Not that we need this extra piece of evidence, but note that the coefficient of $x^{2m+1}/(2m+1)!$ in $G_C(x)$ is indeed 0 since $G_C(x)$ is a power series in x^2. This shows again that $\mathbf{even}(2m+1) = 0$ for all m.

The nice formula we have just proved for $\mathbf{even}(2m)$ certainly calls for a combinatorial proof, and we are going to present one. Let p be a permutation counted by $\mathbf{even}(2m)$, and think about p as a bijection from $[2m]$ onto $[2m]$. Then $p(1)$ can be anything but 1 since that would create a 1-cycle, which is not allowed because of its odd length. So we have $2m-1$ possibilities for $p(1)$. Once $p(1)$ is chosen, $p(p(1))$ can again be anything except for $p(1)$, so we have $2m-1$ choices for $p(p(1))$ as well. If 1 and $p(1)$ form a 2-cycle, then we are done by induction on m, otherwise we continue. In that case, $p(p(p(1)))$ can be anything but 1, $p(1)$, and $p(p(1)))$, so we have $2m-3$ choices for $p(p(p(1)))$. By similar argument, we have $2m-3$ choices for $p^4(1)$ since $p^i(1)$ is not allowed for $i = 1, 2, 3$. Then if $p^4(1) = 1$, we are done by induction, otherwise we continue the same way. In each step, we see that we have $2m-2i+1$ possibilities for each of $p^{2i-1}(1)$ and $p^{2i}(1)$ (since 1 is a possibility for the latter). Therefore, our claim is proved.

Quick Check

1. Let C be the set of all positive integers divisible by 3. Find the closed form of $G_C(x)$.
2. Let $h(n)$ be the number of permutations of length n that contain exactly one 1-cycle. Find the exponential generating function of the numbers $h(n)$.
3. Let $h(n)$ be the number of permutations of length n that contain exactly one cycle that is longer than 1. Find the exponential generating function of the numbers $h(n)$.

4.4 Inversions

In Section 4.1, we studied descents of permutations. To that end, we wrote permutations in one-line notation, then studied pairs of *consecutive entries* that were in the *wrong* order, that is, the larger one preceded the smaller one. Now we will do the same, relaxing the requirement that the entries in the wrong order be consecutive.

Definition 4.40 *Let $p = p_1 p_2 \cdots p_n$ be a permutation. Then we say that the pair (p_i, p_j) is an* inversion *of p if $i < j$, but $p_i > p_j$. The number of inversions of p will be denoted by $i(p)$.*

If a pair (p_i, p_j) is not an inversion, then it is called, less than shockingly, a *non-inversion*.

Example 4.41 *The permutation 31524 has four inversions. These are* $(3,1)$, $(3,2)$, $(5,2)$, *and* $(5,4)$.

The number of n-permutations with k inversions will be denoted by $b(n,k)$. Note that if we read p backwards, then every inversion becomes a non-inversion, and vice versa. So there are as many n-permutations with k inversions as there are with $\binom{n}{2} - k$ inversions.

The number of inversions of the permutation p keeps being interesting even when we look at permutations as products of cycles. In order to prove a simple result in that direction, we define the *full diagram* of a function $f : [n] \rightarrow [n]$. This diagram consists of $2n$ points, n for the domain of f, and n for the range of f, and both of these n-element subsets are arranged vertically, facing each other. If $f(i) = j$, then an arrow goes from point i of the first set to point j of the second set.

Example 4.42 *Figure 4.3 shows the full diagram of the permutation* 24153.

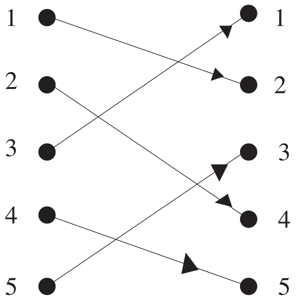

Figure 4.3
The full diagram of 24153.

The following proposition connects the notion of inversions, which was defined using the one-line notations, to the concept of inverse permutations, which was defined considering permutations as functions.

Proposition 4.43 *For every permutation p, we have $i(p) = i(p^{-1})$.*

Proof: If we draw the full diagram of the function $p : [n] \rightarrow [n]$, then $i(p)$ is precisely the number of crossings in this diagram. (The reader should think about this.) However, the full diagram of p^{-1} is the same as that of p, with the arrows reversed. Therefore, the number of crossings in the full diagram of p^{-1} is the same as that in the full diagram of p, proving our statement. $\Diamond$

The following notion turns out to be useful in many parts of mathematics outside combinatorics.

Definition 4.44 *A permutation p is called* even *if $i(p)$ is even. Similarly, p is called* odd *if $i(p)$ is odd.*

One feels that "even" and "odd" should be properties that occur equally often. The following proposition shows that this is indeed the case.

Proposition 4.45 *Let $n \geq 2$. Then the number of even (equivalently, odd) n-permutations is $n!/2$.*

Proof: Let p be any n-permutation, and let p' be the permutation obtained from p by swapping its first two entries. Then the difference between $i(p)$ and $i(p')$ is plus or minus 1, so they are of different parity. Repeating this argument for all n-permutations, we see that S_n can be split into two subsets of equal size, one consisting of even permutations, the other one consisting of odd permutations. ♢

It turns out that, if we know the parity of the permutations p and q, then we can figure out that of pq and qp. One way to do this is through the following very useful representation of permutations by matrices.

Definition 4.46 *Let $p \in S_n$, with $p = p_1 p_2 \cdots p_n$. The* permutation matrix *of p is the $n \times n$ matrix A_p defined by*

$$A_p(i,j) = \begin{cases} 1 & \textit{if } p_i = j, \\ 0 & \textit{otherwise.} \end{cases}$$

In other words, each row and column of A_p contains exactly one 1 and $n-1$ zeros. To figure out which entry of row i is equal to 1, just find the value of the ith *position* in p. To figure out which entry of column j is equal to 1, find the *entry* that is in position j of p, that is, p_j.

Example 4.47 *If $p = 3241 = (2)(431)$, then*

$$A_p = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The crucial property of representing permutations by the matrices A_p is that it is a *homomorphism*, that is, that these matrices can be multiplied together as the corresponding permutations.

Lemma 4.48 *Let $p = p_1 p_2 \cdots p_n$ and $q = q_1 q_2 \cdots q_n$ be n-permutations. Then*

$$A_p A_q = A_{pq}.$$

Proof: We know from the definition of permutation matrices that A_p, A_q, and A_{pq} are all 0-1 matrices. It is easy to see that so is A_pA_q, since the entries of that matrix can be obtained as dot products of a row of A_p and a column of A_q and are therefore equal to either 0 or 1. It is therefore sufficient to prove that $x = A_{pq}(i,j) = 1$ if and only if $y = (A_pA_q)(i,j) = 1$.

It is a direct consequence of the definition of matrix multiplication that $y = A_pA_q(i,j) = \sum_{k=1}^{n} A_p(i,k)A_q(k,j)$. That is, $y = 1$ if and only if there is a $k \in [n]$ so that both $A_p(i,k) = 1$ and $A_q(k,j) = 1$ hold. Considering p and q as functions, this is equivalent to $p(i) = k$ and $q(k) = j$, meaning that $q(p(i)) = (pq)(i) = j$, which by definition is equivalent to $x = A_{pq}(i,j) = 1$. $\diamondsuit$

Many important pieces of information about p can easily be read off A_p.

Proposition 4.49 *The permutation* p *is odd if and only if* $\det A_p = -1$*. Similarly, the permutation* p *is even if and only if* $\det A_p = 1$*. In other words,* $\det A_p = (-1)^{i(p)}$*.*

Proof: We prove the statement by induction on n. For $n = 1$ and $n = 2$, the statement is true. Assume the statement is true for $n-1$ and let $p = p_1p_2\cdots p_n$. Let $p_j = 1$. Then it follows from the expansion theorem of determinants that

$$\det A_p = (-1)^{j-1} \det A_{p'},$$

where p' is the $(n-1)$-permutation obtained from p by deleting the entry 1 and relabeling.

Indeed, let us expand A_p with respect to its first column, and we get the above identity. Finally, note that $i(p) = i(p') + (j-1)$, and then our statement follows from the induction hypothesis applied to p'. $\diamondsuit$

Corollary 4.50 *Figure 4.4 shows what happens if we multiply together permutations of various parities.*

	EVEN	ODD
EVEN	EVEN	ODD
ODD	ODD	EVEN

Figure 4.4
The parity of the product of two permutations.

In particular, the product of even permutations is always even, so the set of even permutations is closed under multiplication. Similarly, the inverse of an even permutation is always even. Therefore, the set of all even n-permutations is interesting on its own, and it is called the *alternating group of degree n*, denoted by A_n.

We point out that the parity of a permutation is often called the *sign* of the permutation. The reason for this is that, as we have just seen, permutations of various parities multiply together like real numbers of various signs.

A permutation that simply interchanges two elements of $[n]$ and leaves all other elements fixed is called a *transposition.* It turns out that transpositions are all odd permutations.

Proposition 4.51 *If p is a transposition, then $i(p)$ is odd.*

Proof: First assume that $p = (i\ i+1)$, that is, p interchanges two *consecutive* elements of $[n]$. Then p has one inversion, and the statement is true. Now assume that $p = (i, i+k)$, that is, there are $k-1$ elements between the two entries that p moves. We claim that $i(p) = 2k-1$. Indeed, each of the $k-1$ elements located between i and $i+k$ is a part of two inversions, one with i, one with $i+k$. Since $(i, i+k)$ forms the last inversion, $i(p)$ is odd. ♢

The following lemma may sound a little bit counterintuitive.

Lemma 4.52 *The permutation $a = (a_1\ a_2 \cdots a_n)$ that consists of an n-cycle is an even permutation if and only if n is odd.*

Proof: For the purposes of this proof, we will *omit* all 1-cycles from the cycle notation of a permutation. For instance, the 6-permutation (1)(32)(54)(6) would be written as (32)(54). This does not cause any ambiguity, since entries that are not shown in the cycle notation must be fixed points.

We prove the statement by induction on n. The initial cases of $n = 1$ and $n = 2$ are true because the permutation (x) has an even number of inversions (zero), while the permutation $(y\ z)$ has an odd number of inversions, as we have seen in Proposition 4.51.

Now let us assume the statement is true for all positive integers less than n, and let $a = (a_1\ a_2 \cdots a_n)$. The crucial observation is that

$$a = (a_{n-1}\ a_n)(a_1\ a_2 \cdots\ a_{n-1}).$$

Setting $q = (a_{n-1}\ a_n)$ and $a' = (a_1\ a_2 \cdots\ a_{n-1})$, the identity $p = qp'$ holds. Taking determinants, and using Proposition 4.49, we see that

$$\det A_a = \det A_q \cdot \det A_{a'} = -\det A_{a'},$$

since $\det A_q = -1$ by Proposition 4.51. So the parity of a is the opposite of that of a', and our induction step, and therefore our proof, is complete. ♢