CHAPTER 11

Statistics on Permutations and Words

11.0. Introduction

This chapter is devoted, as the previous one, to combinatorial properties of permutations, considered as words. The starting point in this subject is the bivalent status of permutations, which can be considered as products of cycles as well as a sequence of the first n integers written is disorder.

The fundamental results concerning this area are presented in Chapter 10 of Lothaire 1983. They consist essentially in two transformations on words. The first one (First Fundamental Transformation) is an encoding of the cycle decomposition of a permutation. The second one (Second Fundamental Transformation) accounts for a statistical property of permutations, namely the equidistribution of the number of inversions and the inverse major index on permutations with a given shape.

In the previous chapter (Chapter 10) some other properties are presented, including basic facts on q-calculus and additional statistics on permutations.

In this chapter, we carry on with complements focused on two main aspects. The first one is a shortcut avoiding the Second Fundamental Transformation by a simple evaluation of determinants. The second one is the analogy between the First Fundamental Transformation and the Lyndon factorization (the Gessel Normalisation).

The organization of the chapter is the following: After some preliminaries, Sections 11.2 provides a determinantal expression for the commutative image of some sets of words. This expression is used in Sections 11.3 and 11.4, for evaluating respectively the inverse major index and the number of inversions of permutations with a given shape. In Section 11.5 the Gessel Normalisation is introduced. In Section 11.6, it is then applied to evaluating the major index of permutations with a given cycle structure.

11.1. Preliminaries

Let us recall some notations and preliminary results.

In the sequel, $[n]$ will denote the set of integers $\{1, \ldots, n\}$. We shall also use alphabets whose letters are the nonnegative integers. By N_k we mean the alphabet $\{0, 1, \ldots k\}$ equipped with the natural ordering. By letting k tend to infinity, we obtain the infinite alphabet $\mathbb{N}$. Quite obviously, if $k < r$, then $N_k \subset N_r$. In that way, a word on N_k is a finite sequence of nonnegative integers which do not exceed k.

To each N_k one can associate the set X_k of commuting indeterminates $\{x_0, x_1 \ldots x_k\}$. Given a word $w = w_1 w_2 \ldots w_n$ on N_k, its *commutative image* is the commutative monomial $\mathrm{GS}(w) = x_{w_1} x_{w_2} \ldots x_{w_n}$. This definition can be extended to a set of words. If A is such a set, its *generating series* $\mathrm{GS}(A)$ is the sum of the commutative images of its elements. When A is infinite, so is its generating series. This does not yield any problem of convergence. When the number of letters (finite or infinite) is irrelevant, we shall simply write N for the alphabet and X for the associated indeterminates.

A particular—and fundamental—example is the following. Let a and k be integers. By $W_a(N_k)$ we denote the set of all nonincreasing words of length a over the alphabet N_k. Its commutative image, denoted by $S_a(X_k)$ is known as the complete symmetric function.

A favorite operation for deriving generating functions is the substitution of powers of a new indeterminate q in the generating series.

First, recall the definition of the *q-factorial* (*cf.* Chapter 10):

$$(q)_n = (1-q)(1-q^2)\cdots(1-q^n),$$

and define the *Gaussian polynomial* (or q-binomial) by

$$\begin{bmatrix} n \\ k \end{bmatrix} = (q)_n/(q)_k(q)_{n-k}.$$

Substituting x_i by q^i in generating series will provide generating functions for various statistics on words or permutations. In that respect, we shall need two preliminary results. The first one is a reformulation of Proposition 10.1.1.

PROPOSITION 11.1.1. *Let $S_a(\{1, q, q^2, \ldots, q^k\})$ be the result of the substitution of x_i by q^i in $S_a(X_k)$, $0 \le i \le k$. Then*

$$S_a(\{1, q, q^2, \ldots, q^k\}) = \begin{bmatrix} a+k \\ k \end{bmatrix}.$$

The next one is the limit of the former when k tends to infinity.

PROPOSITION 11.1.2. *Let $S_a(\{1, q, q^2, \ldots\})$ be the result of the substitution of x_i by q^i in $S_a(X_{\mathbb{N}})$, $i \ge 0$. Then*

$$S_a(\{1, q, q^2, \ldots\}) = 1/(q)_a.$$

The series $S_a(\{1, q, q^2, \ldots\})$ has a classical combinatorial interpretation. It is the generating function of the number of partitions of integers in parts less than a. A *partition* of an integer n is a nonincreasing sequence of positive integers (the *parts*) whose sum is n. Removing any restriction on the size of the parts yields the celebrated Euler generating function $1/(q)_\infty$ for the number of partitions partitions.

Without the nonincreasing condition, the corresponding combinatorial object is called a *composition* of the integer n. So it is a sequence of integers whose sum is n.

We shall enumerate various statistics on permutations. Let us recall that a *permutation* of $[k]$ can be thought of either as a bijection from $[k]$ onto itself or as a word of length k with distinct letters in $[n]$. If $\sigma = \sigma(1)\sigma(2)\ldots\sigma(k)$ is such a permutation, an *inversion* of σ is a pair (i, j) such that $1 \le i < j \le k$ and $\sigma(i) > \sigma(j)$. The number of inversions of σ will be denoted by $\operatorname{inv}\sigma$.

A *descent* of σ is an index i, $1 \le i < k$ such that $\sigma(i) > \sigma(i+1)$. The set of the descents of σ, its *descent set* is denoted by $\operatorname{DES}\sigma$. The sum of the elements of this set is the so called *major index*, $\operatorname{maj}\sigma$.

We say that i, $0 \le i < k$ is a *backstep* of σ when the letter $i+1$ appears on the left of i in the word σ. This condition is equivalent to saying that i is a descent of the inverse of σ. The set of the descents of σ is designated by $\operatorname{BS}\sigma$. As for descents, we can sum all the backsteps of σ to obtain $\operatorname{imaj}\sigma$, the *inverse major index* of σ.

11.2. Words with a given shape

Each word $w = w_1 w_2 \cdots w_n$ can be uniquely factored as a product of maximal nonincreasing words: $w = u_1 u_2 \cdots u_k$, where each u_j is nonincreasing, its last letter being strictly smaller than the first letter of u_{j+1}. The respective lengths a_1, a_2, ...of u_1, u_2, ...constitute a composition $\mathbf{a}$ of n. This composition is called the *shape* of w.

EXAMPLE 11.2.1. Let $w = 1\,0\,2\,2\,0\,4\,7\,5\,1$. Its shape is $\mathbf{a} = (2, 3, 1, 3)$.

Let $(b_1 \le b_2 \le \cdots \le b_k)$ a nondecreasing sequence of integers, $\mathbf{N} = (N_{b_1} \subseteq N_{b_2} \subseteq \cdots \subseteq N_{b_k})$ the sequence of corresponding alphabets and $\mathbf{a}$ a composition of n. Let us consider the set $W(\mathbf{a}, \mathbf{N})$ consisting of the words $w = u_1 u_2 \cdots u_k$ of shape $\mathbf{a}$ such that the factor u_i contains only letters in N_{b_i}.

Let us denote by $S(\mathbf{a}, \mathbf{X})$ the generating series of $W(\mathbf{a}, \mathbf{N})$. If all alphabets are equal to the same alphabet X, finite or infinite, we shall simplify the notation in $S(\mathbf{a}, X)$. If furthermore $\mathbf{a}$ is reduced to a single integer a, we have $S(\mathbf{a}, X) = S_a(X)$.

PROPOSITION 11.2.2. *Let* $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ *a shape,* $b_1 \le b_2 \le \cdots \le b_k$ *and* $\mathbf{X} = (X_{b_1}, X_{b_2}, \ldots, X_{b_k})$. *Then* $S(\mathbf{a}, \mathbf{X}) = \det(M)$, *where* M *is the matrix*

$M = (M_{i,j})_{\{1\leq i,j\leq k\}}$ *with*

$$M_{i,j} = \begin{cases} S_{a_i+a_{i+1}+\cdots+a_j}(X_{b_i}) & \textit{if } i \leq j, \\ 1 & \textit{if } i = j+1, \\ 0 & \textit{if } i > j+1. \end{cases} \tag{11.2.1}$$

Proof. Fully written, the matrix M is:

$$M = \begin{pmatrix} S_{a_1}(X_{b_1}) & S_{a_1+a_2}(X_{b_1}) & \cdots & S_{a_1+\cdots+a_{k-1}}(X_{b_1}) & S_{a_1+\cdots+a_k}(X_{b_1}) \\ 1 & S_{a_2}(X_{b_2}) & \cdots & S_{a_2+\cdots+a_{k-1}}(X_{b_2}) & S_{a_2+\cdots+a_k}(X_{b_2}) \\ 0 & 1 & \cdots & S_{a_3+\cdots+a_{k-1}}(X_{b_3}) & S_{a_3+\cdots+a_k}(X_{b_3}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & S_{a_k}(X_{b_k}) \end{pmatrix}.$$

The proof is by induction on the length k of the shape $\mathbf{a}$ of w.

If $k = 1$, Equation 11.2.1 is trivially the definition of $S_a(X)$. For a general k, let us expand the determinant along its last row:

$$S(\mathbf{a}, \mathbf{X}) = S_{a_k}(X_{b_k}) \det(M_1) - \det(M_2), \tag{11.2.2}$$

where M_1 consists of the first $k-1$ rows and columns of M and M_2 is identical to M_1, except for its last column, which consists of the first $k-1$ rows of the last column of M, and so is:

$$S_{a_i+a_{i+1}+\cdots+a_k}(X_{b_i}) \qquad \text{for } 1 \leq i \leq k.$$

By the recurrence hypothesis,

$$\det(M_1) = S(\mathbf{a}_1, \mathbf{X}_1) = S((a_1, a_2, \ldots, a_{k-1}), (X_{b_1}, X_{b_2}, \ldots, X_{b_{k-1}})),$$

and

$$\det(M_2) = S(\mathbf{a}_2, \mathbf{X}_1) = S((a_1, a_2, \ldots, a_{k-2}, a_{k-1} + a_k), (X_{b_1}, X_{b_2}, \ldots, X_{b_{k-1}})).$$

To the term $S_{a_k}(X_{b_k}) \det(M_1)$ of Equation 11.2.2 contribute exactly pairs of words made of a word w' in $W(\mathbf{a}_1, \mathbf{X}_1)$ and a nonincreasing word w'' of length a_k over the alphabet X_{b_k}. Let $w = w'w''$. Then either w is an element of $W(\mathbf{a}, \mathbf{X})$ if the last letter of w' is strictly smaller than the first letter of w'', or it is an element of $W(\mathbf{a}_2, \mathbf{X}_1)$ otherwise.

In the first case it contributes to $S(\mathbf{a}, \mathbf{X})$. In the latter case, it contributes to $S(\mathbf{a}_2, \mathbf{X}_1) = \det(M_2)$. This combinatorial interpretation yields precisely Equation 11.2.2. ∎

11.3. Backsteps of permutations with a given shape

Let $\sigma = \sigma(1)\sigma(2)\ldots\sigma(n)$ a permutation of $[n]$. Let a_1 be the first index such that $\sigma(a_1) > \sigma(a_1 + 1)$. Let $a_1 + a_2$ the second such index and, more generally, let $a_1 + a_2 + \cdots a_i$ the i-th such index. (We suppose, by convention, that $\sigma(n+1) = 0$.) The sequence $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ is a composition of n called the *shape* of σ. If the permutation is considered as a word with distinct letters, its shape as a word coincides with its shape as a permutation, provided that the order is reversed. This apparent complication actually keep the results of the next sections reasonably simple to state.

EXAMPLE 11.3.1. Let $\sigma = 6\,8\,4\,5\,9\,3\,1\,2\,7$. Its shape is $\mathbf{a} = (2,3,1,3)$.

Let $w = w_1 w_2 \cdots w_n$ be a word of shape $\mathbf{a}$. On $[n]$ define the total order $\preceq$ by $i \prec j$ iff $w_i > w_j$ or $w_i = w_j$ and $i < j$. Let $\sigma(i)$ be the rank of index i according to this total order. This implies that $i \prec j \Leftrightarrow \sigma(i) < \sigma(j)$. Then σ is a permutation called the *standard normalization* of w.

Let $\varphi(w)$ be the pair (σ, s) consisting of the standard normalization σ of w and of the nonincreasing reordering s of the letters of w. In the next theorem, as well as in Theorem 11.6.1, we shall say that the nonincreasing sequence $s = s_1 s_2 \ldots$ is *compatible* with a set E of positive integers $s_i > s_{i+1}$ whenever i is an element of E.

THEOREM 11.3.2. *Let* $\mathbf{a}$ *be a shape. Then* φ *is a bijection between the set of words* w *of shape* $\mathbf{a}$ *and the set of pairs* (σ, s)*, where* σ *is a permutation of shape* $\mathbf{a}$ *and* s *a nonincreasing sequence compatible with* $\mathrm{BS}\,\sigma$.

Proof. It is clear that the shape of σ and the shape of w are identical.

Suppose $i = \sigma(u)$ and $i + 1 = \sigma(v)$. Then $\sigma(u) < \sigma(v)$ hence $u \prec v$. Then, from the very definition of $\preceq$, we have $w_u \geq w_v$, which can also be written $w_{\sigma^{-1}(i)} \geq w_{\sigma^{-1}(i)}$. Since the application which, to i, associates $w_{\sigma^{-1}(i)}$ is nonincreasing, it is the nonincreasing rearrangement of w. This means that $s_i = w_{\sigma^{-1}(i)}$.

Suppose moreover that i is a backstep of σ, that is $u > v$. We already know that $u \prec v$. Those last two conditions are compatible only if $w_u > w_v$, which is the same as $w_{\sigma^{-1}(i)} > w_{\sigma^{-1}(i)}$ or $s_i > s_{i+1}$.

Conversely, suppose we are given a pair (σ, s) where s is compatible with $\mathrm{BS}\,\sigma$. Let w the word of length n given by $w_u = s_{\sigma(u)}$. Consider the order $\prec$ defined by $u \prec v$ iff $\sigma(u) < \sigma(v)$. We shall prove that this order is precisely the same as the order $\prec$ which has been defined earlier on w. This will prove that $\varphi(w) = (\sigma, s)$. To do so, suppose $\sigma(u) < \sigma(v)$. Since s is nonincreasing, we have $s_{\sigma(u)} \geq s_{\sigma(v)}$ and so $w_u \geq w_v$. Either $w_u > w_v$, which proves the point, or $w_u = w_v$.

In this latter case we have $s_{\sigma(u)} = s_{\sigma(v)}$. This implies (because s is compatible with $\mathrm{BS}\,\sigma$) that none of $\sigma(u)$, $\sigma(u)+1$, $\ldots$, $\sigma(v)-1$ is a backstep. Hence

$$u = \sigma^{-1}(\sigma(u)) < \sigma^{-1}(\sigma(u)+1) < \cdots < \sigma^{-1}(\sigma(v)-1) < \sigma^{-1}(\sigma(v) = v.$$

We have then proved that $u \prec v$ and $w_u = w_v$ imply $u < v$, which completes the proof of the theorem. ■

EXAMPLE 11.3.3. Let $w = 1\,0\,2\,2\,0\,4\,7\,5\,1$. Then $\varphi(w) = (\sigma, s)$ where

$$\sigma = 6\,8\,4\,\mathbf{5}\,9\,\mathbf{3}\,1\,\mathbf{2}\,\mathbf{7},$$
$$s = 7\,\mathbf{5}\,\mathbf{4}\,2\,\mathbf{2}\,1\,\mathbf{1}\,0\,0.$$

The backsteps of σ and the corresponding elements of s appear in boldface. It can be noted that, although $s_1 > s_2$, the integer 1 is not a backstep of σ. The shape of both w and σ is $(2,3,1,3)$.

COROLLARY 11.3.4. *Let $\mathbf{a}$ be a composition of n and A be a subset of $[n-1]$. Denote by $D_A(\mathbf{a})$ the number of permutations of n of shape $\mathbf{a}$ whose backsteps are precisely the elements of A. Then*

$$S(\mathbf{a}, X_{\mathbb{N}}) = \sum_{A \subset [n-1]} D_A(\mathbf{a}) \sum_{s} \mathrm{GS}(s), \tag{11.3.1}$$

where the second sum is over the set of all nonincreasing sequences s compatible with A.

Proof. A word of shape $\mathbf{a}$ corresponds to a commutative monomial of $S(\mathbf{a}, \mathbf{X}_{\mathbb{N}})$. Applying the bijection φ of Proposition 11.3.2 and summing over subsets of $[n-1]$ yields the proposition. ∎

It can be noted that the second sum in Corollary 11.3.4 is independent of the shape $\mathbf{a}$. As those sums are linearly independent, the numbers $D_A(\mathbf{a})$ are uniquely determined by $S(\mathbf{a}, X_{\mathbb{N}})$. See Problem 11.6.2 for a use of this property.

As a corollary, we shall now derive the enumeration of permutations with shape $\mathbf{a}$ by imaj, by substituting successive powers q^i to the letters i.

COROLLARY 11.3.5. *Let $\mathbf{a}$ be a composition of n. Then*

$$\sum_{\sigma} q^{\mathrm{imaj}\,\sigma} = (q)_n S(\mathbf{a}, \{1, q, q^2, \ldots\}), \tag{11.3.2}$$

where the sum is over the set of permutations of $[n]$ of shape $\mathbf{a}$.

Proof. Let A be a subset of $[n-1]$ and s be a nonincreasing sequence compatible with A. From s define a sequence d of nonnegative integers by

$$d_k = \begin{cases} s_k - s_{k+1} & \text{if } k \notin A \text{ and } 0 \le k < n, \\ s_k - s_{k+1} - 1 & \text{if } k \in A, \\ s_n & \text{if } k = n. \end{cases} \tag{11.3.3}$$

The set of sequences d of length n consisting of nonnegative integers is in that way in bijection with the set of nonincreasing sequences s of integers compatible with A. This bijection depends on A.

Let ΣA denote the sum of the elements of A. Substituting q^i to i transforms $\mathrm{GS}(s)$ into q to the power $\sum_{1 \le k \le n} s_k$. Now, from Equation 11.3.3, one obtains

$$\sum_{1 \le k \le n} s_k = \sum_{1 \le k \le n} k d_k + \Sigma A\,.$$

Therefore,

$$\sum_s q^{s_1+s_2+\cdots+s_n} = q^{\Sigma A} \sum_d q^{d_1+2d_2+\cdots+nd_n}.$$

The latter sum is the generating series for partitions into positive parts not greater than n, which is equal to $1/(q)_n$. This, combined with Corollary 11.3.4 yields the conclusion. ■

Example 11.3.6. In Example 11.3.3, we had

$$\sigma = 6\,8\,4\,\mathbf{5}\,9\,\mathbf{3}\,1\,\mathbf{2}\,\mathbf{7},$$
$$s = 7\,\mathbf{5}\,\mathbf{4}\,2\,\mathbf{2}\,1\,\mathbf{1}\,0\,0,$$

and $\mathrm{BS}\,\sigma = \{2,3,5,7\}$. The sequence d defined by Equation 11.3.3 is then

$$d = 2\,0\,1\,0\,0\,0\,0\,0\,0,$$

corresponding to partition $1^2 3$.

Proposition 11.3.7. *Let* $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ *be a composition of* n. *Then* $\sum_\sigma q^{\mathrm{imaj}\,\sigma} = (q)_n \det(N)$. *The sum is over the set of permutations of* $[n]$ *of shape* $\mathbf{a}$ *and* $N = (N_{i,j})_{\{1\le i,j\le k\}}$ *with*

$$N_i, j = \begin{cases} 1/(q)_{(a_i+a_2+\cdots+a_j)} & \text{if } i \le j, \\ 1 & \text{if } i = j+1, \\ 0 & \text{if } i > j+1. \end{cases} \tag{11.3.4}$$

Proof. Apply Proposition 11.2.2 in the case when all alphabets X_{b_i} are equal to $X_{\mathbb{N}}$, then substitute q^i to i. From Proposition 11.1.2, one obtains precisely Formula 11.3.4. ■

Using Proposition 11.3.7 one can obtain explicit expressions for the enumeration of permutations of special shapes by imaj. This has been done for alternating permutations and permutations with a given number of descents, thus leading to q-analogues of tangent and secant numbers as well as q-analogues of Eulerian polynomials. See Problems 11.3.2 and 11.3.3 for more specific details.

11.4. Inversions of permutations with a given shape

The inversions of a permutation can be conveniently taken care of by a simple encoding with particular words.

Let σ be a permutation of $[n]$. For $1 \le i \le n$, let ℓ_i be the number of indices $j < i$ such that $\sigma(j) > \sigma(i)$. The word $\ell = \ell_1\ell_2\cdots\ell_n$ will be called *Lehmer encoding* of σ.

Example 11.4.1. To permutation

$$\sigma = 6\,8\,4\,5\,9\,3\,1\,2\,7$$

corresponds the Lehmer encoding

$$\ell = 0\,0\,2\,2\,0\,5\,6\,6\,2\,.$$

It can be noted that σ and ℓ have the same shape $\mathbf{a} = (2,3,1,3)$. This point will be established in the next proposition.

PROPOSITION 11.4.2. *The Lehmer encoding is a bijection between the set of permutations of $[n]$ and the set of words ℓ of length n such that $0 \le \ell_i \le i-1$ for $1 \le i \le n$. This bijection has the following properties:*
(i) *σ and ℓ have the same shape,*
(ii) *The sum of the letters of ℓ is the number of inversions of σ.*

Proof. From the definition, it is clear that $0 \le \ell_i \le i$ for $1 \le i \le n$. Proving that the Lehmer encoding is a bijection is done by describing its reverse. This is left as an elementary exercise (To start, observe that the position of 1 in σ is the greatest index i such that $\ell_i = i-1$).

If $\sigma(i+1) < \sigma(i)$ then for any $j < i$ one has $\sigma(j) > \sigma(i) \Rightarrow \sigma(j) > \sigma(i+1)$. Therefore $\ell_{i+1} \ge \ell_i$. Since i is smaller than $i+1$ and $\sigma(i) > \sigma(i+1)$, one has in fact $\ell_{i+1} > \ell_i$. Conversely, if $\sigma(i+1) > \sigma(i)$ then for any $j < i$ one has $\sigma(j) > \sigma(i+1) \Rightarrow \sigma(j) > \sigma(i)$. Therefore $\ell_(i+1) \le \ell_(i)$. This proves that σ and ℓ have the same shape.

The second assertion is obvious from the definition of the Lehmer encoding. ■

PROPOSITION 11.4.3. *Let $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ be a shape, σ be a permutation of shape $\mathbf{a}$ and ℓ be the Lehmer encoding of σ. Denote by $\mathbf{N}$ the sequence $(N_0, N_{a_1}, N_{a_1+a_2}, \ldots, N_{a_1+a_2+\cdots+a_{k-1}})$. Then ℓ is an element of $W(\mathbf{a}, \mathbf{N})$. Furthermore, the Lehmer encoding induces a bijection between the set of permutations of shape $\mathbf{a}$ and $W(\mathbf{a}, \mathbf{N})$.*

Proof. Let $0 \le i < k$ and let r be 0 if $i = 0$ and $a_1 + a_2 + \cdots + a_i$ otherwise. As $\ell_{r+1} \le r$ (general property of Lehmer codes) and $\ell_{r+1} \ge \ell_{r+2} \ge \cdots \ell_{r+a_{i+1}}$ (because ℓ has shape $\mathbf{a}$), it follows that, for $r+1 \le j \le r + a_{i+1}$, one has $0 \le \ell_j \le r$. This implies that ℓ is in $W(\mathbf{a}, \mathbf{N})$.

The conditions on the alphabets ensure that every element of $W(\mathbf{a}, \mathbf{N})$ is an admissible Lehmer encoding. The corresponding permutation has the same shape $\mathbf{a}$, which prove the bijection part of the proposition. ■

Using the same arguments than at the end of Section 11.3, it is possible to derive the enumeration of permutations of special shapes by number of inversions. This leads to the following theorem, which can also be proved using Foata's "Second Fundamental Transformation". See Lothaire 1983.

THEOREM 11.4.4 (Foata-Schützenberger). *Let $\mathbf{a}$ be a composition of n. Then, for any integer m, the number of permutations of shape $\mathbf{a}$ having m inversions is the same as the number of permutations of shape $\mathbf{a}$ having m backsteps.*

Proof. Proposition 11.3.7 gives a determinantal expression for the generating polynomial of permutations of given shape by imaj. We shall establish a similar expression for the generating polynomial of the same permutations by number of inversions. Finally, we shall verify that both determinants are equal.

If σ is a permutation of shape $\mathbf{a}$, its number of inversions $\operatorname{inv}\sigma$ is the sum of the letters of ℓ (Proposition 11.4.2). This implies that the generating polynomial $\sum_\sigma q^{\operatorname{inv}\sigma}$ is obtained by substituting q^i to i in $S(\mathbf{a},\mathbf{X})$, where $\mathbf{X}$ is defined in Proposition 11.4.3.

We use the determinantal formula of Proposition 11.2.2 $S(\mathbf{a},\mathbf{X}) = \det(M)$ where, in this particular case:

$$M_i, j = \begin{cases} S_{a_i+a_{i+1}+\cdots+a_j}(X_{a_1+\ldots+a_{i-1}}) & \text{if } i \le j, \\ 1 & \text{if } i = j+1, \\ 0 & \text{if } i > j+1. \end{cases} \tag{11.4.1}$$

Proposition 11.1.1 implies that, when substituting q^i to i in the entries of this determinant, its generic element becomes:

$$\begin{cases} (q)_{a_1+\cdots+a_j}/(q)_{a_1+\cdots+a_{i-1}}(q)_{a_i+\cdots+a_j} & \text{if } i \le j, \\ 1 & \text{if } i = j+1, \\ 0 & \text{if } i > j+1. \end{cases}$$

We can then factor $(q)_{a_1+\cdots+a_j}$ in column j and $(q)^{-1}_{a_1+\cdots+a_{i-1}}$ in row i.

Thus, the generating polynomial of permutations of shape $\mathbf{a}$ by number of inversions $\sum_\sigma q^{\operatorname{inv}\sigma}$ is equal to

$$\prod_{1\le i,j\le k} \frac{(q)_{a_1+\cdots+a_j}}{(q)_{a_1+\cdots+a_{i-1}}} \times \det(((q)_{a_i+\cdots+a_j})_{\{1\le i,j,\le k\}}),$$

with the conventions that the generic term of the determinant is 1 if $i = j+1$ and 0 if $i > j+1$. After canceling we obtain

$$(q)_{a_1+\cdots+a_k}\det((1/(q)_{a_i+\cdots+a_j})_{\{1\le i,j,\le k\}}),$$

which, since $a_1+\cdots+a_k = n$, is Equation 11.3.4 of Proposition 11.3.7. ∎

11.5. Lyndon factorization and cycles of permutations

Recall from Chapter 1, Section 1.2.1 that a *Lyndon word* of length n is a word $w = w_1w_2\cdots w_n$ whose letters are nonnegative integers, which is strictly smaller lexicographically than its conjugates. As a consequence, a Lyndon word is primitive.

The following result, due to Lyndon, will play the role of the factorization of Section 11.2.

Theorem 11.5.1 (Lyndon). *Any word w can be written uniquely as a nonincreasing product $w = u_1u_2\cdots u_k$ of Lyndon words.*

The lengths of the Lyndon factors constitute a partition λ of n, which will be called the *type* of w.

EXAMPLE 11.5.2. The word $w = 2\,1\,0\,1\,2\,0\,1\,0\,1$ of length 9 has the following Lyndon factorization:

$$w = 2 \quad 1 \quad 0\,1\,2 \quad 0\,1 \quad 0\,1.$$

The type of w is the partition $\lambda = 32211$ of 9.

The same Lyndon factorization can be performed on permutations (for the same technical reasons as in Section 11.3, the order has to be reversed). Start with a permutation τ considered as the concatenation of its values. Its Lyndon factorization (for the reverse order) is $\tau = \theta_1\theta_2\ldots\theta_k$. Consider each Lyndon word θ_j as the sequence of the values of cyclic permutation. Finally, let σ be the product (in the symmetric group) of those cycles.

This transformation from τ to σ is a bijection of the symmetric group onto itself. Its inverse is known as Foata's "first fundamental transformation". In the case of permutations, the first fundamental transformation can be easily described: Start with a permutation σ. Consider its decomposition as a product of cycles. Write each cycle with its greatest value first. Finally, concatenate those words in increasing order of their first element. The resulting word is τ.

If σ is a permutation of $[n]$, the multiset of the lengths of its cycles is a partition of n, which will also be called the *type* of σ. The type of a permutation is characteristic of its conjugacy class in the symmetric group, but we shall not use this property in the sequel.

EXAMPLE 11.5.3. Let

$$\tau = \tau(1)\tau(2)\ldots\tau(9) = 1\,4\,7\,3\,2\,8\,5\,9\,6.$$

As a word, its Lyndon factorization (for the reverse order) is

$$\tau = 1 \quad 4 \quad 7\,3\,2 \quad 8\,5 \quad 9\,6.$$

Hence the resulting permutation σ is the product of cycles

$$\sigma = (1)(4)(7\,3\,2)(8\,5)(9\,6).$$

As a word,

$$\sigma = \sigma(1)\sigma(2)\ldots\sigma(9) = 1\,7\,2\,4\,8\,9\,3\,5\,6.$$

We are now ready to describe the *Gessel normalization* of a word w, which will play the same role for the cycle decomposition as the standard normalization of Section 11.3 did for the shape.

Let $w = w_1w_2\cdots w_n$ be a word of length n and $w = u_1u_2\cdots u_k$ be its Lyndon decomposition. Suppose that letter w_i of w is in the Lyndon factor $u_r = w_{r_1}w_{r_2}\cdots w_{r_s}$. Let $p(i) = w_iw_{i+1}\cdots w_{r_s}u_r^\omega$ be the infinite word obtained by writing the suffix of u_r starting with w_i and concatenating to it an infinite number of copies of u_r. Then, we can define the total order $\preceq$ on $[n]$ by

$$i \prec j \text{ iff } \begin{cases} p(i) > p(j), \text{ or} \\ p(i) = p(j) \text{ and } i < j. \end{cases} \tag{11.5.1}$$

Let $\tau(i)$ be the rank of index i according to this total order. Now apply to τ the inverse of Foata's first fundamental transformation to obtain σ. This last permutation is the Gessel normalization of w.

We shall need the following technical lemma to prove Proposition 11.5.5.

LEMMA 11.5.4. *Let u and v be two words such that lexicographically $u > v$. Suppose that u is a Lyndon word. Then, as infinite words and for the lexicographic order, $u^\omega > v^\omega$.*

Proof. Let us say that u is strongly greater that v—which we write $u \gg v$—when $u > v$ and v is not a proper prefix of u. The following statement is easy to prove: If $u \gg v$, then $ux > vy$ for any words x and y.

Thus, if $u \gg v$, the lemma is true even if u is not a Lyndon word.

Suppose now that v is a proper prefix of u. We can factor $u = v^k u'$ for some $k \geq 1$, where v is not a proper prefix of u'. (The case when u' is empty is to be excluded, as $u \neq v$ and u is Lyndon, hence primitive.) Then, being a Lyndon word, u is strictly smaller than any of its proper suffixes (Lothaire1, Proposition 5.1.2), that is $u < u'$. As $u > v$ by hypothesis, we have $u' > v$. As v is not a proper prefix of u', we have in fact $u' \gg v$. Then $u'u^\omega > vv^\omega$. Multiplying on the left by v^k yields $u^\omega > v^\omega$. ∎

PROPOSITION 11.5.5. *A word w and its Gessel normalization σ have the same type.*

Proof. We shall prove that the Lyndon factorizations of w and that of permutation τ have corresponding Lyndon factors of the same length. That will imply the proposition since the factors of τ correspond to the cycles of σ.

Consider $w = u_1 u_2 \cdots u_k$. The factor u_r, written as a concatenation of letters, is equal to $w_{r_1} w_{r_2} \cdots w_{r_s}$. Let i be an index such that $r_1 < i \leq r_s$. Then

$$p(i) = w_i \cdots w_{r_s} u_r^\omega.$$

Since u_r is a Lyndon word, $p(r_1) < p(i)$ so that $i \prec r_1$ and, consequently, $\tau(r_1) > \tau(i)$. This proves that $\tau(r_1)$ is strictly greater than any of the $\tau(i)$, $i = r_1 + 1, \ldots, r_s$. So $\tau(r_1)\tau(r_1+1)\cdots\tau(r_s)$ is eligible as a Lyndon factor of τ.

To finish the proof, we must show that the first letters of those potential factors of τ are increasing. Let $u_r = w_{r_1} w_{r_2} \cdots w_{r_s}$ and $u_f = w_{f_1} w_{f_2} \cdots w_{f_g}$ be two Lyndon factors of w such that $r_1 < f_1$. Then, either $u_r = u_f$. In that case $p(r_1) = p(f_1)$ and $r_1 < f_1$ so $r_1 \prec f_1$, hence $\tau(r_1) < \tau(f_1)$, which is what is expected. In the other case $u_r \neq u_f$. Then, for the lexicographic order $u_r > u_f$. We can then apply Lemma 11.5.4 so that $p(r_1) = u_r^\omega > p(f_1) = u_f^\omega$. This implies that $r_1 \prec f_1$ which in turn implies that $\tau(r_1) < \tau(f_1)$. This is exactly what was needed to complete the proof. ■

Example 11.5.6. Let $w = 2\,1\,0\,1\,2\,0\,1\,0\,1$ as in Example 11.5.2. Its Lyndon factorization is

$$w = 2 \quad 1 \quad 0\,1\,2 \quad 0\,1 \quad 0\,1\,.$$

For that w, we find:

$$\begin{array}{ll} p(1) = 222222\ldots & p(2) = 111111\ldots \\ p(3) = 012012\ldots & p(4) = 120120\ldots \\ p(5) = 201201\ldots & p(6) = 010101\ldots \\ p(7) = 101010\ldots & p(8) = 010101\ldots \\ p(9) = 101010\ldots & \end{array}$$

The order $\preceq$ on the indices is then:

$$1 \prec 5 \prec 4 \prec 2 \prec 7 \prec 9 \prec 3 \prec 6 \prec 8\,.$$

Consequently,

$$\tau = 1\,4\,7\,3\,2\,8\,5\,9\,6,$$

which has the following Lyndon decomposition:

$$\tau = 1 \quad 4 \quad 7\,3\,2 \quad 8\,5 \quad 9\,6\,.$$

As a product of cycles,

$$\sigma = (1)(4)(732)(85)(96),$$

which, written as the sequence of its values is

$$\sigma = 1\,7\,2\,4\,8\,9\,3\,5\,6\,.$$

11.6. Major index of permutations with a given cyclic type

In Section 11.5, a shape-preserving normalization was used to enumerate permutations with a given shape by backsteps. In this section, the type-preserving Gessel normalization will allow the same enumeration for permutations with a given type by descents.

Let w be a word and $\psi(w)$ be the pair (σ, s) consisting of the Gessel normalization of σ and of the nonincreasing reordering s of the letters of w.

Theorem 11.6.1. *Let λ be a partition of n. Then ψ is a bijection between the set of words w of type λ and the set of pairs (σ, s), where σ is a permutation of type λ and s a nonincreasing sequence compatible with* $\operatorname{DES}\sigma$.

Proof. We already know (Proposition 11.5.5) that w and σ have the same type.

Suppose that $i < j$ and call $\tau^{-1}(i) = a$ and $\tau^{-1}(j) = b$. As $\tau(a) < \tau(b)$, we deduce from the definition of τ that $a \prec b$ and so $p(a) \geq p(b)$. This latter relation implies that the first letters of each infinite word also satisfy $w_a \geq w_b$. We have then proved

$$i < j \Rightarrow w_{\tau^{-1}(i)} \geq w_{\tau^{-1}(j)}.$$

As for Theorem 11.3.2, this proves that $s(i) = w_{\tau^{-1}(i)}$.

To prove that s is compatible with $\operatorname{DES}\sigma$, we shall prove the (apparently) more general result that if $i < j$ and $\sigma(i) = a > \sigma(j) = b$, then $s_i > s_j$. We already know that $s(i) \geq s(j)$.

Let us suppose then that $i < j$ (that is $a \prec b$) and $s_i = s_j$. This is the same as $w_a = w_b$. We also know that $p(a) \geq p(b)$. But $p(a) = w_a p(\bar{a})$ and $p(b) = w_b p(\bar{b})$. As $w_a = w_b$, it follows that $p(\bar{a}) \geq p(\bar{b})$. The index $\bar{a}$ is the index of the element immediately following i cyclically in the Lyndon factor to which it belongs, so that $\tau(\bar{a}) = \sigma(i)$.

We face two possibilities:

If $p(\bar{a}) > p(\bar{b})$, then, by definition, $\bar{a} \prec \bar{b}$, which implies $\tau(\bar{a}) < \tau(\bar{b})$, which is also $\sigma(i) < \sigma(j)$.

If $p(\bar{a}) = p(\bar{b})$ then $p(a) = p(b)$. As $a \prec b$, we must have $a < b$. Then w_a and w_b are in two equal Lyndon factors of w and the one containing w_a precedes the one containing w_b. But $w_{\bar{a}}$ and $w_{\bar{b}}$ belong to the same factors, which implies $\bar{a} \prec \bar{b}$. Then, as in the previous case, $\sigma(i) < \sigma(j)$.

We have then proved that $i < j$ and $s_i = s_j$ imply $\sigma(i) < \sigma(j)$, which implies the compatibility of s with the set $\operatorname{DES}\sigma$.

To prove that ψ is a bijection, start with σ, then construct τ by rearranging the cycles of σ using Foata's first fundamental transformation. Then define the word w by $w_a = s_{\tau(a)}$. To verify that $\psi(w) = (\sigma, s)$ we only have to verify that the Lyndon decompositions of w and of τ have corresponding factors of the same length.

To do so, given an index a, define a $p(a)$ from τ: If $\tau(a)$ belongs to the Lyndon factor $\theta_r = \tau(r_1)\cdots\tau(r_s)$, let $p(a) = w_a \cdots w_{r_s} w_{r_1} \cdots w_a \cdots$ The nonincreasing property of s ensures that, if $\tau(a) < \tau(b)$, then $w_a = s_{\tau(a)} \geq s_{\tau(b)} = w_b$.

Suppose then that $\tau(a)$ and $\tau(b)$ belong to the same Lyndon factor of τ and that $\tau(b)$ is the first (and greatest) letter of that factor. If $w_a > w_b$ we have $p(a) > p(b)$ which implies that the corresponding factor of w satisfies the minimality property of Lyndon words. If $w(a) = w(b)$ consider the cyclic successors $\bar{a}$ and $\bar{b}$. Then, as before, $\tau(\bar{a}) = \sigma(\tau(a))$. As s is compatible, we have $\sigma(\tau(a)) < \sigma(\tau(b))$, which is $\tau(\bar{a}) < \tau(\bar{b})$. If $w_{\bar{a}} > w_{\bar{b}}$, we can again conclude that $p(a) > p(b)$, otherwise we iterate until the iterated cyclic successor of a is b, which leads to a contradiction with the fact that θ_r is a Lyndon word.

The factors of w corresponding to the Lyndon factors of τ are consequently Lyndon words. We still have to prove that they constitute the Lyndon decomposition of w, *ie* that they are in nonincreasing order.

Suppose then that $\tau(a)$ and $\tau(b)$ do not belong to the same Lyndon factor of τ. Suppose that each of them is the first letter of its respective Lyndon factor, and $a < b$. This implies that $\tau(a) < \tau(b)$. If $w_a > w_b$ we have as above $p(a) > p(b)$ which implies from Lemma 11.5.4 that the corresponding factors of w are in nonincreasing order. Otherwise, if $w_a = w_b$, and for the same reason as above, either we find successors of a' of a and b' of b such that, for the first time, $p(a') > p(b')$, and so $p(a) > p(b)$. In the other case, for all corresponding letters of both factors we have $p(a') = p(b')$ which implies (as Lyndon words are primitive) that the corresponding factors of w are equal, and so in nonincreasing order. ∎

EXAMPLE 11.6.2. Proceed with Example 11.5.6. We have found that

$$\begin{aligned} w &= 2\,1\,0\,1\,2\,0\,1\,0\,1, \\ \tau &= 1\,4\,7\,3\,2\,8\,5\,9\,6, \\ \sigma &= 1\,7\,2\,4\,8\,9\,3\,5\,6 \quad \text{and} \\ s &= 2\,2\,1\,1\,1\,1\,0\,0\,0. \end{aligned}$$

The descent set of σ is $\{2, 6\}$. Notice that $s_2 > s_3$ and $s_6 > s_7$.

Since the descent set of a permutation is the backstep set of its inverse, and since both permutations have the same type, Theorem 11.6.1 can also be used for counting permutations with a given type by its backsteps.

Let $L(\lambda, X)$ the commutative image of the sum of all words on the alphabet N with type λ.

COROLLARY 11.6.3. *Let λ be a partition of n and A be a subset of $[n-1]$. Denote by $E_A(\lambda)$ the number of permutations with type λ whose descents are precisely the elements of A. Then*

$$L(\lambda, X) = \sum_{A \subset [n-1]} E_A(\lambda) \sum_s GS(s), \tag{11.6.1}$$

where the second sum is over the set of all nonincreasing sequences s compatible with λ.

Proof. It is identical to that of Corollary 11.3.4 ∎

There is also an analogue of Corollary 11.3.5.

COROLLARY 11.6.4. *Let λ be a partition of n. Then*

$$\sum_\sigma q^{\operatorname{maj}\sigma} = \sum_\sigma q^{\operatorname{imaj}\sigma} = (q)_n L(\lambda, \{1, q, q^2, \ldots\}), \tag{11.6.2}$$

where the sum is over the set of permutations of $[n]$ of type λ.

As a consequence, any information about $L(\lambda, X)$ can be used to derive information about the distribution of descents on permutations with type λ. No "general" formula, similar to the determinant of Proposition 11.2.2, is known.

Some particular cases of types, such as cyclic permutations, involutions, derangements will be given as exercises.

Contrary to what happens for permutations with a given shape, the distribution of inversions is in general different from that of descents. There is no analogue of Theorem 11.4.4 for permutations with a given type.

Problems

Section 11.1

11.1.1 (The q-binomial theorem) The generating series for all words on the alphabet N is:

$$E(X) = \sum_{a \geq 0} S_a(X) = \prod_{i \in N} (1 - x_i)^{-1}.$$

From this, it is easy to derive the q-binomial theorem:

$$\sum_{a \geq 0} \begin{bmatrix} a+k \\ k \end{bmatrix} t^a = \prod_{0 \leq i \leq k} (1 - tq_i)^{-1}$$

and Euler's q-exponential series:

$$e(t;q) = \sum_{a \geq 0} \frac{t^a}{(q)_a} = \prod_{0 \leq i} (1 - tq_i)^{-1}.$$

See for example Andrews 1976.

Section 11.2

11.2.1 The simplest nontrivial case for Theorem 11.2.2 is when $\mathbf{a} = (k, n-k)$. In that case,

$$S(\mathbf{a}, X) = S_k(X) S_{n-k}(X) - S_n(X).$$

11.2.2 Consider alternating words of odd length n, *i.e.* words with shape $\mathbf{a} = (2, 2, \ldots, 2, 1)$. Denote by X' the set of indeterminates $\{x_1, x_2, \ldots\}$. Prove that the generating series $S(\mathbf{a}, X) = \tan(X)$ for alternating words satisfy the recurrence relation:

$$\tan(X) - \tan(X') = x_0(1 + \tan(X)\tan(X')).$$

To do so, consider the last occurrence of the letter 0 in an alternating word. Note the similarity with the classical differential equation satisfied by the tangent function.

From this recurrence, by recurrence on the size of X, and by letting this size tend to infinity, derive the formula:

$$\tan(X) = \frac{1}{i} \frac{E(iX) - E(-iX)}{E(ix) + E(-iX)}.$$

(By iX, we mean the set obtained by multiplying each indeterminate by the square root of -1 in the series $E(X)$ as defined in Problem 11.1.1.) Similarly, for alternating words of even length, one obtains as generating series:

$$\sec(X) = \frac{2}{E(ix) + E(-iX)}.$$

See Désarménien 1983.

11.2.3 Let $A_{n,k}(X)$ be the generating series for words of length n whose shapes contain k parts. Let $A(X) = \sum_{n,k\geq 0} A_{n,k}(X)u^k$. By considering the first occurrence of the letter r, prove that:

$$A(X_r)(1 - x_r F(X_{r-1})) = (1 - x_r(1-u))A_(X_{r-1}).$$

It then follows that:

$$A(X) = \frac{1-u}{1 - uE((1-u)X)}.$$

See Désarménien 1983.

Section 11.3

11.3.1 From Problem 11.2.1 and from Corollary 11.3.5, it follows that the enumeration by imaj of permutations of $[n]$ with only one descent in position k is:

$$\begin{bmatrix} n \\ k \end{bmatrix} - 1.$$

This is a particular case of a more general result proved in Gessel and Reutenauer 1993.

11.3.2 (The q-Euler numbers)Consider the q-exponential $e(t; q)$. The q-tangent and q-secant series may be defined by:

$$\tan(t; q) = \frac{1}{i}\frac{e(it; q) - e(-it; q)}{e(it; q) + e(-it; q)} \quad \text{and} \quad \sec(x; q) = \frac{2}{e(it; q) + e(-it; q)}.$$

The q-Euler numbers $\mathrm{EUL}_n(q)$ (also called tangent and secant numbers) are the coefficients of the series expansions of those functions:

$$\sum_{n\geq 0} \mathrm{EUL}_n(q)\frac{t^n}{(q)_n} = \tan(t; q) + \sec(t; q).$$

Using Problem 11.2.2, prove that $\mathrm{EUL}_n(q)$ enumerates alternating permutations of $[n]$ by imaj. (Alternating permutations are those whose shape is $(2, 2, 2, \ldots 2)$ or $(2, 2, 2, \ldots 1)$, depending on the parity of n.) By letting q tend to 1, one obtains André's classical interpretation of the Euler numbers as counting alternating permutations. See Désarménien 1983.

11.3.3 (The q-Eulerian polynomials) The q-Eulerian polynomials are defined by

$$\sum_{n\geq 0} A_n(u;q)\frac{t^n}{(q)_n} = \frac{1-u}{1-ue((1-u)t;q)}.$$

From Problem 11.2.3, prove that the coefficient of u^k in $A_n(u;q)$ enumerates permutations of $[n]$ with $k-1$ descents (*i.e.* their shape is a composition with k parts) by imaj. This generalizes the classical interpretation of the Eulerian polynomials as generating functions for permutations according to the number of descents. See Désarménien 1983.

Section 11.4

11.4.1 (The q-Euler numbers again) According to Theorem 11.4.3, the q-Euler numbers also enumerate the alternating permutations of $[n]$ by number of inversions. This can be proved directly from the definitions of the q-tangent and q-secant series. The q-derivative of a series $f(t;q)$ is $D_q f(t;q) = (f(t;q) - f(tq;q))/t$. Prove that the q-tangent and q-secant series satisfy the following q-differential equations:

$$D_q(\tan(t;q) + \sec(t;q)) = 1 + \tan(t;q)(\tan(tq;q) + \sec(tq;q)).$$

It follows that the q-Euler numbers satisfy the following quadratic recurrence:

$$\mathrm{EUL}_{n+1}(q) = \sum_{0\leq j\leq (n-1)/2} \begin{bmatrix} n \\ 2j+1 \end{bmatrix} q^{n-2j-1}\, \mathrm{EUL}_{2j(+1}\, q)\, \mathrm{EUL}_{n-2j-1}(q).$$

By considering the position of $n+1$ in an alternating permutation of length $n+1$ and counting the inversions, it can be shown that the enumeration of permutations by number of inversions satisfy the same quadratic recurrence. See Désarménien 1982.

Section 11.5

11.5.1 Actually, Lemma 11.5.4 provides a characterization of Lyndon words. Prove that the following statements are equivalent:

(i) u is a Lyndon word;

(ii) for any word v, it is equivalent that $u > v$ and $u^\omega > v^\omega$.

Section 11.6

11.6.1 (The q-counting of cycles) The generating series of Lyndon words of length n on the alphabet X is

$$L_n(X) = \frac{1}{n}\sum_{d|n} \mu(d)\Big(\sum_i x_i^d\Big)^{n/d}.$$

This can be obtained by observing that any word of length n is some power of a primitive word, taking the commutative image and using Möbius inversion. By substituting powers of q to indeterminates, one obtains the enumeration of n-cycles by imaj:

$$C_n(q) = \frac{(q)_n}{n} \sum_{d|n} \frac{\mu(d)}{(1-q^d)^{n/d}}.$$

See Gessel and Reutenauer 1993.

11.6.2 (Derangements and desarrangements) A derangement is a permutation without fixed points. A desarrangement is a permutation whose first ascent is even (*i.e.* its shape starts with an odd number of 1's). A derangement is a permutation with a given cycle structure (no 1-cycle) and a desarrangement is a permutation with a given shape.
If A is a subset of $[n-1]$, then the number of derangements whose backsteps are the elements of A is equal to the number of desarrangements whose backsteps are the elements of A. This can be proved by showing that the generating series of both types of permutations are equal, then applying Corollaries 11.3.4 and 11.6.3.
Then the number of derangements and of desarrangements counted by imaj are equal. Their common value is:

$$d_n(q) = [n]! \sum_{0 \le k \le n} \frac{(-1)^k q^{k(k-1)/2}}{[k]!},$$

where $[n]! = (q)_n/(1-q^n)$. This is the natural q-analogue of the number of derangements. This problem has been considered in Désarménien and Wachs 1988, Désarménien and Wachs 1993 and Gessel and Reutenauer 1993.

11.6.3 (Involutions) An involutions has cycles of length 1 or 2. Let $I_{n,k}(X)$ be the generating series for words on the alphabet N corresponding to involutions of $[n]$ with k fixed points. Prove that:

$$\sum_{n,k} I_{n,k}(X)u^k = \prod_{i \in N}(1-ux_i)^{-1} \prod_{i<j \in N}(1-x_ix_j)^{-1}.$$

From this generating series, one can derive the generating series for the number $I_{n,k}$ of involutions of $[n]$ with k fixed points:

$$\sum_{n,k} I_{n,k}(X)u^k \frac{t^n}{(q)_n} = \prod_{0 \le i}(1-utq^i)^{-1} \prod_{0 \le i<j}(1-t^2q^iq^j)^{-1}.$$

See e.g. Désarménien and Foata 1985 and Gessel and Reutenauer 1993.

11.6.4 (A symmetry property) The generating series considered for words on the alphabet N with a given shape or with a given type are symmetric functions of the indeterminates. This translates into a symmetry property for the distribution of the backsteps on permutations on $[n]$ with a given shape or with a given type. More precisely, any subset $A = \{a_1 < a_2 < \cdots < a_k\}$ of $[n]$ can be encoded by a composition $c(A)$ of n, namely, $(a_1, a_2 - a_1, \ldots, n - a_k)$. Then, given a composition $\mathbf{a}$ of n, the number of permutations of $[n]$ with a given shape or with a given type, such that their backsteps are a subset of $c^{-1}(\mathbf{a})$ does not depend on the order of the parts of $\mathbf{a}$.

For example, with $n = 4$, to the partition $(2,1,1)$ correspond 3 compositions, $(2,1,1)$, $(1,2,1)$ and $(1,1,2)$. The corresponding sets A are respectively $\{2,3\}$, $\{1,3\}$ and $\{1,2\}$. There are 5 permutations of $[4]$ of shape $(2,2)$: 1324 (backstep 2), 1423 (backstep 3), 2314 (backstep 1), 3412 (backstep 2) and 2413 (backsteps 1 and 3). Among those permutations 3 have backsteps in each of the sets A. See Désarménien 1990.

Notes

The major ingredients to this chapter are q-calculus and symmetric functions. What is needed of the former can be found in Andrews 1976. An excellent introduction to symmetric function is contained in Chapter 1 of Macdonald 1995. In it can also be found the essence of Corollary 11.3.5.

Actually, the determinant in Section 11.2 is a particular case of a Schur function on a flag of alphabets. This concept is due to Lascoux, and can be found in Lascoux 1974. If all alphabets are equal, it becomes the determinantal expression of a Schur function of ribbon shape. Corollary 11.3.5, as well as Corollary 11.6.4, can be extended to the case of finite alphabets. What arises is a double generating function for imaj and the number of descents. This is Theorem 4.1 of Désarménien and Foata 1985, which contains various applications of this theorem, in particular to involutions (*cf.* Problem 11.6.3). See also Désarménien and Foata 1991.

The key to Section 11.4, which is the use of Lehmer encoding together with a Schur function on a flag of alphabets is due to Thibon. This leads to a new proof of Theorem 11.4.4, which was originally proved bijectively in Foata and Schützenberger 1970.

A proof of Theorem 11.5.1 can be found in Chapter 5 of Lothaire 1983. In Chapter 10 of the same reference, Foata's "First Fundamental Transformation" is described.

The Gessel Normalisation is to be found in Gessel and Reutenauer 1993, along with many enumerative results related to descent sets and cycle structure. This article contains different formulations of Sections 11.3, 11.5 and 11.6 in the setting of symmetric functions. This encoding had been exploited earlier in Désarménien and Wachs 1988 and Désarménien and Wachs 1993.