To use language from Section 3.4, they are 3-connected, but any proper subgraph is at most 2-connected.)

2.4 Orbits on Pairs

Let G be a transitive permutation group acting on the set V. Then G acts on the set of ordered pairs $V \times V$, and in this section we study its orbits on this set. It is so common to study G acting on both V and $V \times V$ that the orbits of G on $V \times V$ are often given the special name *orbitals*.

Since G is transitive, the set

$$\{(x, x) : x \in V\}$$

is an orbital of G, known as the *diagonal orbital*. If $\Omega \subseteq V \times V$, we define its *transpose* Ω^T to be

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

It is a routine exercise to show that Ω^T is G-invariant if and only if Ω is. Since orbits are either equal or disjoint, it follows that if Ω is an orbital of G, either $\Omega = \Omega^T$ or $\Omega \cap \Omega^T = \emptyset$. If $\Omega = \Omega^T$, we call it a *symmetric* orbital.

Lemma 2.4.1 *Let G be a group acting transitively on the set V, and let x be a point of V. Then there is a one-to-one correspondence between the orbits of G on $V \times V$ and the orbits of G_x on V.*

Proof. Let Ω be an orbit of G on $V \times V$, and let Y_Ω denote the set $\{y : (x, y) \in \Omega\}$. We claim that the set Y_Ω is an orbit of G_x acting on V. If y and y' belong to Y_Ω, then (x, y) and (x, y') lie in Ω and there is a permutation g such that

$$(x, y)^g = (x, y').$$

This implies that $g \in G_x$ and $y^g = y'$, and thus y and y' are in the same orbit of G_x. Conversely, if $(x, y) \in \Omega$ and $y' = y^g$ for some $g \in G_x$, then $(x, y') \in \Omega$. Thus Y_Ω is an orbit of G_x. Since V is partitioned by the sets Y_Ω, where Ω ranges over the orbits of G on $V \times V$, the lemma follows. □

This lemma shows that for any $x \in V$, each orbit Ω of G on $V \times V$ is associated with a unique orbit of G_x. The number of orbits of G_x on V is called the *rank* of the group G. If Ω is symmetric, the corresponding orbit of G_x is said to be *self-paired*. Each orbit Ω of G on $V \times V$ may be viewed as a directed graph with vertex set V and arc set Ω. When Ω is symmetric this directed graph is a graph: (x, y) is an arc if and only if (y, x) is. If Ω is not symmetric, then the directed graph has the property that if (x, y) is an arc, then (y, x) is not an arc. Such directed graphs are often known as oriented graphs (see Section 8.3).

Lemma 2.4.2 *Let G be a transitive permutation group on V and let Ω be an orbit of G on $V \times V$. Suppose $(x, y) \in \Omega$. Then Ω is symmetric if and only if there is a permutation g in G such that $x^g = y$ and $y^g = x$.*

Proof. If (x, y) and (y, x) both lie in Ω, then there is a permutation $g \in G$ such that $(x, y)^g = (x^g, y^g) = (y, x)$. Conversely, suppose there is a permutation g swapping x and y. Since $(x, y)^g = (y, x) \in \Omega$, it follows that $\Omega \cap \Omega^T \neq \emptyset$, and so $\Omega = \Omega^T$. □

If a permutation g swaps x and y, then (xy) is a cycle in g. It follows that g has even order (and so G itself must have even order). A permutation group G on V is *generously transitive* if for any two distinct elements x and y from V there is a permutation that swaps them. All orbits of G on $V \times V$ are symmetric if and only if G is generously transitive.

We have seen that each orbital of a transitive permutation group G on V gives rise to a graph or an oriented graph. It is clear that G acts as a transitive group of automorphisms of each of these graphs. Similarly, the union of any set of orbitals is a directed graph (or graph) on which G acts transitively. We consider one example. Let V be the set of all 35 triples from a fixed set of seven points. The symmetric group $\mathrm{Sym}(7)$ acts on V as a transitive permutation group G, and it is not hard to show that G is generously transitive. Fix a particular triple x and consider the orbits of G_x on V. There are four orbits, namely x itself, the triples that meet x in 2 points, the triples that meet x in 1 point, and those disjoint from x. Hence these correspond to four orbitals, the first being the diagonal orbital, with the remaining three yielding the graphs $J(7,3,2)$, $J(7,3,1)$, and $J(7,3,0)$. It is clear that G is a subgroup of the automorphism group of each of these graphs, but although it can be shown that G is the full automorphism group of $J(7,3,2)$ and $J(7,3,0)$, it is not the full automorphism group of $J(7,3,1)$!

Lemma 2.4.3 *The automorphism group of* $J(7,3,1)$ *contains a group isomorphic to* $\mathrm{Sym}(8)$.

Proof. There are 35 partitions of the set $\{0,1,\ldots,7\}$ into two sets of size four. Let X be the graph with these partitions as vertices, where two partitions are adjacent if and only if the intersection of a 4-set from one with a 4-set from the other is a set of size two. Clearly, $\mathrm{Aut}(X)$ contains a subgroup isomorphic to $\mathrm{Sym}(8)$. However, X is isomorphic to $J(7,3,1)$. To see this, observe that a partition of $\{0,1,\ldots,7\}$ into two sets of size four is determined by the 4-set in it that contains 0, and this 4-set in turn is determined by its nonzero elements. Hence the partitions correspond to the triples from $\{1,2,\ldots,7\}$ and two partitions are adjacent in X if and only if the corresponding triples have exactly one element in common. $\square$

2.5 Primitivity

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

An example of a system of imprimitivity is readily provided by the cube Q shown in Figure 2.2. It is straightforward to see that $\mathrm{Aut}(Q)$ acts transitively on Q (see Section 3.1 for more details).

For each vertex x there is a unique vertex x' at distance three from it; all other vertices in Q are at distance at most two. If $S = \{x, x'\}$ and $g \in \mathrm{Aut}(Q)$, then either $S^g = S$ or $S \cap S^g = \emptyset$, so S is a block of imprimitivity. There are four disjoint sets of the form S^g, as g ranges over

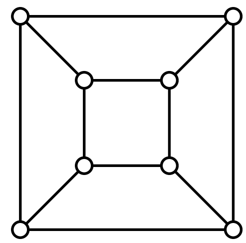

Figure 2.2. The cube Q

the elements of $\mathrm{Aut}(Q)$, and these sets are permuted among themselves by $\mathrm{Aut}(Q)$.

The partition of V into singletons is a system of imprimitivity as is the partition of V into one cell containing all of V. Any other system of imprimitivity is said to be nontrivial. A group with no nontrivial systems of imprimitivity is *primitive*; otherwise, it is *imprimitive*. There are two interesting characterizations of primitive permutation groups. We give one now; the second is in the next section.

Lemma 2.5.1 *Let G be a transitive permutation group on V and let x be a point in V. Then G is primitive if and only if G_x is a maximal subgroup of G.*

Proof. In fact, we shall be proving the contrapositive statement, namely that G has a nontrivial system of imprimitivity if and only if G_x is not a maximal subgroup of G. First some notation: We write $H \leq G$ if H is a subgroup of G, and $H < G$ if H is a proper subgroup of G.

Suppose first that G has a nontrivial system of imprimitivity and that B is a block of imprimitivity that contains x. Then we will show that $G_x < G_B < G$ and therefore that G_x is not maximal. If $g \in G_x$, then $B \cap B^g$ is nonempty (for it contains x) and hence $B = B^g$. Thus $G_x \leq G_B$. To show that the inclusion is proper we find an element in G_B that is not in G_x. Let $y \neq x$ be another element of B. Since G is transitive it contains an element h such that $x^h = y$. But then $B = B^h$, yet $h \notin G_x$, and hence $G_x < G_B$.

Conversely, suppose that there is a subgroup H such that $G_x < H < G$. We shall show that the orbits of H form a nontrivial system of imprimitivity. Let B be the orbit of H containing x and let $g \in G$. To show that B is a block of imprimitivity it is necessary to show that either $B = B^g$ or $B \cap B^g = \emptyset$. Suppose that $y \in B \cap B^g$. Then because $y \in B$ there is an element $h \in H$ such that $y = x^h$. Moreover, because $y \in B^g$ there is some element $h' \in H$ such that $y = x^{h'g}$. Then $x^{h'gh^{-1}} = x$, and so $h'gh^{-1} \in G_x < H$. Therefore, $g \in H$, and because B is an orbit of H we have $B = B^g$. Because $G_x < H$, the block B does not consist of x alone, and because $H < G$, it does not consist of the whole of V, and hence it is a nontrivial block of imprimitivity. $\square$

2.6 Primitivity and Connectivity

Our second characterization of primitive permutation groups uses the orbits of G on $V \times V$, and requires some preparation. A path in a directed graph D is a sequence $u_0, \ldots, u_r$ of distinct vertices such that (u_{i-1}, u_i) is an arc of D for $i = 1, \ldots, r$. A *weak path* is a sequence $u_0, \ldots, u_r$ of distinct vertices such that for $i = 1, \ldots, r$, either (u_{i-1}, u_i) or (u_i, u_{i-1}) is an arc. (We will use this terminology in this section only.) A directed graph is *strongly connected* if any two vertices can be joined by a path and is *weakly connected* if any two vertices can be joined by a weak path. A directed graph is weakly connected if and only if its "underlying" undirected graph is connected. (This is often used as a definition of weak connectivity.) A *strong component* of a directed graph is an induced subgraph that is maximal, subject to being strongly connected. Since a vertex is strongly connected, it follows that each vertex lies in a strong component, and therefore the strong components of D partition its vertices.

The *in-valency* of a vertex in a directed graph is the number of arcs ending on the vertex, the *out-valency* is defined analogously.

Lemma 2.6.1 *Let D be a directed graph such that the in-valency and out-valency of any vertex are equal. Then D is strongly connected if and only if it is weakly connected.*

Proof. The difficulty is to show that if D is weakly connected, then it is strongly connected. Assume by way of contradiction that D is weakly, but not strongly, connected and let $D_1, \ldots, D_r$ be the strong components of D. If there is an arc starting in D_1 and ending in D_2, then any arc joining D_1 to D_2 must start in D_1. Hence we may define a directed graph D' with the strong components of D as its vertices, and such that there is an arc from D_i to D_j in D' if and only if there is an arc in D starting in D_i and ending in D_j. This directed graph cannot contain any cycles. (Why?) It follows that there is a strong component, D_1 say, such that any arc that ends on a vertex in it must start at a vertex in it. Since D is weakly connected, there is at least one arc that starts in D_1 and ends on a vertex not in D_1. Consequently the number of arcs in D_1 is less than the sum of the out-valencies of the vertices in it. But on the other hand, each arc that ends in D_1 must start in it, and therefore the number of arcs in D_1 is equal to the sum of the in-valencies of its vertices. By our hypothesis on D, though, the sum of the in-valencies of the vertices in D_1 equals the sum of the out-valencies. Thus we have the contradiction we want. $\square$

What does this lemma have to do with permutation groups? Let G act transitively on V and let Ω be an orbit of G on $V \times V$ that is not symmetric. Then Ω is an oriented graph, and G acts transitively on its vertices. Hence each point in V has the same out-valency in Ω and the same in-valency. As the in- and out-valencies sum to the number of arcs in Ω, the in- and out-valencies of any point of V in Ω are the same. Hence Ω is weakly connected if and only if it is strongly connected, and so we will refer to weakly or strongly connected orbits as connected orbits.

Lemma 2.6.2 *Let G be a transitive permutation group on V. Then G is primitive if and only if each nondiagonal orbit is connected.*

Proof. Suppose that G is imprimitive, and that $B_1, \dots, B_r$ is a system of imprimitivity. Assume further that x and y are distinct points in B_1 and Ω is the orbit of G (on $V \times V$) that contains (x, y). If $g \in G$, then x^g and y^g must lie in the same block; otherwise B^g contains points from two distinct blocks. Therefore, each arc of Ω joins vertices in the same block, and so Ω is not connected.

Now suppose conversely that Ω is a nondiagonal orbit that is not connected, and let B be the point set of some component of Ω. If $g \in G$, then B and B^g are either equal or disjoint. Therefore, B is a nontrivial block and G is imprimitive. □

Exercises

1. Show that the size of the isomorphism class containing X is
$$\frac{n!}{|\mathrm{Aut}(X)|}.$$

2. Prove that $|\mathrm{Aut}(C_n)| = 2n$. (You may assume that $2n$ is a lower bound on $|\mathrm{Aut}(C_n)|$.)

3. If G is a transitive permutation group on the set V, show that there is an element of G with no fixed points. (What if G has more than one orbit, but no fixed points?)

4. If g is a permutation of a set of n points with support of size s, show that $\mathrm{orb}_2(g)$ is maximal when all nontrivial cycles of g are transpositions.

5. The goal of this exercise is to prove Frobenius's lemma, which asserts that if the order of the group G is divisible by the prime p, then G contains an element of order p. Let Ω denote the set of all ordered p-tuples $(x_1, \dots, x_p)$ of elements of G such that $x_1 \cdots x_p = e$. Let π denote the permutation of G^p that maps $(x_1, x_2, \dots, x_p)$ to $(x_2, \dots, x_p, x_1)$. Show that π fixes Ω as a set. Using the facts that π

fixes $(e, \ldots, e)$ and $|\Omega| = |G|^{p-1}$, deduce that π must fix at least p elements of Ω and hence Frobenius's lemma holds.

6. Construct a cubic planar graph on 12 vertices with trivial automorphism group, and provide a proof that it has no nonidentity automorphism.

7. Decide whether the cube is a Halin graph.

8. Let X be a self-complementary graph with more than one vertex. Show that there is a permutation g of $V(X)$ such that:
   (a) $\{x, y\} \in E(X)$ if and only if $\{x^g, y^g\} \in E(\overline{X})$,
   (b) $g^2 \in \mathrm{Aut}(X)$ but $g^2 \neq e$,
   (c) the orbits of g on $V(X)$ induce self-complementary subgraphs of X.

9. If G is a permutation group on V, show that the number of orbits of G on $V \times V$ is equal to
$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)|^2$$
and derive a similar formula for the number of orbits of G on the set of pairs of distinct elements from V.

10. If H and K are subsets of a group G, then HK denotes the subset
$$\{hk : h \in H,\ k \in K\}.$$
If H and K are subgroups and $g \in G$, then HgK is called a *double coset*. The double coset HgK is a union of right cosets of H and a union of left cosets of K, and G is partitioned by the distinct double cosets HgK, as g varies over the elements of G. Now (finally) suppose that G is a transitive permutation group on V and $H \leq G$. Show that each orbit of H on V corresponds to a double coset of the form $G_x gH$. Also show that the orbit of G_x corresponding to the double coset $G_x g G_x$ is self-paired if and only if $G_x g G_x = G_x g^{-1} G_x$.

11. Let G be a transitive permutation group on V. Show that it has a symmetric nondiagonal orbit on $V \times V$ if and only if $|G|$ is even.

12. Show that the only primitive permutation group on V that contains a transposition is $\mathrm{Sym}(V)$.

13. Let X be a graph such that $\mathrm{Aut}(X)$ acts transitively on $V(X)$ and let B be a block of imprimitivity for $\mathrm{Aut}(X)$. Show that the subgraph of X induced by B is regular.

14. Let G be a generously transitive permutation group on V and let B be a block for G. Show that $G{\restriction}B$ and the permutation group induced by G on the translates of B are both generously transitive.

15. Let G be a transitive permutation group on V such that for each element v in V there is an element of G with order two that has v as its only fixed point. (Thus $|V|$ must be odd.) Show that G is generously transitive.
16. Let X be a nonempty graph that is not connected. If $\mathrm{Aut}(X)$ is transitive, show that it is imprimitive.
17. Show that $\mathrm{Aut}(J(4n-1, 2n-1, n-1))$ contains a subgroup isomorphic to $\mathrm{Sym}(4n)$. Show further that $\omega(J(4n-1, 2n-1, n-1)) \leq 4n-1$, and characterize the cases where equality holds.

Notes

The standard reference for permutation groups is Wielandt's classic [5]. We also highly recommend Cameron [1]. For combinatorialists these are the best starting points. However, almost every book on finite group theory contains enough information on permutation groups to cover our modest needs. Neumann [3] gives an interesting history of Burnside's lemma.

The result of Exercise 15 is due to Shult. Exercise 17 is worth some thought, even if you do not attempt to solve it, because it appears quite obvious that $\mathrm{Aut}(J(4n-1, 2n-1, n-1))$ should be $\mathrm{Sym}(4n-1)$. The second part will be easier if you know something about Hadamard matrices.

Call a graph *minimal asymmetric* if it is asymmetric, but any proper induced subgraph with at least two vertices has a nontrivial automorphism. Sabidussi and Nešetřil [2] conjecture that there are finitely many isomorphism classes of minimal asymmetric graphs. In [4], Sabidussi verifies this for all graphs that contain an induced path of length at least 5, finding that there are only two such graphs. In [2], Sabidussi and Nešetřil show that there are exactly seven minimal asymmetric graphs in which the longest induced path has length four.

References

[1] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[2] J. Nešetřil and G. Sabidussi, *Minimal asymmetric graphs of induced length 4*, Graphs Combin., 8 (1992), 343–359.

[3] P. M. Neumann, *A lemma that is not Burnside's*, Math. Sci., 4 (1979), 133–141.

[4] G. Sabidussi, *Clumps, minimal asymmetric graphs, and involutions*, J. Combin. Theory Ser. B, 53 (1991), 40–79.

[5] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.