- 1100, 1010, 1001,
- 2211, 2121, 2112,
- 0022, 0202, 0220.

Again, this example can be generalized for larger values of k, and we will discuss that more in the Notes section.

Quick Check

1. Let $\mathcal{D}$ be a balanced uniform (and therefore regular) design. Is there an analogous version of Corollary 8.26 that uses the *columns* of the incidence matrix M of $\mathcal{D}$ instead of the rows?
2. We have mentioned that the code of Example 8.25 is not perfect. Now let us extend that code by adding nine new codewords, namely the all-0 word, the all-1 word, and the complement of each of the original seven codewords. (The complement of a codeword w is the word in which each letter in w is replaced by the opposite letter.) Is the new code C still 1-error correcting?
3. Is the code C of the previous Quick Check exercise perfect?

8.4 Counting symmetric structures

The reader may remember that, in Chapter 5, when we counted graphs, we typically counted graphs with *labeled* vertices, which prevented symmetries. We mentioned that the enumeration of *unlabeled* graphs is usually harder. This is true for other structures as well. To see why, let us consider the job of painting each of the six sides of a cube with one of k colors. If the sides are all considered different, for instance, because they are labeled 1 through 6, then the number of ways to do this is 6^k. However, if the faces are indistinguishable, the problem is much more difficult. Say we consider two colorings identical if one can be transformed into the other by a series of rotations. We cannot simply count the number of all possible colorings regardless of rotations and then divide by the number of all possible rotations, since the number of possible rotations is not the same for each coloring. (Compare a coloring that uses only one color and a coloring that uses all six.) If we allow reflection through planes in addition to rotations, the situation is even more complex. Again, the problem is that not all equivalence classes will have the same size.

In order to be able to discuss the machinery relevant to problems like the one above, we need to introduce basic notions of *Group Theory*, in particular the *theory of permutation groups*. Readers who have taken a class in abstract algebra before will probably be familiar with these notions.

Definition 8.28 *A* group *is a set G of elements and an operation that we will call* multiplication *on the set of ordered pairs of G so that the following axioms hold.*

(1) There exists an identity *element in G, that is, there exists an element $e \in G$ so that $a \cdot e = e \cdot a = a$ for all $a \in G$.*

(2) The set G is closed under multiplication, that is, if $a \in G$ and $b \in G$, then $a \cdot b \in G$.

(3) Multiplication is associative, that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(4) Each element of G has a unique inverse*, that is, for each $a \in G$, there exists a unique element $b \in G$ so that $ab = ba = e$. We then write $b = a^{-1}$.*

Note that the operation "multiplication" can be defined in any way that satisfies the axioms; that is, it does not have to be what we typically call multiplication when dealing with real numbers.

If this is the first occasion the reader has heard about groups, then the reader should take the time and prove (by verifying that all axioms hold) that the set of real numbers with addition as the operation form a group and that the set of nonzero real numbers with traditional multiplication as the operation form a group. After this, the reader should explain why the set of *all real numbers* does not form a group with traditional multiplication as the operation.

While an entire chapter could be filled with examples of interesting groups, we will focus on the group of all *permutations* of length n. First, of course, we have to prove that this set indeed forms a group with the operation that naturally comes to mind, that is, multiplication of permutations as defined in Chapter 4. Recall, in Definition 4.13, we simply said that the product of n-permutations f and g is simply their composition as bijections from $[n]$ to $[n]$.

Proposition 8.29 *The set of all n-permutations, equipped with multiplication of permutations as the operation, forms a group.*

As we mentioned in Chapter 4, this group is called the *symmetric group*, denoted by S_n.

Proof: We will check that all the axioms hold.

1. The permutation $p = (1)(2)\cdots(n)$ is the identity element of this group.
2. The product of two n-permutations is an n-permutation, since the composition of two bijections from $[n]$ to $[n]$ is a bijection from $[n]$ to $[n]$.

3. Let f, g, and h be three permutations, and let $f(i) = j$, $g(j) = k$, and $h(k) = m$. Then

$$((f \cdot g)) \cdot h)(i) = h(g(f(i))) = h(g(j)) = h(k) = m,$$

and

$$(f \cdot (g \cdot h))(i) = (g \cdot h)(f(i))) = h(g(j)) = h(k) = m.$$

4. The inverse of the permutation f is simply the inverse of f as a bijection.

$\Diamond$

We say that a subset H of elements of the group G forms a *subgroup* of G if H is a group itself with the same operation as G. Subgroups of the symmetric group S_n are called *permutation groups*. This is because their elements are permutations.

The crucial concept is that permutations *move* (permute) objects. In our examples so far in this chapter, as well as those in Chapter 4, these objects were most often simply elements of the set $[n]$. However, permutations can act on other sets as well. Recall the definition of an automorphism of a graph M on vertex set $[n]$ from Chapter 5. Such an automorphism was a bijection f from the vertex set of G onto itself so that $f(a)$ and $f(b)$ were adjacent if and only if a and b were. In other words, an automorphism is a *permutation* of the vertices of M. It is straightforward to show that all automorphisms of M form a group. Call this group $Aut(M)$; then $Aut(M)$ is a *permutation group*; indeed, it is a subgroup of S_n.

Graphs and their automorphism groups provide a simple way to visualize the next notion we are going to discuss, the *orbit* of an object under the action of a permutation group.

The reader is asked to consider the graph G shown in Figure 8.4. The group $Aut(M)$ permutes the vertices of this graph among themselves. However, no matter what element $f \in Aut(M)$ we choose, $f(4) = 4$ will always hold, since 4 is the only vertex of G with degree five, and we know that the degrees of 4 and $f(4)$ must agree since an automorphism must preserve degrees. By an analogous argument, $f(1)$ must be either 1, 2, or 3, since these are the only vertices of degree three. The same holds for $f(2)$ and $f(3)$. Similarly, $f(5)$ must be equal to 5 or 6, and the same holds for $f(6)$, since 5 and 6 are the only vertices of degree one.

Finally, any one of these choices is indeed possible, that is, there exists an $f \in Aut(M)$ so that $f(1) = 3$, there exists an $f \in Aut(M)$ so that $f(1) = 2$, and so on.

The phenomena described above are so important that they deserve a name.

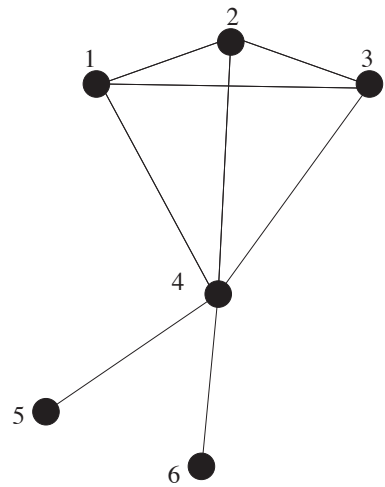

Figure 8.4
The orbits of the vertex set of this graph M are $\{1, 2, 3\}$, $\{4\}$, and $\{5, 6\}$.

Definition 8.30 *Let G be a permutation group acting on a set S. Let $i \in S$. Set*

$$i^G = \{g(i) | g \in G\}.$$

In other words, i^G is the set of all vertices into which i can be mapped by an element of G. Then i^G is called the orbit *of i under G.*

Example 8.31 *If S is the vertex set of the graph M shown in Figure 8.4, and $G = Aut(M)$, then the orbits of the elements of M under $Aut(M)$ are as follows:*

- $1^G = 2^G = 3^G$,
- 4^G, *and*
- $5^G = 6^G$.

The reader might have noticed that the orbits of two elements are either equal or disjoint; it never happens that they have a few common elements and a few different elements. As the following lemma shows, this is always the case.

Lemma 8.32 *Let G be a permutation group acting on a set S. Let i and j be two distinct elements of S. Then either $i^G = j^G$ or $i^G \cap j^G = \emptyset$.*

In other words, the orbits form a *partition* of S if we remove repeated copies of the same orbit.

Proof: (of Lemma 8.32) First assume that $j \in i^G$, that is, there exists an $f \in G$ so that $f(i) = j$. Assume now that $k \in j^G$, since $h(j) = k$ for some $h \in G$. Then we also have $k \in i^G$, since $(f \cdot h)(i) = h(f(i)) = h(j) = k$. Therefore, $j^G \subseteq i^G$. Now note that $f^{-1}(j) = i$, so $i \in j^G$. Therefore, we can switch the roles of i and j in the previous argument and show that $i^G \subseteq j^G$, yielding that $i^G = j^G$.

Now assume that $j \notin i^G$. We claim that then i^G and j^G must be disjoint. Assume not; that is, assume that there exists an element $s \in S$ so that $p(i) = s$ and $q(j) = s$ for some p and q in G. Then $q^{-1}(s) = j$, so $(p \cdot q^{-1})(i) = q^{-1}(p(i)) = q^{-1}(s) = j$, contradicting the assumption that $j \notin i^G$. $\Diamond$

That is, the relation "i and j have the same orbit" is an equivalence relation on S. The number of equivalence classes is just the number of distinct orbits. In our quest to enumerate structures that are not equivalent, we will try to reduce our problems to the problem of counting orbits of a permutation group acting on a set.

There is one last notion we need to introduce before our main result. It is a natural counterpart of the notion of orbits. The size of the orbit of an element i told us into how many different elements i could be mapped by a given permutation group G. We could also ask how many elements of G will keep i where it was, or we could ask how many elements of S a given element g will keep fixed. We need both of these useful notions.

Definition 8.33 *Let G be a permutation group acting on a set S, and let $i \in S$. Then the set*

$$G_i = \{g \in G | g(i) = i\}$$

is called the stabilizer *of i.*

In Supplementary Exercise 15, the reader is asked to verify that G_i is always a *subgroup* of G.

It is reasonable to conjecture at this point that, when G and S are fixed, the larger i^G is, the smaller G_i will be. Indeed, the more places i can go to, the fewer elements should fix it. We would also like to point out that Example 8.31 suggests that $|i^G|$ is always a *divisor* of G. The following lemma will show that both of these observations hold in the general case.

Lemma 8.34 *Let G be a finite permutation group acting on a set S, and let $i \in S$. Then*

$$\frac{|G|}{|G_i|} = \left|i^G\right|.$$

Proof: If $g \in G$, let gG_i denote the set $\{h \in G | gx = h \text{ for some } x \in G_i\}$. These sets gG_i are called the *cosets* of G_i in G. We now claim that two cosets of G_i in G are either equal or disjoint. The proof of this claim is very similar to that of Lemma 8.32, and therefore will be left for Exercise 12.

We ask the reader to verify that all cosets gG_i have the same size as G_i. Indeed the elements of gG_i are the products gx, where x ranges over all elements $x \in G_i$. This means there are $|G_i|$ products, and they are all different. If they were not, then $gx = gx'$ would hold, which, after multiplying by g^{-1} from the left, would result in $x = x'$.

As the distinct cosets of G_i partition G, this proves that $|G_i|$ divides $|G|$. Now that we have discussed the *size* of these cosets, let us turn our attention to their *number*. We claim that the number of the cosets of G_i is $\left|i^G\right|$, the size of the orbit of i.

We will prove this claim by constructing a bijection α from i^G onto the set of all cosets of G_i in G. Elements of i^G can be written in the form $g(i)$, with $g \in G$ where g is not necessarily unique. Now set $\alpha(g(i)) = gG_i$.

Before we try to prove that this map α is indeed a bijection, we have to prove that it is indeed well-defined, that is, if g and g_1 are such that $g(i) = g_1(i)$, then $\alpha(g(i)) = \alpha(g_1(i))$. This will show that α is indeed a map that is defined on the elements of the orbit of i and which does not depend on anything else, such as the choice of g.

To see this, note that $g(i) = g_1(i)$ is equivalent to $g_1^{-1}g(i) = i$, meaning that $g_1^{-1}g \in G_i$. That leads to $g_1^{-1}gG_i = G_i$, and therefore $gG_i = g_1G_i$; so $\alpha(g(i)) = \alpha(g_1(i))$ as claimed.

Finally, to prove that α is a bijection, let us construct its inverse. Let gG_i be a coset of G_i. Then all elements of this coset are of the form gx, where $x(i) = i$. Therefore, for all elements gx of this coset, $gx(i) = g(i)$. Then $g(i) \in i^G$ is the preimage of gG_i under α. This preimage is unique, since, if $\alpha(g(i)) = \alpha(g_1(i))$, then $gG_i = g_1G_i$, yielding that $g_1^{-1}g \in G_i$. That would lead to $g(i) = g^{-1}(i)$, meaning that $g(i)$ and $g^{-1}(i)$ are in fact identical as elements of i^G.

So the number of cosets of G_i is $\left|i^G\right|$, proving our lemma. $\Diamond$

Note that the simple fact that two cosets of G_i in G must be either disjoint or equal is true in a more general way. See Exercise 12 for that more general version.

Definition 8.35 *Let G be a permutation group acting on a set S, and let $g \in G$. Let*

$$F_g = \{i \in S | g(i) = i\}.$$

Now we are in a position to announce and prove the main result of this section.

Theorem 8.36 *Let G be a permutation group acting on a set S. Then the number of orbits of S under the action of G is equal to*

$$\frac{1}{|G|} \sum_{g \in G} |F_g|.$$

This theorem is a classic, and it has many names, such as Frobenius' theorem, Cauchy's theorem, Burnside lemma, or a name consisting of a nonempty subset of the previous three names.

The following example provides an opportunity to practice the notions of this theorem before proving it.

Example 8.37 *Let S be the vertex set of the graph M shown in Figure 8.4, and let $G = Aut(M)$. Then $|G| = 6 \cdot 2 = 12$, since vertices 1, 2, and 3 can be permuted among each other in any way, vertices 5 and 6 can be permuted among each other in any way, and there are no other automorphisms. Each of these 12 automorphisms will map 4 to 4. Half of them will map 5 to 5 and 6 to 6, and the other half will map 5 to 6 and 6 to 5. On the set $\{1, 2, 3\}$, two of them will have three fixed points, six of them will have one fixed point, and four of them will have no fixed point.*

So altogether, there is one element of G (the identity) with six fixed points; there are four with four fixed points (one of which fixes 1, 2, 3, and 4, and one of which fixes i, 4, 5, and 6 for some $i \in [3]$); there are two with three fixed points (fixing 4, 5, and 6); there are three with two fixed points (fixing i and 4, for some $i \in [3]$); and there are two with one fixed point (fixing 4).

Therefore, Theorem 8.36 says that the number of orbits of G on S is

$$\frac{1}{12}\sum_{g\in G}|F_g| = \frac{1\cdot 6 + 4\cdot 4 + 2\cdot 3 + 3\cdot 2 + 2\cdot 1}{12} = \frac{36}{12} = 3,$$

which is in accordance with what we have seen, that is, that the orbits are $\{1, 2, 3\}$, $\{4\}$, and $\{5, 6\}$.

Proof: (of Theorem 8.36) The number of orbits of G is certainly equal to $\sum_i \frac{1}{|i^G|}$, where i ranges over all elements of S. Indeed, the total contribution of each orbit to this sum will be 1. Now let us transform this sum as follows:

$$\sum_i \frac{1}{|i^G|} = \sum_i \frac{|G_i|}{|G|} = \frac{1}{|G|}\sum_i |G_i|.$$

We applied Lemma 8.34 in the first step. The last displayed equation is promising, since it already contains the factor $\frac{1}{|G|}$, which is multiplied by a sum. The only problem is that this sum is over all values of i, not g. However, taking a closer look at the sum $\sum_i |G_i|$, we see that it in fact counts all pairs (g, i) so that $g \in G$, $i \in S$, and $g(i) = i$. Therefore, this sum does not change if we compute it by summing over values of i first and g second. This shows that

$$\sum_i |G_i| = \sum_{g\in G} |F_g|$$

and proves our theorem. $\Diamond$

In a typical application of Theorem 8.36, we count structures that are nonequivalent according to some definition. It then turns out that this

nonequivalence means that they belong to different orbits under some group action, and that the number of orbits is the number of these nonequivalent structures. Then we count the orbits using Theorem 8.36 and conclude that it equals the number of nonequivalent structures.

Let us start with a very simple example.

Example 8.38 *We have a rectangular, fenced backyard of size* 90×100. *We want to color the four sides of the fence using red and blue paint, using only one color on each side. In how many different ways can we do this if two colorings are considered equivalent if they differ only by a 180-degree rotation?*

Solution: In this example, the group R of rotations consists of just two elements, the identity and the 180-degree rotation. This group acts on the set of all 16 possible colorings (if we consider the sides all distinguishable and do not identify colorings that differ by a rotation, then there are $2^4 = 16$ colorings). The orbits of this action are precisely the nonequivalent colorings, since two colorings are identical precisely when they can be rotated into each other. The identity will fix all 16 possible colorings, while the 180-degree rotation will fix those four colorings in which opposite pairs are of the same color. Therefore, by Theorem 8.36, the number of nonequivalent colorings is

$$\frac{1}{2}(16 + 4) = 10.$$

$\Diamond$

The following example is somewhat more difficult.

Example 8.39 *We color the sides of a square either red or blue. We consider two colorings equivalent if there is symmetry (rotation or reflection) that takes one coloring into the other. How many nonequivalent colorings are there?*

Solution: It is not hard to see that the square has eight symmetries: four rotations (counting the identity, we call them r, r^2, r^3, and id) and four reflections. Two of these reflections (a and b) are through diagonals, and the other two are through lines bisecting opposite sides (c and d).

These symmetries permute the sides of our square, and while doing that, they permute colorings among each other. So they are the permutations acting on the set of all colorings. Now we are going to find out how many colorings each of them fixes. Each symmetry fixes the colorings that use only one color. Rotations r and r^3 do not fix anything else, since they map sides into adjacent sides (so if they fixed a coloring, that coloring would have to use one color only). Rotation r^2 fixes two 2-colorings, those in which opposite sides are of the same color. Reflections c and d fix two 2-colorings each, those in which sides intersecting each other on the reflection axis are monochromatic. Reflections a and b fix six 2-colorings each (in these colorings, the sides parallel to the axis

of reflection are monochromatic). See Figure 8.5 for a list. Finally, *id* fixes all 16 colorings.

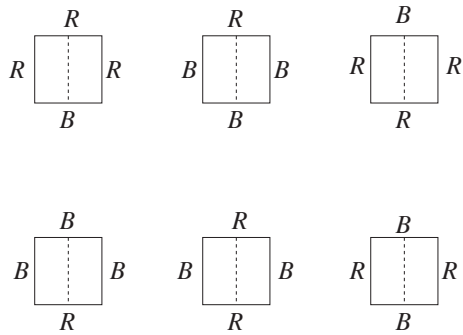

Figure 8.5
The six 2-colorings fixed by reflection a.

Applying Theorem 8.36, and remembering that all symmetries fix the two colorings that use only one color, we get that the number of nonequivalent colorings is

$$\frac{1}{8}(2 \cdot 2 + 3 \cdot 4 + 2 \cdot 8 + 1 \cdot 16) = \frac{48}{8} = 6.$$

◊

The reader should not get the impression that coloring sides of polygons is the only application of Theorem 8.36. In Supplementary Exercise 16, we ask the reader to use Theorem 8.36 to re-prove the fact that the average n-permutation has one fixed point. In Exercise 13, we ask the reader to prove a classic number-theoretical result by Fermat using the same technique. Exercise 14 claims that Theorem 5.7 is just a special case of Lemma 8.34.

Quick Check

1. Let A be a complete graph on four vertices with one edge removed. How many ways are there two color the edges of A using only the colors red, blue, and green if two colorings are considered identical if there is an automorphism that takes one coloring to the other?
2. Find the number of ways to color each side of a regular pentagon red, blue, or green if two colorings are considered identical if there is a rotation or reflection that takes one coloring into the other.
3. Let A be a graph that is a C_5 with a diagonal added. Find the number of ways to color each edge of A red, blue, or green if two