Chapter 6

Not So Vicious Cycles. Cycles in Permutations

We have considered several enumeration problems in the previous three chapters. One of them, that of permutations, stands out by its omnipresence in mathematics. The reason for that is that permutations can be viewed not only as linear orders of different objects, most often elements of $[n]$, but also as *functions* from $[n]$ to $[n]$. In particular, a permutation $p = p_1p_2 \cdots p_n$ can be conceived as the unique function $p : [n] \rightarrow [n]$ for which $p(i) = p_i$.

Example 6.1. The permutation 312 can be viewed as the (bijective) function $f : [3] \rightarrow [3]$ defined by $f(1) = 3$, $f(2) = 1$, and $f(3) = 2$.

The advantage of this approach is that now one can define the *product* of two permutations on $[n]$ by simply taking their composition as a composition of functions.

Example 6.2. Let $f = 312$ and let $g = 213$. Then $(f \cdot g)(1) = g(f(1)) = g(3) = 3$, $(f \cdot g)(2) = g(f(2)) = g(1) = 2$, and $(f \cdot g)(3) = g(f(3)) = g(2) = 1$. Therefore, $fg = 321$.

Example 6.3. Let f and g be defined as in the preceding example. Then $(g \cdot f)(1) = f(g(1)) = f(2) = 1$, $(g \cdot f)(2) = f(g(2)) = f(1) = 3$, and $(g \cdot f)(3) = f(g(3)) = f(3) = 2$. Therefore, $gf = 132$.

As these two examples show, multiplication of permutations is *not* a commutative operation, that is, it is *not* true in general that $fg = gf$. The reader may have seen examples of such operations before, such as matrix multiplication. Exercise 11 explains why multiplication of permutations is a special case of that.

Operations involving multiplications of permutations are the subject of the theory of *permutation groups*. Our book walks through Combinatorics, and will not contain a digression to that very interesting field. Some of the exercises at the end of this chapter do relate to the multiplication of permutations, however.

6.1 Cycles in Permutations

Take the permutation 321564. Again, this permutation can be viewed as a function $g : [6] \rightarrow [6]$. Let us take a closer look at g. First, $g(2) = 2$, in other words, 2 is a *fixed point* of the permutation g. Second, $g(1) = 3$, and $g(3) = 1$. This implies in particular that $g^2(1) = 1$, and $g^2(3) = 3$, moreover, $g^3(1) = 3$, and $g^3(3) = 1$, and so on. In other words, if we repeatedly apply g, the elements 1 and 3 will only be permuted among each other, without any interference from the other entries, g^2 has the effect of the identity permutation $12 \cdots n$ on the entries 1 and 3, but g does not. To describe this phenomenon, we will say that 1 and 3 form a *2-cycle* in g. Similarly, $g(4) = 5, g(5) = 6$, and $g(6) = 4$. Iterating g, we see that $g^2(4) = 6, g^2(5) = 4$, and $g^2(6) = 5$. Finally, $g^3(4) = 4$, $g^3(5) = 5$, and $g^3(6) = 6$. Again, we notice that g permutes elements 4, 5, and 6 among each other so that g^3 has the effect of the identity permutation on the entries 4, 5, and 6, but g and g^2 do not. To describe this phenomenon, we will say that 4, 5 and 6 form a *3-cycle* in g.

Before we can formally define cycles, we need the following lemma.

Lemma 6.4. *Let $p : [n] \rightarrow [n]$ be a permutation, and let $x \in [n]$. Then there exists a positive integer $1 \leq i \leq n$ so that $p^i(x) = x$.*

Proof. Consider the entries $p(x), p^2(x), \cdots, p^n(x)$. If none of them is equal to x, then the Pigeon-hole Principle implies that there are two of them that are equal, say $p^j(x) = p^k(x)$, with $j < k$. Then, applying p^{-1} to both sides of this equation, we get $p^{j-1}(x) = p^{k-1}(x)$, repeating this step, we get $p^{j-2}(x) = p^{k-2}(x)$, and repeating this step $j - 3$ more times, we get $p(x) = p^{k-j+1}(x)$. □

Time has come for us to make a formal definition of the notion of cycles in permutations.

Definition 6.5. Let $p : [n] \rightarrow [n]$ be a permutation. Let $x \in [n]$, and let i be the smallest positive integer so that $p^i(x) = x$. Then we say that the entries $x, p(x), p^2(x), \cdots, p^{i-1}(x)$ form an *i-cycle* in p.

Corollary 6.6. *All permutations can be decomposed into the disjoint unions of their cycles.*

Proof. Lemma 6.4 shows that each entry is a member of a cycle. By the definition of cycles, distinct cycles are disjoint. □

Example 6.7. The cycles of 321564 are (31), (2), and (564).

Given the cycle decomposition (31)(2)(564) of g, it is easy to reconstruct g as follows: the image $g(i)$ of i is the entry immediately following i in its cycle, or, if i is the last entry in its cycle, then $g(i)$ is the first entry of that same cycle.

While the cycle decomposition of a permutation f is unique, the same cycle decomposition can be written in many different ways. The convention is to write entries that belong to the same cycle in parentheses. The order of the entries in the parentheses is such that j immediately follows i if $f(i) = j$, and $f(b) = a$, where b is the last entry and a is the first entry in the parentheses. That, in itself, does not preclude multiple notations for the same permutation, however. For instance, (241)(35) and (53)(412) denote the same permutation. In that permutation, $f(2) = 4$, $f(4) = 1$, $f(1) = 2$, $f(3) = 5$, and $f(5) = 3$.

We would like to avoid the danger of confusion caused by the phenomenon we have just described. Therefore, we will write our permutations in *canonical cycle form*. That is, each cycle will be written with its largest element first, and the cycles will be written in increasing order of their first elements. Thus the permutation f of our previous example has canonical cycle form (412)(53).

Recall that besides using the canonical cycle form, we can also write a permutation $f : [n] \rightarrow [n]$ as a *list*, or *linear order*, by simply writing $f(1)f(2)\cdots f(n)$. This is sometimes called the *one-line notation* of permutations.

Example 6.8. Our running example, (412)(53) would be written as 24513 in the one-line notation.

The next section will show the extreme usefulness of our ability to write permutations in two different notations. Figure 6.1 illustrates the two different ways one can think about the same permutation.

The cycle decomposition of a permutation contains a lot of information

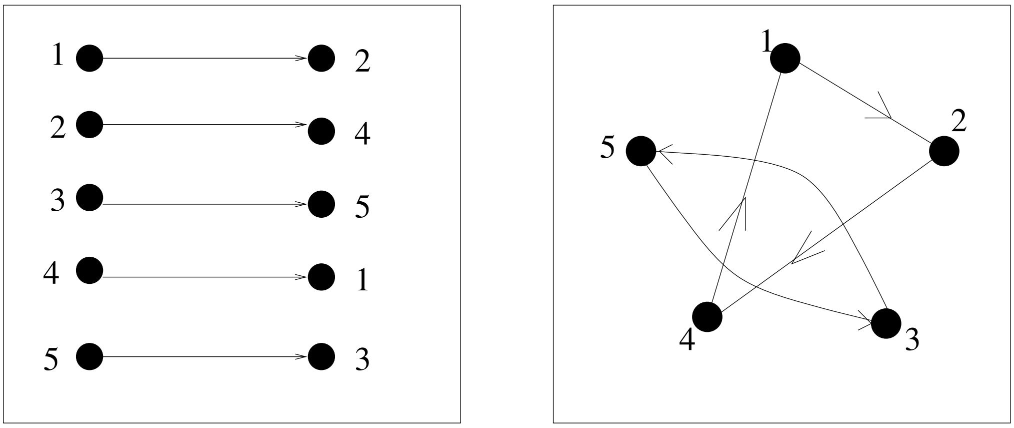

Fig. 6.1 Two ways to look at 24513 = (412)(53).

about the permutation. It is therefore important to enumerate permutations according to their cycle decompositions.

In the rest of this section, all permutations will be taken on the set $[n]$, and for shortness we will call them n-permutations. The set of all n-permutations is denoted by S_n. This is because in group theory, this set is called the *symmetric group*.

Theorem 6.9. *Let $a_1, a_2, \cdots, a_n$ be nonnegative integers so that the equality $\sum_{i=1}^n i \cdot a_i = n$ holds. Then the number of n-permutations with a_i cycles of length i where $i \in [n]$, is*

$$\frac{n!}{a_1!a_2! \cdots a_n! \cdot 1^{a_1} 2^{a_2} \cdots n^{a_n}}. \tag{6.1}$$

Proof. Write down all elements of $[n]$ in a row in some order, then insert parentheses going left to right, according to the required cycle lengths: first a_1 pairs of parentheses creating a_1 1-cycles, then a_2 pairs of parentheses creating a_2 2-cycles, and so on. This way we obtain a permutation in which the cycle lengths are nondecreasing left to right.

There are $n!$ ways to do this- that is the number of ways to write down the elements of $[n]$, and there is only one way to insert the parentheses in the described manner. However, there are several ways of writing down the n integers that will lead to the same permutation once the parentheses are inserted. We must figure out how many.

The elements within any cycle of length i can be in i different orders and still yield the same cyclic permutation. Therefore, every permutation can be obtained at least $\Pi_{i=1}^n i^{a_i}$ times as there are a_i cycles of size i. Moreover, if two ways of writing down the elements of $[n]$ result in permutations which have the exact same cycles of length i for all i, just in different order, then again they lead to the same permutation. As a_i cycles can be permuted in $a_i!$ different ways, and permuting the cycles can be done independently from the order of the elements within the cycles, we have shown that each permutation can be obtained $\Pi_{i=1}^{n} i^{a_i} a_i!$ ways, and the proof follows. □

If an n-permutation p has a_i cycles of length i, for $i = 1, 2, \cdots, n$, then we say that $(a_1, a_2, \cdots, a_n)$ is the *type* of p. Thus (6.1) provides a formula for the number of permutations with a given type.

Example 6.10. The number of n-permutations having only one cycle, in other words, the number of n-permutations of type $(0, 0, \cdots, 0, 1)$ is equal to $(n-1)!$.

One combinatorial meaning of Example 6.10 is this. The number of ways n people can sit around a table is $(n-1)!$. (We consider two seating assignments identical if everyone has the same left neighbor in the first seating as in the second.)

Now we are in a position to fulfill an old promise, namely we can define the Stirling numbers of the first kind.

Definition 6.11. The number of n-permutations with k cycles is called the (n, k) *signless Stirling number* of the first kind, and is denoted by $c(n, k)$. The number $s(n, k) = (-1)^{n-k} c(n, k)$ is called the (n, k) *Stirling number of the first kind.*

We will explain the reason for including $(-1)^{n-k}$ in the definition of $s(n, k)$ shortly. It will not surprise anyone that $c(n, 0) = 0$ if $n > 0$ as nonempty permutations all have cycles. Moreover, we set $c(0, 0) = 1$, and $c(n, k) = 0$ if $n < k$, just as it was the case with the Stirling numbers of the second kind.

Similarly to the numbers $S(n, k)$, the numbers $c(n, k)$ also satisfy a simple recurrence relation.

Theorem 6.12. *Let n and k be positive integers satisfying $n \geq k$. Then*

$$c(n, k) = c(n-1, k-1) + (n-1)c(n-1, k). \tag{6.2}$$

Proof. We show that the right-hand side counts all n-permutations with k cycles, just as the left-hand side. In such a permutation, there are two possibilities for the position of the entry n.

(1) The entry n can form a cycle by itself, and then the remaining $n-1$ entries have to form $k-1$ cycles. This can happen in $c(n-1, k-1)$

ways, so the first member of the right-hand side of (6.2) enumerates these permutations.

(2) If the entry n does not form a cycle by itself, then the remaining $n-1$ entries must form k cycles, and then the entry n has to be inserted somehow into one of these cycles. The k cycles can be formed in $c(n-1,k)$ ways, then the entry n can be inserted in any of these cycles, after each element. This multiplies the number of possibilities by $n-1$, and explains the second term of the right-hand side of (6.2).

Readers should test their understanding by trying to explain why we did not miss any permutations by inserting n after each entry in each cycle, and not into the front of each cycle. □

The reader is probably wondering whether there is some strong connection between the Stirling numbers of the first kind and the Stirling numbers of the second kind that justifies the similar names. The following Lemma is our main tool in establishing that connection.

Lemma 6.13. *Let n be a fixed positive integer. Then*

$$\sum_{k=0}^{n} c(n,k)x^k = x(x+1)\cdots(x+n-1). \tag{6.3}$$

Proof. We prove that the coefficients of x^k on the right-hand side also satisfy the recursive formula (6.2) that is satisfied by the signless Stirling numbers of the first kind.

Let $G_n(x) = x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} a_{n,k}x^k$. Then

$$G_n(x) = (x+n-1)G_{n-1}(x) = (x+n-1)\sum_{k=0}^{n-1} a_{n-1,k}x^k$$
$$= \sum_{k=1}^{n} a_{n-1,k-1}x^k + (n-1)\sum_{k=0}^{n-1} a_{n-1,k}x^k.$$

Now we are using a technique that will return in countless applications in Chapter 8. We have just proved that

$$\sum_{k=0}^{n} a_{n,k}x^k = \sum_{k=1}^{n} a_{n-1,k-1}x^k + (n-1)\sum_{k=0}^{n-1} a_{n-1,k}x^k.$$

In other words, we proved that two *polynomials* were identical. The only way that can happen is when the coefficients of the corresponding terms agree in the two polynomials. That is, the equality

$$a_{n,k} = (n-1)a_{n-1,k-1} + a_{n-1,k}$$

must hold for all positive integers n and k so that $n \geq k$. Therefore, the numbers $a_{n,k}$ and $c(n,k)$ do satisfy the same recurrence relation. As their initial terms trivially agree, that is, $c(0,0) = a_{0,0} = 1$, $c(n,0) = a_{n,0} = 0$ if $n > 0$, this implies that $c(n,k) = a_{n,k}$. □

Let us replace x by $-x$ in (6.3), and multiply both sides by $(-1)^n$. We get

$$\sum_{k=0}^{n} s(n,k)x^k = (x)_n. \tag{6.4}$$

Now the reader can see why we included the term $(-1)^{n-k}$ in the definition of $s(n,k)$. Comparing this equation to (5.2), that stated

$$x^n = \sum_{k=0}^{n} S(n,k)(x)_k,$$

we see that the Stirling numbers of the first kind have the "inverse effect" of the Stirling numbers of the second kind. To formulate this observation in a more precise way, we need some notions from linear algebra, and we will assume that the reader has taken a basic course in that field.

It is well-known that the set of all polynomials with real coefficients is a vector space V over the field of real numbers. The most obvious basis of V is $B = \{1, x, x^2, x^3, \cdots\}$, but it is not the only interesting basis. It is easy to show that $B' = \{1, (x)_1, (x)_2, (x)_3, \cdots\}$ is also a basis of V.

Now let S (resp. s) be the infinite matrix whose entry in position (n,k) is $S(n,k)$ (resp. $s(n,k)$). Then (6.4) shows that s is the transition matrix from B to B', while (5.2) shows that S is the transition matrix from B' to B. This proves the promised connection between the two different kinds of Stirling numbers.

Theorem 6.14. *The matrices S and s are inverses of each other, that is, $Ss = sS = I$.*

6.2 Permutations with Restricted Cycle Structure

The following lemma turns the canonical cycle form into a very powerful tool.

Lemma 6.15. *[Transition Lemma] Let $p : [n] \rightarrow [n]$ be a permutation written in canonical cycle notation. Let $g(p)$ be the permutation obtained from p*

by omitting the parentheses and reading the entries as a permutation in the one-line notation. Then g is a bijection from the set S_n of all permutations on $[n]$ onto S_n.

Example 6.16. Let p be our running example, that is, $p = (412)(53)$. Then w $g(p) = g((412)(53)) = 41253$.

Solution. It suffices to show that for each permutation $q = q_1q_2 \cdots q_n$ written in the one-line notation, there exists exactly one permutation $p \in S_n$ so that $q = g(p)$. In other words, we have to show that there is exactly one way to insert parentheses into the string $q = q_1q_2 \cdots q_n$ so that we get a permutation in canonical cycle form.

To see this, note that q_1 certainly starts a new cycle, so the first left parenthesis has to be inserted to the front of the string. Where will this first cycle end? As we are looking for a permutation in canonical cycle form, q_1 has to be the largest of its cycle. Therefore, if i is the smallest index so that $q_1 < q_i$, then the first cycle has to end before q_i. On the other hand, if $j < i$, then the second cycle cannot start with q_j as we know that $q_j < q_1$, and the cycles have to be in increasing order of their first elements. This implies that the second cycle has to start with q_i, and thus we have to insert the first right parenthesis, and the second left parenthesis between q_{i-1} and q_i.

Then we can continue this deterministic procedure to find all our cycles. By an analogous argument, we have to start a new cycle at q_k if and only if q_k is larger than the leading entries of all previous cycles, which means in particular that q_k is larger than all entries on its left. As these entries are uniquely determined by q, the preimage $g^{-1}(q)$ of q exists and is unique.

Example 6.17. The preimage of 4356172 under g is (43)(5)(61)(72).

The entries of q that are larger than all entries on their left are called *left-to-right maxima*. Note that if q has t left-to-right maxima, then $g^{-1}(q) = p$ has t cycles. Also note that the leftmost left-to-right maximum of q is always q_1, and the rightmost left-to-right maximum of q is always the entry n. A surprising application of Lemma 6.15 is the following.

Proposition 6.18. *Let i and j be two elements of $[n]$. Then i and j are in the same cycle in exactly half of all n-permutations.*

Proof. As we can relabel our entries by switching n and i, and switching $n-1$ and j, it is sufficient to prove that the entries n and $n-1$ are in the same cycle in exactly half of all n-permutations. Let $q = q_1 q_2 \cdots q_n$ be an n-permutation, and let $g(p) = q$, where g is the bijection of Lemma 6.15. As we said, the entry n of q is always a left-to-right maximum, namely the rightmost left-to-right maximum of q. Therefore, the last cycle of p starts with n, and the entries in that cycle of q are precisely the entries on the right of n in q.

Therefore, p contains n and $n-1$ in the same cycle if and only if $n-1$ is on the right of n in q. As that happens in half of all n-permutations, the proof follows. □

The following surprising result shows that the likelihood that a given entry i is part of a k-cycle is independent of k. In fact, it is $1/n$.

Lemma 6.19. *Let $i \in [n]$. Then for all $k \in [n]$, there are exactly $(n-1)!$ permutations of length n in which the cycle containing i is of length k.*

Proof. Again, it is sufficient to prove the statement for $i = n$, then the general statement follows by relabeling. Let $q = q_1 q_2 \cdots q_n$ be an n-permutation, let $g(p) = q$, where g is the bijection of Lemma 6.15, and let $q_j = n$. Then the cycle C containing n in p is of length $n - j + 1$ as n itself starts the last cycle. So if we want C to have length k, we must have $j = n + 1 - k$. However, there are clearly $(n-1)!$ permutations of length n that contain n in a given position, and the proof follows. □

Theorem 6.9 tells us how to compute the number of permutations of a given type. Sometimes we do not exactly know the type of our permutations, but we at least know something about it. As it turns out, we can still enumerate the relevant permutations in many cases. In what follows, we will show a nice example for that. Other examples can be found in the Exercises.

Let $ODD(m)$, resp. $EVEN(m)$ be the set of m-permutations with all cycle lengths odd, resp. even.

Lemma 6.20. *For all positive integers m, the equality $|ODD(2m)| = |EVEN(2m)|$ holds.*

Proof. We construct a bijection Φ from $ODD(2m)$ onto $EVEN(2m)$.

Let $\pi \in ODD(2m)$. Then π consists of an even number $2k$ of odd cycles. Denote by $C_1, C_2, \cdots, C_{2k}$ the cycles in canonical order. For all i, $1 \leq i \leq k$, take the last element of C_{2i-1}, and put it to the end of C_{2i} to get $\Phi(\pi)$, the image of π.

Example 6.21. *If* $p = (4)(513)(726)(8)$, *then* $\Phi(p) = (5134)(72)(86)$.

Note that if C_{2i-1} is a singleton, it disappears. Also note that the canonical form is maintained.

We claim that Φ is a bijection from $ODD(2m)$ onto $EVEN(2m)$. Let $\sigma \in EVEN(2m)$, with cycles $c_1, c_2, \cdots, c_h$. To prove that Φ is a bijection, it suffices to show that we can recover the only permutation $\pi \in ODD(2m)$ for which $\Phi(\pi) = \sigma$.

While recovering π, we must keep in mind that it might have more than h cycles, because some of its singletons might have been absorbed by the cycles immediately after them. If the last value in c_h is larger than the first value in c_{h-1}, then create a singleton cycle with this value, placing it in front of c_h and repeat the whole procedure using c_{h-2} and c_{h-1}. Otherwise, move this value from c_h to the end of c_{h-1} and repeat the whole procedure using c_{h-3} and c_{h-2}. If at any point only one cycle remains, create a singleton cycle with the last value in that cycle. It is then straightforward to check that the permutation π obtained this way fulfills $\Phi(\pi) = \sigma$. It also follows from the simple structure of Φ that at no point of the recovering procedure could we have done anything else. □

Example 6.22. The preimage of $(41)(62)(75)(83)$ under Φ is $(412)(6)(753)(8)$.

Example 6.23. The preimage of $(21)(53)(64)(87)$ under Φ is $(1)(2)(534)(6)(7)(8)$.

Now that we so nicely proved that $|ODD(2m)| = |EVEN(2m)|$, we may well ask if there is a formula describing these numbers. The following Theorem answers that question in the affirmative, and has a touch of surprise in it. Would you have thought that the number of these permutations is always a perfect square?

Theorem 6.24. *For all positive integers* m,

$$|ODD(2m)| = |EVEN(2m)| = 1^2 \cdot 3^2 \cdot 5^2 \cdots (2m-1)^2. \qquad (6.5)$$

Solution. Because of Lemma 6.20, it suffices to prove the second equality. Let p be an n-permutation with even cycles only. Clearly, we cannot have $p(1) = 1$, as that would mean that the entry 1 forms a 1-cycle in p. So there are $2m-1$ choices for $p(1)$. Then there are $2m-1$ choices for $p^2(1) = p(p(1))$ as we can choose everything but $p(1)$ itself.

So far we have chosen $p(1)$ and $p(p(1))$. These two elements will either form a 2-cycle (when $p(p(1)) = 1$), or they will not. In either case, we will have $2m-3$ choices for the image of the next entry. That is, if 1 and $p(1)$ form a 2-cycle, and i is an element outside that cycle, then we have $2m-3$ choices for $p(i)$. Indeed, we can choose anything except 1, $p(1)$, these have already been chosen, and $p(i)$, as that would mean that i is a 1-cycle. If, on the other hand 1 and $p(1)$ do not form a 2-cycle, then we choose the next element of their cycle, $p^3(1)$ next. The entry $p^3(1)$ cannot be $p(1)$ and $p^2(1)$ as those elements are already chosen, and cannot be 1 either as that would create the 3-cycle $(1, p(1), p^2(1))$. Thus there are $2m-3$ choices for the next element in this case too.

Continuing this line of argument, we see that selecting our $(2i-1)$st entry we always have $2m-2i+1$ choices, and selecting our $2i$th entry we always have $2m-2i+1$ choices, (as we can close cycles of even length), and the proof follows.

Thus we have a formula for $|ODD(n)|$ if n is even. If n is odd, then clearly, $|EVEN(n)| = 0$, but we can still enumerate $|ODD(n)|$.

Theorem 6.25. *For all positive integers m,*

$$|ODD(2m+1)| = (2m+1) \cdot |ODD(2m)| = 1^2 \cdot 3^2 \cdot 5^2 \cdots (2m-1)^2(2m+1). \tag{6.6}$$

Proof. We construct a bijection Ψ from $ODD(2m) \times [2m+1]$ onto $ODD(2m+1)$. In this bijection, we will need the notion of a *gap position.* This notion will be useful to solve some of the exercises, too. An m-permutation has $m+1$ gap positions, one *before* each element in each cycle, and one at the very end of the permutation, after all entries.

Example 6.26. *The permutation* $(42)(513)$ *has six gap positions, indicated by bars in the following array:* $(|4|2)(|5|1|3|)$.

Let $\pi \in ODD(2m)$, and let $k \leq 2m+1$ be a positive integer. We define $\Psi(\pi, k)$ as follows. First, take $\Phi(\pi)$, where Φ is the bijection of Lemma 6.20. Insert the new entry $2m+1$ to the kth gap position of $\Phi(\pi)$. That will change one cycle to an odd cycle. Run the remaining cycles through Φ^{-1} to get odd cycles. This way we obtain a $(2m+1)$-permutation consisting of odd cycles only, and that permutation is our $\Psi(\pi)$.

Lemma 6.27. *The map Ψ defined above is a bijection from the set $ODD(2m) \times [2m+1]$ onto the set $ODD(2m+1)$.*

Proof. To find the reverse of Ψ, take $\pi' \in ODD(2m+1)$, put the cycle in π' which contains $(2m+1)$ aside, run what's left through Φ to get even cycles. Read off k as the gap position in which $(2m+1)$ is. Remove $(2m+1)$ from its odd cycle, and run all the obtained permutation, which has all even cycles, through Φ^{-1}, to get $\Psi^{-1}(\pi')$. Note that at every step, we have reversed the corresponding step of Ψ. □

This completes the proof of the theorem. □

Notes

A fair part of the results in Section 6.2 were obtained after Herb Wilf asked some intriguing questions in [43]. Most of the results presented here have been generalized in [10]. For example, it has been proved that if p is prime, then the ratio of n-permutations that have a pth root to all n-permutations is steadily decreasing, and converges to zero. See Exercises 21 and 22 for the relevant definitions.

Exercises

(1) Is it true that $c(n, n-1) = S(n, n-1)$?

(2) Find a formula for $c(n, n-2)$.

(3) Compute the values of $c(5, k)$, for $k = 1, 2, 3, 4, 5$.

(4) Prove that for any fixed k, the function $c(n, n-k)$ is a polynomial function of n. What is the degree of that polynomial?

(5) Let $r(n)$ be the number of n-permutations whose square is the identity permutation. Prove that if $n \geq 1$, then $r(n+1) = r(n) + nr(n-1)$, where $r(0) = 1$.

(6) Find a recursive formula for the number $t(n)$ of n-permutations whose cube is the identity permutation.

(7) Prove that on average, permutations of length n have H_n cycles, where

$$H_n = \sum_{i=1}^{n} \frac{1}{i}.$$

(8) How many n-permutations contain entries 1, 2 and 3 in the same cycle?

(9) An alpine sky team has n members. They descend a particular slope one by one every day, and no two of them ever record identical times.

On an average day, how many times will the best record of that day be broken?

(10) An airplane has n seats, and all of them have been sold for a particular flight, with no overbooking. When the last passenger arrives, he finds that his seat is taken. When he shows his reservation to the passenger at his seat, that passenger stands up, and goes to her own assigned seat. If that seat is empty, she seats down, and the seating procedure is over. If not, she shows her reservation to the person seating at that seat. That person stands up, and goes to his assigned seat, and so on. This procedure continues until someone finds his or her assigned seat empty.

Tom was not the last passenger to board the plane. What is the probability that he has to move during this procedure?

(11) Let p be an n-permutation. We associate a *permutation matrix* A_p to p as follows. Let $A_p(i,j) = 1$ if $p(i) = j$, and let $A_p(i,j) = 0$ otherwise. Here $A_p(i,j)$ denotes the entry of A_p that is in the intersection of the ith row and the jth column. Prove that $|\det A| = 1$.

(12) Prove that if p and q are two n-permutations, then $A_pA_q = A_{pq}$.

(13) The *inverse* of an n-permutation is the permutation q for which $pq = qp = 123\cdots n$. We then write $q = p^{-1}$. Prove that each permutation has a unique inverse.

(14) Prove that permutations f and f^{-1} are of the same type.

(15) What is the combinatorial meaning of A_p^T?

(16) In permutations, 1-cycles are often called fixed points. Prove, using permutation matrices, that permutations pq and qp always have the same number of fixed points.

(17) Assume we know the type $(a_1, a_2, \cdots, a_n)$ of an n-permutation. Determine the smallest positive integer d such that $p^d = 123\cdots n$.

(18) A permutation p is called a nontrivial *involution* if $p^2 = 12\cdots n$, but $p \neq 12\cdots n$. Prove that if $n > 1$, then the number of nontrivial involutions in S_n is odd.

(19) Generalize the previous exercise for all prime numbers t.

(20) Let $n \geq 2$. Prove that $\det A_p = 1$ for exactly one half of all n-permutations p.

(21) We say that a permutation $p \in S_n$ has a square root if there is a permutation $q \in S_n$ so that $q^2 = p$. Find a sufficient and necessary condition of p having a square root, in terms of its cycle lengths.

(22) We say that a permutation $p \in S_n$ has a kth root if there is a permutation $q \in S_n$ so that $q^k = p$. Is the following statement true?

"A permutation has a kth root if and only if it is of type $(a_1, a_2, \cdots, a_n)$, and whenever i is divisible by k, a_i is divisible by k."

(23) + Construct a bijection

$$\tau : ODD(2m+1) \times [2m+1] \rightarrow ODD(2m+2).$$

(24) ++ Let $SQ(n)$ be the set of n-permutations having at least one square root. Prove that for all positive integers n, we have $|SQ(2n)| \cdot (2n+1) = |SQ(2n+1)|$. Note that this means that $p(2n) = p(2n+1)$, where $p(m)$ denotes the probability that a randomly chosen m-permutation has a square root.

(25) Let k, m, and r be positive integers, and let $kr = m$. Prove that the number of n-permutations all of whose cycle lengths are divisible by k is

$$1 \cdot 2 \cdots (k-1)(k+1)^2(k+2) \cdots (2k-1)(2k+1)^2(2k+2) \cdots (m-1)$$

$$= \frac{m!}{k^r r!} \cdot (k+1)(2k+1) \cdot ((r-1)k+1).$$

Supplementary Exercises

(26) A group of ten children want to play cards. They split into three groups, one of these groups has four children in it, the other two have three each. Then each group sits around a table. Two seatings are considered the same if everyone's left neighbor is the same.

(a) In how many ways can this be done if the three tables are identical?

(b) In how many ways can this be done if the three tables are distinct?

(27) Let $p = p_1 p_2 \cdots p_n$ be a permutation. An *inversion* of p is a pair of entries (p_i, p_j) so that $i < j$ but $p_i > p_j$.

Let us call a permutation *even* (resp. *odd*) if it has an even *resp. odd* number of inversions.

Prove that the permutation consisting of the one cycle $(a_1 a_2 \cdots a_k)$ is even if k is odd, and is odd if k is even.

(28) Find a combinatorial proof for the fact that there are $n!/2$ even n-permutations.

(29) What is the relation between the parity of a permutation p and $\det A_p$?

(30) Assume we only know the type of the n-permutation p. How can we decide whether p is odd or even?

(31) Let us assume that we know the length n of a permutation p, and the number k of its cycles. Can we figure out from these data whether p is an odd or an even permutation?

(32) Prove the result of Supplementary Exercise 28 by an appropriate substitution into formula (6.3).

(33) How many permutations $p \in S_6$ satisfy $p^3 = 1$?

(34) How many even permutations $p \in S_6$ satisfy $p^2 = 1$?

(35) Let n be divisible by 3. Prove that $c(n, n/3) \geq \frac{n!}{3^{n/3}(n/3)!}$.

(36) Prove that for all positive integers n, r and k such that $n = rk$, the inequality

$$(r-1)!^k \leq \frac{c(n,k)}{S(n,k)} \leq (n-k)!$$

holds.

(37)(a) Prove that in the polynomial

$$(1+x)(1+2x)\cdots(1+(n-1)x)$$

the coefficient of x^{n-k} is $c(n,k)$, for all $k \in n$.

(b) State and prove the corresponding fact for the numbers $s(n,k)$.

(38) Let $a(n,k)$ be the number of permutations of length n with k cycles in which the entries 1 and 2 are in the same cycle. Prove that for $n \geq 2$,

$$\sum_{k=1}^{n} a(n,k)x^k = x(x+2)(x+3)\cdots(x+n-1).$$

(39) + Let $b_r(n,k)$ be the number of permutations of length n with k cycles in which all entries of $[r]$ are in the same cycle. Prove that for $n \geq r$,

$$\sum_{k=1}^{n} b_r(n,k)x^k = (r-1)!\frac{x(x+1)\cdots(x+n-1)}{(x+1)(x+2)\cdots(x+r-1)}.$$

(40) Let $a(n,k)$ be defined as in Supplementary Exercise 38. Let $t(n,k) = c(n,k) - a(n,k)$ be the number of permutations of length n with k cycles in which the entries 1 and 2 are *not* in the same cycle. Prove that $a(n,k) = t(n,k+1)$, for all $k \leq n-1$.

(41) A group of n tourists arrive at a restaurant. They sit down around circular tables, leaving no table empty. Then each table orders one of r possible drinks. Prove that the number of ways this can happen is

$$r(r+1)\cdots(n+r-1).$$

Two seating arrangements are considered the same if each person has the same left neighbor in both of them.

(42) We write each element of $[n-1]$ on a separate card, then randomly select any number of cards, and take the product of the numbers of written on them. Then we do this for all 2^{n-1} possible subsets of the set of $n-1$ cards. (The empty product is taken to be 1.) Finally, we take the sum of the 2^{n-1} products we obtained. What is this sum?

(43) Modify the previous exercise so that instead of considering all 2^{n-1} subsets, we only consider all k-element subsets of the $n-1$ cards. What is the sum of all $\binom{n-1}{k}$ products we obtain in that scenario?

(44) Find a recursive formula for the number $u(n)$ of n-permutations whose fourth power is the identity permutation.

(45) A library has n books. Readers of this library are "almost" careful. That is, after reading a book, they put it back to its shelf, missing its proper place by only one notch. Prove that after a sufficient amount of time, any permutation of the books on the shelves can occur.

(46) Prove that two n-permutations p and q have the same type if and only if there exists an n-permutation g so that $q = gpg^{-1}$ holds.

(47) Inversions of a permutation were defined in Supplementary Exercise 27. Let $I(n,k)$ be the number of n-permutations that have k inversions. Prove that $I(n,k) = I(n, \binom{n}{2} - k)$.

(48) Let $I(n,k)$ be defined as in the previous exercise. Prove that

$$\sum_{k=0}^{\binom{n}{2}} I(n,k)x^k = (1+x)(1+x+x^2)\cdots(1+x+\cdots+x^{n-1}).$$

(49) Deduce from the result of the previous exercise that the number of even n-permutations is the same as the number of odd n-permutations. (See Supplementary Exercise 27 for the definition of even and odd permutations.)

(50) Find an explicit formula for $I(n,3)$.

Solutions to Exercises

(1) Yes, that is true. $S(n,n-1)$ is the number of ways to partition $[n]$ into one doubleton and $n-2$ singletons. To get $c(n,n-1)$, we have to take a permutation consisting of one cycle on each of these $n-1$ subsets. There is only one way to do this, thus $c(n,n-1) = S(n,n-1) = \binom{n}{2}$.

(2) An n-permutation that has $n-2$ cycles can have either two 2-cycles, or one 3-cycle, and the rest must be all 1-cycles. In the first case, we

can choose the elements of the first 2-cycle in $\binom{n}{2}$ ways, the elements of the second 2-cycle in $\binom{n-2}{2}$ ways, then take a 2-cycle on each of them in one way. This yields $\binom{n}{2} \cdot \binom{n-2}{2}/2$ permutations as the order of the cycles is irrelevant. In the second case, we have to choose the elements of the 3-cycle in $\binom{n}{3}$ ways, then take a 3-cycle on them in 2 ways. This yields $2\binom{n}{3}$ permutations, and proves that

$$c(n, n-2) = \frac{n(n-1)(n-2)(n-3)}{8} + \frac{n(n-1)(n-2)}{3}.$$

(3) It follows from (6.10) that $c(5,1) = 4! = 24$. Exercise 1 shows that $c(5,4) = \binom{5}{2} = 10$, and Exercise 2 shows that $c(5,3) = 15 + 20 = 35$. It is obvious that $c(5,5) = 1$. As $\sum_{k=1}^{5} c(5,k) = 5! = 120$, the equality $c(5,2) = 50$ follows.

(4) We prove the statement by induction on k. If $k = 1$, then the statement is true by Exercise 1. Now assume we know the statement for $k-1$. This implies

$$c(n, n-k) = c(n-1, n-k-1) + (n-1)c(n-1, n-k),$$

$$c(n, n-k) - c(n-1, n-k-1) = (n-1)c(n-1, n-k).$$

Here the right-hand side is a polynomial by the induction hypothesis, and therefore so is the left-hand side. However, the left-hand side is the difference of two consecutive values of $c(n, n-k)$, therefore $c(n, n-k)$ must be a polynomial by Exercise 1 of Chapter 2. Similarly, the degree of $c(n, n-k)$ is $2n$, by this same inductive setup, and Exercise 1 of Chapter 2.

(5) In such permutations, all cycles must be 1-cycles or 2-cycles. If the entry $n+1$ forms a 1-cycle, then the remaining n entries can form a good permutation in $r(n)$ ways. If the entry $n+1$ is part of a 2-cycle, then there are n choices for the other entry of that 2-cycle, then there are $r(n-1)$ ways for the remaining $n-1$ entries to form a good permutation.

(6) This is similar to the previous exercise. All cycles of such permutations have length one or three. If $n+1$ is in a 3-cycle, then there are $\binom{n}{2}$ choices for the other two elements of the cycle, and there are 2 choices for the cycle itself, once its elements are known. Then the remaining entries can form a good permutation in $t(n-2)$ ways. If the entry $n+1$ forms a 1-cycle, then the remaining n entries can form a good permutation in $t(n)$ ways. Therefore, $t(n+1) = n(n-1)t(n-2) + t(n)$ if $n \geq 3$.

(7) We prove the statement by induction on n. For $n = 1$, the statement is true. Assume it is true for $n-1$. There is $1/n$ chance that entry 1 forms a 1-cycle, and then the remaining $n-1$ elements form H_{n-1} cycles on average. If entry 1 does not form a 1-cycle, then, take any permutation of the elements $\{2, 3, 4, \cdots, n\}$ in the canonical distribution. Insert entry 1 after any of these elements. This will not change the number of cycles as entry 1 will not start a new cycle. Therefore, the number of permutations with k cycles stays the same for all k, so their average stays the same, too, i.e. $H(n-1)$. Therefore, we get

$$H(n) = \frac{1}{n} \cdot (H(n-1) + 1) + \frac{n-1}{n} \cdot H(n-1) = H(n-1) + \frac{1}{n},$$

and the statement follows.

(8) Entries 1, 2, and 3 are together in one cycle exactly as often as elements $n-2, n-1, n$ are. This latter happens exactly when, after omitting all parentheses from the cycle notation, n precedes both $n-2$ and $n-1$. And that clearly happens in $1/3$ of all permutations. So the probability in question is $1/3$.

(9) This is the same as to ask that on average, how many left-to-right minima does a random n-permutation have. In accordance with the paragraph following Example 6.17, a left-to-right minimum is an entry of a permutation $p = p_1 \cdots p_n$ that is smaller than all entries on its left.

(10) If $1, 2, \cdots, n$ denote the passengers, and $f(1), f(2), \cdots, f(n)$ denote their assigned seats, then it is clear that $f(1)f(2)\cdots f(n)$ is a permutation. Tom will have to move if and only if in this permutation, his seat is part of the same cycle as the seat $f(n)$ of passenger n, who arrived last. We know from Proposition 6.18 that the chance of that is one half.

Exercise 7, and the paragraph following Example 6.17 tell us that for left-to-right *maxima*, the answer is $H(n) = \sum_{i=1}^{n} \frac{1}{n}$. To see that this is also the answer for left-to-right minima, note that $p_1p_2\cdots p_n$ has t left-to-right minima if and only if the permutation $q = q_1q_2\cdots q_n$, where $q_i = n + 1 - p_i$, has t left-to-right maxima. By the way, q is called the *complement* of p.

(11) That is true as each row and column will have exactly one nonzero member. Therefore, when expanding the determinant by any row or column, we will only obtain one nonzero product. That product will be the product of many ones, so the only open question is whether

that product will occur in the determinant with a positive sign or with a negative sign. That depends on p.

(12) Consider $(A_pA_q)(i,j)$. By the definition of matrix multiplication, this is the inner product of the ith row of A_p and the jth column of A_q. As both of these vectors have exactly one nonzero element in them, their inner product will be 1 if and only if those nonzero elements occur in the (same) kth position in both vectors. That, however, happens if and only if $p(i) = k$, and $q(k) = j$, which is also equivalent to $pq(i) = j$. Therefore, $(A_pA_q)(i,j) = A_{pq}(i,j)$.

(13) The n-permutation q is the inverse of the n-permutation p if and only if $p(i) = j$ implies $q(j) = i$. This relation uniquely defines q.

(14) Reversing each cycle of p results in p^{-1}.

(15) If $p(i) = j$, then $A_p(i,j) = 1$, so $A_p^T(j,i) = 1$. Therefore, A_p^T defines a permutation q in which $q(j) = i$ if and only if $p(i) = j$. This means $pq = qp = 12\cdots n$, so q is the inverse of p. Thus the transpose of a permutation matrix is the permutation matrix of the inverse of the original permutation. This also implies $A_pA_p^T = I$.

(16) The number of fixed points of a permutation can be read off its permutation matrix as the number of ones in the main diagonal. As the remaining entries of the main diagonal are zeros, the number of ones in the main diagonal also equals the sum of diagonal elements, which is called the *trace* of the matrix. It is well known in Linear Algebra that $\mathit{trace}(AB) = \mathit{trace}(BA)$ for all $n \times n$ matrices A and B. Therefore,

$$\mathit{trace}(A_pA_q) = \mathit{trace}(A_qA_p),$$

and the claim is proved.

(17) The smallest positive integer d with that property is the least common multiple of the cycle lengths of the permutation, that is, the indices i so that $a_i > 0$. Indeed, the kth, $2k$th, etc. powers of a k-cycle are equal to the identity permutation.

(18) If $n > 1$, then $n!$ is even. Let us arrange all n-permutations into pairs, by placing p and p^{-1} in the same pair. That will create a t pairs, containing altogether $2t$ permutations, but will not match involutions and $12\cdots n$ to anything. Thus the number of these latter is $n! - 2t$, therefore the number of involutions is $n! - 2t - 1$, and that is an odd number.

(19) If t is prime, and $n \geq t$, then the number of n-permutations p so that $p^t = 12\cdots n$, but $p \neq 12\cdots n$ is congruent to -1 modulo t. The proof is analogous to that of the previous exercise.

(20) Consider $(21) = (21)(3)(4)\cdots(p)$, the permutation that simply swaps the first two entries. For any $p \in S_n$, we define $h(p) = (12)p$. As $\det A_{(12)} = -1$, the matrices A_p and $A_{h(p)}$ have determinants of opposite signs. On the other hand, $h(h(p)) = p$, therefore h creates pairs of permutations $(p, h(p))$. Each pair will contain exactly one permutation whose matrix has determinant 1, and the claim is proved.

(21) Let $r \in S_n$, and consider r^2. It is straightforward to verify that if k is odd, then the k-cycles of r will stay k-cycles in r^2, and if k is even, the k-cycles of r will split into two $\frac{k}{2}$-cycles in r^2. So the only way r^2 can have even cycles is by obtaining them from an even cycle of r, that has split into two cycles of the same size, each of them even. Therefore, r^2 will have an even number of cycles of each even length. On the other hand, we claim that this is sufficient. That is, if p has an even number of cycles of each even length, then p has a square root. Indeed, if p has even cycles $(a_1 \cdots a_t)$ and $(b_1 \cdots b_t)$, then they can be obtained by taking the square of the $(2t)$-cycle $(a_1b_1a_2b_2a_3\cdots a_tb_t)$. Odd cycles of p, such as $(d_1d_3d_5\cdots d_kd_2d_4\cdots d_{k-1})$ can be obtained as the square of $(d_1d_2\cdots d_k)$. After finding square roots for all cycles of p, a good choice for the square root of p is the product of those cycles.

We have proved that p has a square root if and only if p has an even number of cycles of each even length.

(22) No, that is not true in this generality. The claim is true if k is prime, and in that case, it can be proved the same way the previous exercise was proved.

If k is not prime, however, then the statement is not true. For instance, if $k = 4$, then the requirements do not say anything about the number of 2-cycles of p. Thus $p = (21)(3)(4)(5)\cdots(n)$ would have to have a fourth root. That is clearly impossible, however, as this p does not even have a square root. (If there were a q so that $q^4 = p$, then q^2 would be a square root of p.) The reader is invited to construct a similar counterexample for a generic composite number k.

(23) Take a pair $(\pi, k) \in ODD(2m+1) \times [2m+1]$, and insert $2m+2$ to the kth gap position. Note that this implies $2m+2$ cannot create a singleton cycle as it cannot go to the last gap position. Take away the cycle C containing $2m+2$, and run Φ (of Lemma 6.20) through the remaining cycles. Then, together with C, we have a permutation in $EVEN(2m+2)$. Run it through Φ^{-1} to get $\tau(\pi, k) \in ODD(2m+2)$.

(24) We are going to construct a bijection κ from $SQ(2n) \times [2n+1]$ onto

$SQ(2n+1)$. As the growth of $|SQ(n)|$ is equal to that of $|ODD(n)|$ when passing from an even n to an odd $n+1$, we try to integrate Ψ of Lemma 6.27 into κ, by "stretching" the odd cycles part of our permutations. We proceed as follows.

Let $(\pi, k) \in SQ(2n) \times [2n+1]$. Take π, and break it into even cycles part and odd cycles part, or, for short, *odd part* and *even part.* Again, let k mark a gap position in π. If this gap position is in the odd cycles, or at the end of π, then interpret the gap position as a gap position for the odd part only, and simply run the odd part and this gap position through Ψ to get $\kappa(\pi)$, together with the unchanged even parts. Note that $2n+1$ will appear in an odd cycle when we are done.

If the gap position marked by k is in one of the even cycles, say c, we can think of it as marking the member of c immediately following it, say x. Replace x by $2n+1$ in c. To keep the information encoded by x, we interpret x as a gap position in the odd part of π. Indeed, if x is larger than exactly $i-1$ entries in the odd part, then let us mark the ith gap position in the odd cycles part. So now we are in a situation like in the previous case, that is, the gap position is in the odd part.

Run the odd part and this gap position through Ψ. Instead of inserting $2n+1$ to the marked position, however, insert temporarily a symbol B, to denote a number larger than all entries in the odd part. Then decrement all entries in the odd part that are larger than x (including B) by one notch. The obtained odd cycles and the unchanged even cycles (except for the mentioned change in c) give us $\kappa(\pi)$. Note that $2n+1$ will be in an even cycle when we're done.

We claim that the map κ defined above is a bijection from the set $SQ(2n) \times [2n+1]$ onto the set $SQ(2n+1)$. First, let us verify that κ maps into $SQ(2n+1)$. Indeed, (π) and $\kappa(\pi)$ have the same number of cycles of each even length, so by Exercise 21, $\pi \in SQ(2n)$ implies $\kappa(\pi) \in SQ(2n+1)$.

To get the reverse of κ, take a permutation $\pi' \in SQ(2n+1)$, and locate $2n+1$. If it is in an odd cycle, then run the odd cycles through Ψ^{-1}. This will yield an odd part one shorter, and an element of $[2n+1]$. Putting this together with the unchanged even part, we get $\kappa^{-1}(\pi')$.

If $2n+1$ is in an even cycle, then run the odd cycles part through Ψ^{-1}. This will specify a gap position in the odd part, and so we recover the entry x. Increment entries larger than x by one notch in the odd part. To get the even part, put x back to the place of $2n+1$. The gap position immediately preceding $2n+1$ is our k in $\kappa^{-1}(\pi')$.

(25) Note that when we proved Theorem 6.24, we proved a special case of this problem, that is, the one when $k = 2$. The very same method will prove this general statement.

Chapter 7

You Shall Not Overcount. The Sieve

7.1 Enumerating The Elements of Intersecting Sets

In a high school class there are 14 students who play soccer and there are 17 students who play basketball. How many students play at least one of these two sports?

The above question may sound extremely simple. However, we cannot answer it from the given information. Simply adding the two given numbers could yield an incorrect answer. Indeed, there may be students who play both sports. If we simply added the number of basketball players and the number of soccer players, we would count these students twice. To correct that, we would have to subtract their number once (so that they are counted only once), but we can only do that if we *know* their number.

Example 7.1. There are 14 students in a high school class who play soccer, and there are 17 students who play basketball. Four students play both games. How many students play at least one of the two games?

Solution. By the above argument, the number of students playing at least one of these two games is $14 + 17 - 4 = 27$.

Figure 7.1 illustrates the above situation.

The situation becomes more complicated, but still controllable, if the students are playing up to three different games. This is the content of our next example.

Example 7.2. In a high school class, there are 14 students who play soccer, 17 students who play basketball, and 18 students who play hockey. Four