We claim that the permutation $p \in S_n$ contains entries $n-1$ and n in the same cycle if and only if in $f(p)$ the entry n is on the *left* of the entry $n-1$. Here f is the map defined in the transition lemma. Indeed, if p does have the property that $n-1$ and n are in the same cycle, then in the canonical cycle notation that cycle starts with n, so $f(p)$ contains n on the left of $n-1$. On the other hand, if n and $n-1$ are in different cycles, then they are both the leftmost entries of their cycles in the canonical cycle notation, and therefore $n-1$ is on the right of n. So our claim is proved. However, it happens that n precedes $n-1$ in exactly half of all n-permutations. Therefore, we proved the following interesting result.

Proposition 4.33 *Let n be any positive integer, and let i and j be two distinct elements of $[n]$. Then exactly half of all n-permutations contain i and j in the same cycle.*

So A has a fifty percent chance of getting to the same table as B.

The transition lemma has other striking applications, leading to fundamental enumeration results on permutations. Therefore, the reader is strongly urged to examine Exercises 10, 11, and 18—and try to solve them—before looking at the solutions we provided.

Quick Check

1. What is the number of permutations of length n that consist of one 1-cycle and one $(n-1)$-cycle?
2. How many permutations of length n are there in which the entries 1 and 2 are in the same cycle, but the entry 3 is in a different cycle?
3. How many permutations of length n are there in which the entry 1 is in a 2-cycle, and the entry 2 is also in a 2-cycle?

4.3 Cycle structure and exponential generating functions

If we think about it for a minute, we see why the exponential formula, learned in the previous chapter, is very useful for counting permutations. Indeed, a permutation is nothing other than a set $[n]$ split into an arbitrary number of nonempty blocks, on each of which a cycle is taken.

We will be particularly interested in the permutation analog of Theorem 3.33 that follows.

Theorem 4.34 *Let C be any set of positive integers, and let $g_C(n)$ be the number of permutations of length n whose cycle lengths are all elements of C. Then*

$$G_C(x) = \sum_{n\geq 0} g_C(n)\frac{x^n}{n!} = \exp\left(\sum_{n\in C}\frac{x^n}{n}\right).$$

Proof: The proof is similar, but not identical, to the proof of Theorem 3.33. Let us partition $[n]$ into blocks. For a block of size m, set $a(m) = 0$ if $m \notin C$, and set $a(m) = (m-1)!$ otherwise. In other words, $a(m)$ is the number of ways we can take an allowed cycle on an m-element block. Then

$$A(x) = \sum_{n\geq 1} a(n)\frac{x^n}{n!} = \sum_{n\in C}\frac{x^n}{n}$$

is the exponential generating function of the number of possibilities of the first task, and the statement is proved by the exponential formula. $\Diamond$

Let us start with a very basic example. Before we start, we remind the reader that $\frac{1}{1-x} = \sum_{n\geq 0} x^n$, and, integrating both sides, we get the equality $\ln(1-x)^{-1} = \sum_{n=1}^{\infty}\frac{x^n}{n}$.

Example 4.35 *Let C be the set of all positive integers. Then*

$$\begin{aligned} G_C(x) &= \exp\left(\sum_{n=1}^{\infty}\frac{x^n}{n}\right) \\ &= \exp\left(\ln(1-x)^{-1}\right) \\ &= \frac{1}{1-x} \\ &= \sum_{n\geq 0} x^n. \end{aligned}$$

So the coefficient of x^n in $G_C(x)$ is 1, and therefore the coefficient of $x^n/n!$ in $G_C(x)$ is $n!$. This is not surprising at all since this says that, if all cycle lengths are allowed, then there are $n!$ permutations of length n.

The following example shows a typical application of Theorem 4.34. A permutation p is called an *involution* if p^2 is the identity permutation. It goes without saying that p is an involution if and only if all cycles in p are of length 1 or 2. Let us use our new technique to compute the number of involutions of length n.

Example 4.36 *The number of all involutions of length n is*

$$f(n) = \sum_{i=0}^{\lfloor n/2\rfloor}(2i-1)!!\binom{n}{2i},$$

where we set $(-1)!! = 1$.

Solution: We use Theorem 4.34, with $C = \{1, 2\}$. Then we have

$$\begin{aligned} G_C(x) &= \exp\left(x + \frac{x^2}{2}\right) \\ &= \left(\sum_{k\geq 0} \frac{x^k}{k!}\right) \cdot \left(\sum_{i\geq 0} \frac{x^{2i}}{i!2^i}\right). \end{aligned}$$

Note that the coefficient of x^n on the right-hand side is equal to $\sum_{i=0}^{\lfloor n/2 \rfloor} \frac{1}{(n-2i)!\cdot i!\cdot 2^i}$. The result now follows if we observe that $i!2^i = \frac{(2i)!}{(2i-1)!!}$. $\Diamond$

With our fresh knowledge, we re-prove the formula for the number of derangements that we proved in Section 2.4.3.4. Recall that derangements are permutations without 1-cycles (or *fixed points*). This time, we will not need to resort to the somewhat cumbersome computation using the principle of inclusion-exclusion.

Indeed, set $C = \{\mathbf{P} - 1\}$. Then Theorem 4.34 yields

$$\begin{aligned} G_C(x) &= \exp\left(\sum_{n\geq 2} \frac{x^n}{n}\right) \\ &= \exp(\log(1-x)^{-1} - x) \\ &= \frac{e^{-x}}{1-x}. \end{aligned}$$

In other words, we get that

$$G_C(x) = \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!}\right) \cdot x^n,$$

so the coefficient of $x^n/n!$ in $G_C(x)$ is

$$n! \cdot \left(\sum_{i=0}^{n} \frac{(-1)^i}{i!}\right), \tag{4.11}$$

just as we have proved in Section 2.4.3.4. Note that, as n goes to infinity, the sum $\sum_{i=0}^{n} \frac{(-1)^i}{i!}$ converges to e^{-1}. That is, for large n, more than one-third of all n-permutations are fixed point free, that is, derangements.

Comparing (4.11) with the result of Lemma 4.12, we find the surprising fact that, for any $n \geq 1$, the number of derangements of length n is equal to the number of desarrangements of length n. This is very interesting as derangements are defined using cycles of permutations, whereas desarrangements are defined using the one-line notation. Recall that a permutation p is called a desarrangement if the first ascent of p occurs in an even position, or if p is the decreasing n-permutation and n is even.

Such a nice identity certainly asks for a bijective proof. Such a proof is reasonably easy to find once we find the right modification of canonical cycle notation.

Let p be any derangement of length n. Let us write p in cycle notation so that each cycle contains its smallest entry in its *second* position, and so that the cycles are ordered in decreasing order of their smallest entries. Define $f(p)$ as the permutation in one-line notation that is obtained from p by omitting all parentheses.

Example 4.37 *If* $p = (324)(51)$*, then* $f(p) = 32451$*. If* $p = (43)(215)$*, then* $f(p) = 43215$*.*

Theorem 4.38 *The "parenthesis omitting map"* f *defined above is a bijection from the set* D_n *of all derangements of length* n *onto the set* J_n *of all desarrangements of length* n*.*

Proof: First we show that f indeed maps into J_n, that is, that $f(p)$ is always a desarrangement. The first cycle C of p contains its smallest entry x in its second position, so, if C contains a third entry y, then $y > x$, and $f(p)$ has its first ascent in the second position, and therefore $f(p)$ is a desarrangement. If C only contains two entries, and the first entry of the second cycle C' is larger than x, then we are done, otherwise repeat the argument applied to C for C'. Continuing this way, we will stop and find the first ascent of $f(p)$ in an even position as soon as we find a cycle with more than two entries or a cycle whose first entry is larger than the last (second) entry of the previous cycle. The only case in which neither of these scenarios occurs is when all cycles are of length two, and the entries in them get smaller and smaller. In that case, we must have $n = 2k$ and $p = (2k\ 2k-1)(2k-2\ 2k-3)\cdots(21)$, and so $f(p)$ is the decreasing permutation of length $2n$, which is a desarrangement.

Now we show that $f : D_n \to J_n$ is a bijection by proving that it has an inverse. Let $q \in J_n$, and set $q = q_1 q_2 \cdots q_n$ in the one-line notation. We are going to find the unique $p \in D_n$ satisfying $f(p) = q$. It follows from the definition of f that, if $q_i = 1$, then the last cycle of p must be $(q_{i-1}\ q_i \cdots q_n)$, as 1 is always the smallest entry of the last cycle. Since q is a desarrangement, it could not happen that $i = 3$ (as that would mean that the first ascent of q is either in the first or in the third position), so the string $q' = q_1 q_2 \cdots q_{i-2}$, when not empty, is at least of length 2. Therefore, we can repeat the same argument for q', that is, we can find its last cycle by starting it at the entry preceding the smallest entry. Iterating this procedure until all of q was broken into cycles, we get the (unique) preimage of q. Uniqueness follows from the fact that f does not change the left-to-right order of the entries, and the cycles cannot start anywhere else without violating our cleverly chosen conditions.

Therefore, f is a bijection as claimed. $\Diamond$

The above example of derangements, while a classic one, was about a special case when the set C of allowed cycle lengths was just one element short of all positive integers. In order to increase the reader's appreciation of the exponential formula as a tool of permutation enumeration, we present an example that concerns an *infinite* set C.

Example 4.39 *The number of n-permutations in which each cycle length is even is zero if n is odd and is*

$$\mathbf{even}(2m) = 1^2 \cdot 3^2 \cdots (2m-1)^2 = (1 \cdot 3 \cdots (2m-1))^2 = (2m-1)!!^2$$

if $n = 2m$.

Solution: We will apply Theorem 4.34, with C being the set of all even positive integers. Then Theorem 4.34 implies

$$G_C(x) = \exp\left(\sum_{m=1}^{\infty} \frac{x^{2m}}{2m}\right).$$

Now note that the right-hand side looks very similar to the formal power series $\exp(\ln(1-x)^{-1})$, only x is replaced by x^2 and then the argument of exp is divided by 2. Therefore, we have

$$G_C(x) = \exp\left(\frac{1}{2}\ln(1-x^2)^{-1}\right) = \sqrt{\frac{1}{1-x^2}}.$$

Therefore, we will get the numbers $\mathbf{even}(2m)$ as the coefficients of $\frac{x^{2m}}{(2m)!}$ in $\sqrt{\frac{1}{1-x^2}}$. We see without any computation that $\mathbf{even}(2m+1) = 0$, since the sum of even integers cannot be odd. To compute $\mathbf{even}(2m)$, we will use the binomial theorem.

$$\begin{aligned} G_C(x) = \sqrt{\frac{1}{1-x^2}} &= (1-x^2)^{-1/2} \\ &= \sum_{m=1}^{\infty} \binom{-1/2}{m} (-1)^m x^{2m} \\ &= \sum_{m=1}^{\infty} (-1)^m \frac{(-1/2)\cdot(-3/2)\cdots(-(2m-1)/2)}{m!} x^{2m} \\ &= \frac{(2m-1)!!}{m!2^m} x^{2m}. \end{aligned}$$

So the coefficient of x^{2m} in $G_C(x)$ is $\frac{(2m-1)!!}{m!2^m}$; therefore, the coefficient of $x^{2m}/(2m)!$ is $(2m)!$ times that. In other words, it is indeed $(2m-1)!!^2$ as claimed. $\Diamond$