Minimal Factorizations of a Cycle and Central Multiplicative Functions on the Infinite Symmetric Group

Philippe Biane

C.N.R.S., Laboratoire de Probabilités, Tour 56, 3ème étage, Université Paris VI, 4, Place Jussieu, 75252 Paris cedex 05, France and
DMI, École Normale Supérieure, 45, rue d’Ulm, 75005 Paris

Communicated by the Managing Editors

Received March 13, 1995

We show that the number of factorizations \( \sigma = \chi_1 \cdots \chi_r \) of a cycle of length \( n \) into a product of cycles of lengths \( a_1, \ldots, a_r \), with \( \sum_{j=1}^r (a_j - 1) = n - 1 \), is equal to \( n^{r-1} \). This generalizes a well known result of J. Denes, concerning factorizations into a product of transpositions. We investigate some consequences of this result, for central multiplicative functions on the infinite symmetric group, and use them to give a new proof of a recent result of A. Nica and R. Speicher on non-crossing partitions.


INTRODUCTION

It is well known that a cycle of order \( n \) cannot be written as a product of less than \( n - 1 \) transpositions. On the other hand, the number of factorizations of such a cycle into a product of exactly \( n - 1 \) transpositions is equal to \( n^{n-2} \). This result was first proved by J. Denes [D]. A bijective proof, consisting in establishing an explicit bijection between the set of factorizations and the set of labelled trees on \( n \) vertices (which has cardinality \( n^{n-2} \) by Cayley’s theorem) has been given by Moszkowski [M] (see also Goulden and Pepper [G-P]).

We shall investigate more general factorizations of a cycle into a product of cycles. If a cycle of order \( n \) has a factorization into a product of \( r \) cycles of orders \( a_1, \ldots, a_r \), all \( \geq 2 \), then

\[
(a_1 - 1) + \cdots + (a_r - 1) \geq n - 1
\]

Such a factorization is called minimal if there is equality in (\text{*}), and we call the sequence \( (a_1, \ldots, a_r) \) the class of the factorization.
**Theorem 1.** Let \((a_1, \ldots, a_r)\) be integers, all \(\geq 2\), and \(n = 1 + \sum_{j=1}^r (a_j - 1)\), then a cycle of order \(n\) has exactly \(n^{r-1}\) distinct factorizations of class \((a_1, \ldots, a_r)\).

In the case where \(a_1 = a_2 = \cdots = a_r\), this result is proved in [G-J], Corollary 5.1. In fact, the argument given in [G-J], which relies on generating series and the theory of symmetric functions, can be extended to yield the full result of Theorem 1. In what follows, we will give a new proof of Theorem 1, by exhibiting a simple explicit bijection between the set of minimal factorizations, as in the statement of Theorem 1, and the set \(E^{r-1}\) where \(E\) is the set of elements permuted by the cycle. Since there are known bijections between the sets of labelled trees on \(n\) vertices and the set of sequences of length \(n-1\) of elements of \([1, \ldots, n]\), we obtain, in the case of product of transpositions, a solution to the problem dealt with in [M, G-P] (we did not check whether the construction we obtain in this case is distinct from that of [M or G-P]).

A number of straightforward corollaries can be drawn from Theorem 1. Let \(k = (k_2, k_3, \ldots, k_m, \ldots)\) be a sequence of nonnegative integers, of which only a finite number are nonzero, and such that \(n = 1 + \sum_{j=2}^m (j-1)k_j\). A factorization of a cycle of order \(n\) into a product of cycles with exactly \(k_j\) cycles of order \(j\) for each \(j \geq 2\) will be called of type \(k\). Of course, such a factorization is minimal. Let \(K\) be the set of sequences \(k_2, k_3, \ldots, k_m, \ldots\) of nonnegative integers, all zero except a finite number, for \(k \in K\), let us introduce the notations

\[
\begin{align*}
  r(k) &= \sum_{j=2}^m k_j, \\
  k! &= \prod_{j=2}^m k_j!, \\
  n(k) &= 1 + \sum_{j=2}^m (j-1)k_j.
\end{align*}
\]

From Theorem 1 one can easily deduce that

**Corollary 1.** The number of minimal factorizations of type \(k\) of a cycle of order \(n(k)\) is

\[
(r(k)!k!)^{n(k)r(k)^{-1}}.
\]

**Corollary 2.** The number of minimal factorizations of a cycle of order \(n\) into a product of \(l\) cycles (with \(1 \leq l \leq n-1\)) is equal to

\[
((n-2)!/(l-1)!/(n-l-1)!)^{n^{l-1}}.
\]

**Corollary 3.** The number of minimal factorizations of a cycle of order \(n\) is \((n+1)^{n-2}\).

We will derive a certain number of consequences of this result, which concern central multiplicative functions on \(S_{\omega}\), the infinite symmetric group (see definition in Section 3 below). Such functions play an important role in the representation theory of \(S_{\omega}\) (see, e.g., [K-V]). The usual convolution is not
well defined for central functions on the infinite symmetric group since the conjugacy classes, except that of the identity element, are infinite, but one can modify the definition by defining the restricted convolution of two functions on $S_\infty$ by the formula

$$f \star g(\pi) = \sum_{|\chi| + |\chi^{-1}\pi| = |\pi|} f(\chi) g(\chi^{-1}\pi),$$

where $|\chi|$ is the word length of $\chi$ with respect to the generating set of all transpositions. This convolution is essentially the same as the convolution of multiplicative functions on the lattice of noncrossing partitions, which has been introduced by Speicher in [S2]. The precise relation between the two notions will be explained in Section 1.3, it is based on a connection between permutations and noncrossing partitions which has already been used in [Bi]. In analogy with Nica and Speicher in [N-S], we will define a “Fourier transform'' for central multiplicative functions on $S_\infty$, and show that it converts the restricted convolution into the multiplication of formal power series. More precisely we will define a bijective map $f \mapsto \mathcal{F} f$ between central multiplicative functions on $S_\infty$ and formal power series in the indeterminate $z$ such that

$$\mathcal{F} f \star \mathcal{F} g = \mathcal{F}(f g).$$

This will give a new proof of the main result of [N-S]. In fact, our original motivation for studying the restricted convolution was to understand Nica and Speicher’s result in terms of the infinite symmetric group. Note that Nica and Speicher have used their result to give a combinatorial treatment of the multiplicative free convolution of measures, introduced by Voiculescu (see [D-N-V]).

It turns out that the computation of the restricted convolution is equivalent to the computation of the top connection coefficients in the symmetric group; see Section 3.1 below. A formula for these coefficients has been given in [G-J], and was one ingredient for deducing the Corollary 5.1, so what we do in this paper is to follow the reverse path and deduce the formula for the top connection coefficients from a direct proof of Theorem 1, without any use of symmetric function theory.

This paper is organized as follows. In the first part we make some remarks on the infinite symmetric group, on minimal factorizations of permutations, and on the connection with noncrossing partitions. In part 2 we prove Theorem 1 and, finally, in part 3 we introduce central multiplicative functions on $S_\infty$, their Fourier transforms, and the restricted convolution; then we prove that Fourier transform converts restricted convolution into multiplication of power series.
1. PERMUTATIONS, MINIMAL FACTORIZATIONS AND NONCROSSING PARTITIONS

1.1. We begin with well known facts about permutations. Let $\mathbb{N}^*$ be the set of positive integers, and $S_\infty$ be the group of permutations of $\mathbb{N}^*$ with finite support (the support of a permutation being the set of points which are not fixed by it). A cycle is a permutation which is transitive on its support, and its order is the cardinal of this support (in the sequel we shall consider only cycles of order $\geq 2$, so we will not consider the identical permutation $e$ as a cycle). For any cycle $\sigma$ of order $n$, let us put $|\sigma| = n - 1$ (and $|e| = 0$). The number $|\sigma|$ is the least number of transpositions needed to write $\sigma$ as a product of transpositions. For any permutation $\pi \in S_\infty$, let $\pi = c_1 \cdots c_r$ be a factorization of $\pi$ into a product of commuting cycles, such a factorization is unique up to order of the factors (indeed the support of each cycle in the factorization is one of the orbits of cardinal greater than 2 of $\pi$ and the cycle is equal to $\pi$ on this orbit), and $c_1, \ldots, c_r$ are called the cycles of $\pi$. The quantity $|\pi| = |c_1| + \cdots + |c_r|$ depends only on $\pi$, indeed $|\pi|$ is easily seen to be the least number of transpositions in a factorization of $\pi$ into a product of transpositions. Note also for future reference that one has $|\pi| + |\theta| = |\pi \theta|$ as soon as $\pi$ and $\theta$ have disjoint supports.

1.2. Let us consider the (unoriented) Cayley graph $\mathcal{G}$ whose set of vertices is $S_\infty$, and whose edges are the pairs $(\pi, \theta)$ such that $\pi \theta = 1$ (or equivalently $\pi^{-1} \theta$) is a transposition. The group $S_\infty$ acts on $\mathcal{G}$ by right and left translations, which are graph automorphisms. This graph is connected, and a path of minimal length between two points of this graph is called a geodesic. The geodesic distance between two points, denoted by $d$, is the length of a geodesic between these points. It is easy to see that for any $\pi, \theta \in S_\infty$, one has $d(\pi, \theta) = |\pi \theta^{-1}| = |\theta^{-1} \pi| = |\pi^{-1} \theta| = |\theta^{-1}|$, and this defines a right and left invariant distance on $S_\infty$.

For any permutation $\pi \in S_\infty$, and any factorization $\pi = \xi_1 \cdots \xi_j$ into a product of cycles, one has, by the triangle inequality, $|\pi| \leq |\xi_1| + \cdots + |\xi_j|$. Again, we call such a factorization minimal if there is equality.

For any pair $(\pi, \theta)$ of vertices of $\mathcal{G}$ let $[\pi, \theta]$ be the set of all points which lie on some geodesic from $\pi$ to $\theta$. Thus $\rho \in [\pi, \theta]$ if and only if one has $d(\pi, \rho) + d(\rho, \theta) = d(\pi, \theta)$. This set can be ordered by declaring that $\chi \leq \rho$ if and only if there is a geodesic from $\pi$ to $\rho$ passing through $\chi$, or equivalently, if there is a geodesic from $\chi$ to $\theta$ passing through $\rho$. For this order, $\pi$ is the smallest element and $\theta$ is the largest of $[\pi, \theta]$. It follows also that $[\theta, \pi] = [\pi^{-1}, \pi]$. For any pair of vertices $(\pi, \theta)$ of $\mathcal{G}$ one has a natural isomorphism of posets $[\pi, \theta] \sim [\pi \theta^{-1}, e]$. 
One has the following elementary lemma, whose proof is left to the reader.

**Lemma 1.** Let $\theta$ be a permutation and $\tau$ a transposition, then $|\theta \tau| = |\theta| - 1$ if and only if the two elements exchanged by $\tau$ are in the same orbit of $\theta$. Moreover, in this case the partition induced by the orbits of $\theta \tau$ is finer than that induced by the orbits of $\theta$.

From this it is easy to deduce that for any element $\tau \in [\pi, e]$ the partition induced by the orbits of $\tau$ is finer than that induced by the orbits of $\pi$. In particular, the support of any element of $[\pi, e]$ is included in that of $\pi$, and thus, $[\pi, e]$ is a finite set.

**Lemma 2.** Let $\pi = \chi_1 \cdots \chi_r$ be a minimal decomposition of $\pi \in S_n$, then for every $j = 1, \ldots, r$ the support of the cycle $\chi_j$ is included in some orbit of $\pi$.

**Proof.** By the remark just above, the support of $\chi_1$ is contained in some orbit of $\pi$. This implies that every orbit of $\chi_1^{-1} \pi$ must be contained in some orbit of $\pi$. The claim now follows by induction on the number $r$, since $\chi_1^{-1} \pi = \chi_2 \cdots \chi_r$, is a minimal decomposition of $\chi_1^{-1} \pi$.

**Lemma 3.** If $c_1, \ldots, c_r$ are the cycles of a permutation $\pi$, there is an isomorphism of posets $[\pi, e] \sim \prod_{j=1}^r [c_j, e]$.

**Proof.** Let $\chi \in [\pi, e]$, and let $\sigma$ be a cycle of $\chi$, then by Lemma 2, its support is included in some orbit of $\pi$. Let now $c_j$ be a non-trivial cycle of $\pi$, and let $c_j'$ be the product of the cycles of $\chi$ whose support lie in the support of $c_j$. By the triangular inequality we have $|c_j| \leq |c_j'| + |(c_j')^{-1} c_j|$. On the other hand $|\chi| = \sum_{j=1}^r |c_j|$ by hypothesis, and $|\chi^{-1} \pi| = \sum_{j=1}^r |(c_j')^{-1} c_j|$ since the permutations $(c_j')^{-1} c_j$ have disjoint support, also $|\chi| + |\chi^{-1} \pi| = |\pi|$ since $\chi \in [\pi, e]$, so that $|c_j| = |(c_j')^{-1}| + |(c_j')^{-1} c_j|$, and $c_j' \in [c_j', e']$ for all $j$. We leave the reader to verify that the map $\chi \mapsto (c_1', \ldots, c_r')$ is an isomorphism of posets between $[\pi, e]$ and $\prod_{j=1}^r [c_j, e]$.

1.3. We now review some results on noncrossing partitions and show the connection with the material above.

A partition of the set $\{1, 2, \ldots, n\}$ is called crossing if there exists $i < j < k < l \in \{1, 2, \ldots, n\}$ such that $i \sim k, j \sim l$, but one does not have $i \sim j$ (where $\sim$ is the equivalence relation defined by the partition). A partition which is not crossing is called noncrossing.

The notion of a noncrossing partition has been introduced and studied by Kreweras [K]. Some further investigations have been made by Poupart, Edelman, Simion and Ullman (see [P, E1, E2, S-U]). Recently, some connections with the theory of free convolution introduced by Voiculescu (see [D-N-V]), have been discovered by Speicher [S1].
The set of all noncrossing partitions of \( \{1, 2, \ldots, n\} \), denoted by \( \text{NC}(n) \), can be ordered by refinement of partitions; namely one has \( p \leq q \) for \( p, q \in \text{NC}(n) \) if \( q \) is a finer partition than \( p \). The set \( \text{NC}(n) \) becomes a lattice for this order [K]. For any pair \( (p, q) \) in \( \text{NC}(n) \), with \( p \leq q \), the interval \([p, q]\) is the set of elements \( r \) of \( \text{NC}(n) \) which satisfy \( p \leq r \leq q \). One has \( \text{NC}(n) = [0_n, 1_n] \), where \( 0_n \) is the partition with one class and \( 1_n \) is the partition with \( n \) classes.

**Lemma 4.** Every interval \([p, q]\) in \( \text{NC}(n) \) is isomorphic, as a poset, to some product \( [p, q] \sim \{[0_2, 1_2]^{k_2} \times \cdots \times [0_n, 1_n]^{k_n}\} \), where the sequence of numbers \( k_2, k_3, \ldots \) is uniquely determined by \( p \) and \( q \).

This result is in [S2, Proposition 1, Section 3]; see also [N-S, Section 1.3].

In [Bi, Theorem 1], using Lemma 1, we proved that \( \text{NC}(n) \) is isomorphic, as a poset, to \([\sigma_n, e]\) (see also [Be, Du] for related results). Indeed, the isomorphism is given by the trace map, called \( t \) and defined as follows. Each element \( \pi \in [\sigma_n, e] \) has its support in \( \{1, 2, \ldots, n\} \), so its orbits determine a partition of \( \{1, 2, \ldots, n\} \), which turns out to be non-crossing and which we call \( t(\pi) \). The map \( t \) is an isomorphism of posets [Bi, Theorem 1], its inverse is given by the following prescription; Given a noncrossing partition \( p \) of \( \{1, 2, \ldots, n\} \), the permutation \( t^{-1}(p) \) satisfies \( t^{-1}(p)(j) = \sigma_p^{-1}(j) \), where \( \pi(j, p) \) is the first exponent \( k \geq 1 \) such that \( \sigma_p^k(j) \) is in the same class of the partition \( p \) as \( j \). It follows that for any \( p, q \in \text{NC}(n) \), the map \( t \) is an isomorphism between the posets \([t^{-1}(p), t^{-1}(q)] ) \) and \([p, q] \). Speicher’s factorization of Lemma 4, and the factorization of Lemma 3 coincide through the map \( t \) (this follows from the uniqueness of this factorization, but it can also be verified directly from the constructions), so we see that the numbers \( k_2, k_3, \ldots \) verifying \([p, q] \sim \{[0_2, 1_2]^{k_2} \times \cdots \times [0_n, 1_n]^{k_n}\} \) in Lemma 4 are just the numbers of cycles of given order of the permutation \( t^{-1}(p)(t^{-1}(q))^{-1} \) (i.e., \( k_j \) is the number of cycles of order \( j \)).

1.4. Let \((a_1, \ldots, a_r)\) be a class, the type of this class is of course given by \( k_2, \ldots, k_n \), where \( k_j \) is the number of \( j \)'s in the sequence \((a_1, \ldots, a_r)\).

**Proposition 1.** The number of minimal factorizations of class \((a_1, \ldots, a_n)\) of a permutation depends only on the type of the factorizations.

Proof. We consider the group algebra of the symmetric group on \( n \) objects \( S_n \). For any conjugacy class \( C \) in \( S_n \), let \( H_C \) the sum of the elements of \( C \) in this algebra, and let \( C_k \) be the conjugacy class of cycles of length \( k \). The number of minimal factorizations of class \((a_1, \ldots, a_n)\) of some permutation in \( C \) is equal to the coefficient of \( H_C \) in the decomposition of \( H_{C_2} \cdots H_{C_k} \) into a linear combination of the \( H_{C_k} \). Since the elements \( H_C \) all commute in the group-algebra of \( S_n \), we get the result.
We have the straightforward

**Corollary 4.** The number of minimal factorizations of type $k$ of some permutation $\pi$ is equal to $(r(k)!/k!)$ (the number of minimal factorizations of $\pi$ of class $(a_1, \ldots, a_r)$), where $(a_1, \ldots, a_r)$ is any class corresponding to the type $k$.

We shall now sketch how to define an action of the permutation group of $r$ objects on the set of minimal factorizations of a given type $k$, with $r(k)=r$, such that the image of a factorization of class $(a_1, \ldots, a_r)$ under a permutation $\delta$ of $\{1, \ldots, r\}$ is a factorization of class $(a_{\delta(1)}, \ldots, a_{\delta(r)})$, and the factorization is unchanged by $\delta$ if $(a_1, \ldots, a_r) = (a_{\delta(1)}, \ldots, a_{\delta(r)})$. This will give a bijective proof of Proposition 1.

First we need the elementary

**Lemma 5.** Let $\sigma$ be a cycle of order $n$, $\pi$ be an element in the support of $\sigma$, and $2 \leq l \leq n-1$, then there is a unique minimal factorization $\sigma = \chi \rho$ such that $|\chi|=l$, and $\pi$ belongs to the supports of $\chi$ and $\rho$ (this implies that $|\rho|=n-l-1$, and $\pi$ is the only element common to these supports).

*Proof.* We can assume that $\sigma = (12\ldots n)$ and $\pi = 1$, then it is easy to see that necessarily $\rho = (12\ldots(n-l))$ and $\chi = ((n-l+1)(n-l+2)\ldots n)$.

We now construct the action of the permutation group of $\{1, \ldots, r\}$ by its Coxeter generators. The image of a factorization $\pi = \chi_1 \cdots \chi_r$ by the transposition $\tau_i = (i, i+1)$ will be as follows: If $\chi_i$ and $\chi_{i+1}$ have the same order, then the factorization is unchanged. Suppose that $\chi_i$ and $\chi_{i+1}$ have different orders $a_i$ and $a_{i+1}$ then, since $|\chi_i| + |\chi_{i+1}| = |\chi_i \chi_{i+1}|$, using Lemma 2 we see that their supports have at most one point in common. If they have no point in common, $\chi_i$ and $\chi_{i+1}$ commute and the image is obtained by replacing $\chi_i \chi_{i+1}$ by $\chi_{i+1} \chi_i$. If they do not commute, their product is a cycle, and we apply Lemma 5 to replace the product $\chi_i \chi_{i+1}$ by $\zeta_i \zeta_{i+1}$ where the cycles $\zeta_i$ and $\zeta_{i+1}$ have orders $a_{i+1}$ and $a_i$, respectively, and they have the same common element in their supports as $\chi_i$ and $\chi_{i+1}$.

In order to verify that this action of the $\tau_i$'s can be extended to an action of the permutation group on $r$ objects, we just need to check the Coxeter relations, namely $\tau_i^2 = id$, $\tau_i \tau_j = \tau_j \tau_i$ if $|i-j| \geq 2$, and $(\tau_i \tau_{i+1})^3 = id$. The first two relations are trivial. The third can be verified by tedious but straightforward case by case inspection. So it remains only to prove that a factorization of class $(a_1, \ldots, a_r)$ is fixed by a permutation $\delta$ such that $(a_{\delta(1)}, \ldots, a_{\delta(r)}) = (a_1, \ldots, a_r)$. Again, considering Coxeter generators, it is enough to prove that for any $i \leq r$, if $j$ is the smallest number $>i$ such that $a_j = a_i$ (if this number exists), the transposition $(ij)$ leaves any factorization of class $(a_1, \ldots, a_r)$ invariant. Let us call $\phi$ such a factorization. One has $(ij) = \tau_{i+1} \tau_i \cdots \tau_{j-2} \tau_{j-1} \tau_{j-2} \cdots \tau_i$. Furthermore, the factorization
\( \tau_{j-2} \cdots \tau_{1}(\phi) \) is of type \((b_1, \ldots, b_j)\), with \( b_j = b_{j-1} \); hence, it is unchanged by \( \tau_{j-1} \). It follows that \( \tau_{i+1} \cdots \tau_{j-2} \tau_{j-1} \tau_{j-2} \cdots \tau_{1}(\phi) = \tau_1 \tau_{i+1} \cdots \tau_{j-2} \tau_{j-1} \tau_{j-2} \cdots \tau_{1}(\phi) = \phi \).

In the next section we shall give a direct proof of these results when \( \pi \) is a cycle, by computing explicitly the number of factorizations of a given class.

2. PROOF OF THEOREM 1

Let \( E \) be a finite set with \( n \) elements, and \( \sigma \) a circular permutation of \( E \). For any sequence \((a_1, \ldots, a_r)\) of integers, all \( \geq 2 \), such that \( n = 1 + \sum_{i=1}^{r} (a_i - 1) \), denote by \( \Phi(a_1, \ldots, a_r) \) the set of all minimal factorizations of type \((a_1, \ldots, a_r)\) of \( \sigma \). It is clear that \( \Phi(n) \) has only one element. We shall define a bijection between the sets \( \Phi(a_1, \ldots, a_r) \) and \( E \times \Phi(a_1, \ldots, a_{r-2}, a_{r-1} + a_r - 1) \). By induction we will thus have an explicit bijection between \( \Phi(a_1, \ldots, a_r) \) and \( E^{-1} \times \Phi(n) \), which will finish the proof of Theorem 1.

Let \( \sigma = \chi_1 \cdots \chi_r \) be a minimal factorization of \( \sigma \), of class \((a_1, \ldots, a_r)\), then by 1.3, \( \chi_j \) is the trace of \( \sigma \) on its support, hence each cycle of \( \sigma \chi_j^{-1} \) contains a unique element in the support of \( \chi_j \). Since the factorization \( \sigma \chi_j^{-1} = \chi_1 \cdots \chi_{j-1} \) is minimal, by Lemma 2 the support of \( \chi_{j-1} \) is included in the support of some cycle \( \rho \) of \( \sigma \chi_j^{-1} \). Let \( \alpha \) be the unique element of the support of \( \chi_j \) which is in the support of \( \rho \), and let \( k \) be the smallest non-negative integer such that \( \rho^{-k}(\alpha) \) belongs to the support of \( \chi_{j-1} \). Since \( \rho \) commutes with \( \sigma \chi_j^{-1} = \chi_1 \cdots \chi_{j-1} \), one has \( \sigma = (\rho^k \chi_1 \rho^{-k}) (\rho^k \chi_2 \rho^{-k}) \cdots (\rho^k \chi_{j-1} \rho^{-k}) \chi_j \), and this is a factorization of class \((a_1, \ldots, a_r)\). The two cycles \( \rho^k \chi_{j-1} \rho^{-k} \) and \( \chi_j \) have a unique point in common in their supports, which is \( \alpha \), hence their product \( \zeta \) is a cycle of order \( a_{j-1} + a_r - 1 \), so that, putting \( \epsilon_j = \rho^k \chi_j \rho^{-k} \), one sees that \( \sigma = \epsilon_1 \cdots \epsilon_{j-1} \zeta \) is a minimal factorization of class \((a_1, \ldots, a_r)\), to the pair formed of the point \( \beta = \chi_{j-1} \rho^{-k}(\alpha) \in E \) and the factorization \( \sigma = \epsilon_1 \cdots \epsilon_{j-1} \zeta \).

Here is an explicit example. Let \( \sigma = (123456789) \), and consider the minimal factorization \( \sigma = (547)(19)(56)(12378) \), of class \((3, 2, 2, 5)\), thus \( \chi_1 = (457), \chi_2 = (19), \chi_3 = (56), \) and \( \chi_4 = (12378) \). One has \( \sigma \chi_4^{-1} = (19)(4567) \), thus \( \rho = (4567) \) contains the support of \( \chi_3 = (56) \), the element \( \alpha = 7 \) is the unique common point in the supports of \( \chi_4 \) and \( \rho \); furthermore \( \rho^{-1}(\alpha) = 6 \) belongs to the support of \( \chi_5 \), so that \( k = 1 \) and \( \beta = \chi_4(\rho^{-1}(\alpha)) = 5 \). The image of the factorization is the pair formed by \( 5 \) and by the factorization \( \sigma = (456)(19)(12378) \). If we continue the process, at the next step we obtain \( \beta = 9 \), and then \( \beta = 4 \), so that the factorization corresponds to the triple \((5, 9, 4) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}^3 \).
In order to prove that the above map is a bijection we shall construct its inverse. So let \( \sigma = e_1 e_2 \cdots e_{a-2} e_a \) be a factorization of type \((a_1, \ldots, a_r)\), \(a_1 + \cdots + a_r = 1\), and \( \beta \in E \). Let \( k \) be the smallest nonnegative integer such that \( \gamma = \sigma^k(\beta) \) belongs to the support of \( \xi \). Let \( \alpha \) be the point \( \xi^{a_{r-1}}(\gamma) \). The cycle \( \xi \) is the product \( e_{r-1} \gamma \) of the cycles \( e_{r-1} = (\gamma \xi(\gamma) \cdots \xi_{a_{r-1}}^{-1}(\gamma) \xi) \) and \( \chi_r = (\xi(\gamma) \cdots \xi_{a_{r-1}}^{-1}(\gamma)) \), so that \( \sigma = e_1 \cdots e_{a-1} \gamma \) is a minimal factorization of type \((a_1, \ldots, a_r)\). Let \( \rho \) be the cycle of \( \sigma^{-1} \) which contains the support of \( e_{r-1} \). Putting \( \chi_j = \rho^{-j} e_j \beta^k \), we have a minimal factorization \( \sigma = \chi_1 \cdots \chi_r \), of type \((a_1, \ldots, a_r)\). Let \( \\$$ / \$$ \) be the cycle of \( \chi_j^{-1} \) which contains the support of \( e_{r-1} \). Putting \( \chi_j^{-1} = \rho^{-j} \chi_j \), we take this factorization as the image of the pair formed by \( \beta \in E \) and the factorization \( \sigma = e_1 \cdots e_{a-2} \xi \).

Let us take again the example, with the factorization \( \sigma = (456)(19)(123678) = e_1 e_2 \xi \) and \( \beta = 5 \). Then \( \gamma = 6 = \sigma(\beta) \) is in the support of \( \xi \), and \( \gamma(6) = 7 = \alpha \). One thus has \( e_1 = (67), \chi_4 = (12378), \) and \( \rho = (4567) \), and one recovers the original factorization \( \sigma = (456)(19)(56)12378) \).

We leave to the reader the task of verifying, in the general case, that the maps that we have just defined are inverses of each other.

### 3. CENTRAL MULTIPLICATIVE FUNCTIONS ON \( S_\infty \)

#### 3.1. We shall consider functions defined on \( S_\infty \), with values in some commutative complex algebra \( K \), with a unit. Such a function will be called central if it is constant on conjugacy classes of \( S_\infty \). It will be called multiplicative if \( f(e) = 1 \) and, for all pairs of permutations \( (\pi, \theta) \) with disjoint supports, one has \( f(\pi \theta) = f(\pi)f(\theta) \). A central multiplicative function on \( S_\infty \) is completely determined by its values on the cycles \( e_n \), for \( n \geq 2 \). Indeed if \( \pi \) is any permutation with cycles \( e_1, \ldots, e_r \), of orders \( u_1, \ldots, u_r \), then \( f(\pi) = \prod_{j=1}^r f(e_u) \). For a multiplicative function \( f \) we shall define its characteristic series denoted by \( \varphi_j(z) \), as the formal power series in one indeterminate \( z \), with coefficients in \( K \),

\[
\varphi_j(z) = z + \sum_{j \geq 2} f(e_j)z^j
\]

Thus a multiplicative function and its characteristic series determine each other uniquely.

The usual convolution of functions on the group \( S_\infty \) is not well defined on central functions, since conjugacy classes in \( S_\infty \) are generally infinite, but one can define another binary operation on functions on \( S_\infty \), called restricted convolution and given by the formula

\[
f \star g(\pi) = \sum_{\rho, \pi, \rho' \in S_\infty} f(\rho') g(\rho) = \sum_{\pi \in S_\infty} f(\chi) \ g(\chi^{-1} \pi).
\]
Since the set $[\pi, e]$ is finite this operation is well defined.

**Lemma 6.** The restricted convolution of two central multiplicative functions is central and multiplicative.

**Proof.** The restricted convolution of two central functions is clearly central since the norm $|.|$ is conjugation invariant. The fact that restricted convolution of central multiplicative functions is again multiplicative follows from the second formula for $\star$ and the factorization of $[\pi, e]$ described in Lemma 3.

Characters of factor representations of the infinite symmetric group are examples of central multiplicative functions on $S\infty$ (see e.g. [K-V]), however we do not know whether the restricted convolution has a representation theoretic interpretation.

Given a central multiplicative function $f$ on $S\infty$, with characteristic series $\varphi_f$, let $\psi_f$ be the inverse, for composition of formal power series, of $\varphi_f$, and define the Fourier transform $\mathcal{F}$ of $f$ as the formal power series $\mathcal{F}(z) = (1/z) \psi_f(z)$. One can recover the characteristic series of $f$ from its Fourier transform, simply by inverting $z \mathcal{F}(z)$, so Fourier transform is a bijective map from central multiplicative functions to formal power series with coefficients in $\mathbb{R}$, with leading coefficient 1. We shall prove, as a consequence of Theorem 1, the following

**Theorem 2.** For any central multiplicative functions $f$ and $g$ on $S\infty$, one has

$$\mathcal{F} \star g = \mathcal{F} \mathcal{F}.$$ 

This shows that the Fourier transform converts restricted convolution into multiplication of power series. It also gives a practical way to perform such a convolution. 

We shall explain the relation of restricted convolution with the problem of computing the top connexion coefficients in the symmetric group. If $\pi$ is a partition of $n$, we denote by $l(\pi)$ the number of positive parts in $\pi$, and $m_i(\pi)$ the number of parts equal to $i$. Suppose that $x_j, j \geq 2,$ and $y_j, j \geq 2$ are indeterminates and consider the functions $f$ and $g$ on $S\infty$, with values in $\mathbb{C}[x_j; y_j; j \geq 2]$, given by the characteristic series $z^+ \sum_{j \geq 2} x_j z^j$ and $z^+ \sum_{j \geq 2} y_j z^j$, then the value of $f \star g$ on a permutation $\pi$, whose cycle structure is given by a partition $\gamma$ of $n$, is a polynomial in the $x_j$ and the $y_j$. For partitions $\alpha$ and $\beta$ of $n$, denote by $x^\alpha, y^\beta$ the monomials $\prod_{j \geq 2} x_j^{m(j)}$ and $\prod_{j \geq 2} y_j^{m(j)}$, then the coefficient of $x^\alpha y^\beta$ in $f \star g(\pi)$ is nonzero only if $l(\alpha) + l(\beta) = l(\gamma) + n$ and, in this case, is equal to the number of minimal factorizations of $\pi$ into a product $\pi_1 \pi_2$ of permutations with cycle structures given by $\alpha$ and $\beta$. This number is nothing else but the top connection
coefficient \([K_1, K_2, K_3]\) of the algebra of the symmetric group, in the notations of [G-J]. So the formula for restricted convolution on \(S_\infty\) gives a way of computing this top connection coefficient by extracting a coefficient in a generating series. A similar formula has been given in [G-J, Lemma 2.1], so our proof of Theorem 2 yields another approach to this result. Note that our approach is elementary and self-contained, in particular we do not use any properties of trees and such structures, although this may be thought as hidden behind the Lagrange inversion formula in Lemma 7 below.

3.2. Before we proceed to the proof of Theorem 2, we shall make the connection with the work of Nica and Speicher [N-S]. Recall the notations of part 1.3. Let \(\text{Int}_n\) be the set of all intervals in \(NC(n)\), and \(\text{Int}\) the disjoint union over all \(n \geq 2\) of the sets \(\text{Int}_n\). A complex function on \(\text{Int}\) is called multiplicative if for every \([p, q] \in NC(n)\) such that \([p, q] \sim [0_n, 1_n] \cdots [0_n, 1_n]^3\), one has \(f([p, q]) = \prod_{j=2} f([0_j, 1_j])^{k_j}\). A multiplicative function is completely determined by the values \(f([0_j, 1_j])\) for \(j \geq 2\) and, hence, by its characteristic series, denoted again by \(\varphi_f\), which is the formal power series in the indeterminate \(z\) given by the formula \(\varphi_f(z) = z + \sum_{j \geq 2} f([0_j, 1_j]) z^j\).

One can define a binary operation, called convolution on the set of functions on \(\text{Int}\), defined by the formula

\[
(f \star g)([p, q]) = \sum_{\{r \in [r, q]\}} f([p, r], [r, q]).
\]

Now, let \(f\) be a central multiplicative function on \(S_\infty\), one can define a function \(\tilde{f}\) on \(\text{Int}\) by \(\tilde{f}([p, q]) = f(t^{-1}(p)(t^{-1}(q))^{-1})\). Because of the coincidence of the decompositions in Lemmas 3 and 4, this function is multiplicative on \(\text{Int}\), with the same characteristic series as \(f\). Furthermore, if \(g\) is another central multiplicative function on \(S_\infty\), then using the second formula for restricted convolution, one sees that

\[
\tilde{f} \star \tilde{g} = \tilde{f} \star \tilde{g}.
\]

It follows that the restricted convolution of central multiplicative functions on \(S_\infty\) and the convolution of multiplicative functions on \(\text{Int}\) can be computed by the same procedure, in terms of their characteristic series. Having remarked this, Theorem 2 is nothing but a rephrasing of the main theorem of [N-S] using central multiplicative functions on \(S_\infty\) instead of multiplicative functions on \(\text{Int}\). So we will obtain a new proof of Theorem 1 in [N-S]. Although our proof may not be simpler than that of Nica and Speicher, its mainline is rather easy to grasp because of the geometric significance of the minimal factorizations, in terms of distances on the
Cayley graph of $S_n$. Also, it is interesting to note that multiplicative functions on noncrossing partitions correspond to very natural functions on the symmetric group. In this respect, it would be interesting to find an interpretation of the restricted convolution in terms of the representation theory of the symmetric group.

3.3. We shall now prove Theorem 2. We first need a preliminary lemma.

**Lemma 7.** Let $F = \sum_{j=2}^{\infty} x_j z^{j-1}$ and $G = z + \sum_{j=2}^{\infty} w_j z^j$ be formal power series in the variable $z$, with coefficients in some commutative complex algebra with unit $R$, which satisfy the equation

$$G(z) = ze^{F(G(z))},$$

then there exists sequences of polynomials with rational coefficients $P_2, P_3, \ldots, P_n, \ldots$ and $Q_2, Q_3, \ldots, Q_n, \ldots$ such that $P_j$ and $Q_j$ are polynomials in $j$ indeterminates (with $Q_2 = P_2 = 0$), and $x_j = w_j + P_j(w_2, \ldots, w_{j-1})$. Furthermore, one has

$$w_j = \sum_{k+j}^{j} f^{(k)} x^k \quad (\ast\ast)$$

(with the notation $x^k = \prod_{j \geq 2} x_j^{k_j}$).

**Proof.** We first prove the formula (\ast\ast). By Lagrange’s inversion formula for power series (see, e.g., [J]), if $G$ satisfies $G(z) = ze^{F(G(z))}$, the coefficient of $z^j$ in $G$ is equal to $(1/j)$ (the coefficient of $z^{j-1}$ in the expansion of $e^{F(z)}$). We deduce (\ast\ast) from this. The existence of the polynomials $Q_j$ follows easily from inspection of (\ast\ast), and the existence of the $P_j$’s now follows from the existence of $Q_j$’s and an induction argument.

For $k \in K$ let $\gamma(\pi, k)$ be the set of minimal factorizations of $\pi$ of type $k$, and let $v(\pi, k)$ be the cardinal of $\gamma(\pi, k)$. If $\sigma$ is a cycle of length $n(k)$, we put $v(\sigma, k) = v(k)$. We have $v(\pi, k) = 0$ if $|\pi| \neq n(k) - 1$.

For any class $a = (a_1, \ldots, a_r)$ and $\pi \in S_n$, we let $\mu(\pi, a)$ be the number of minimal factorizations of class $a$ of $\pi$. From Corollary 4 we see that $v(\pi, k) = (r(k)!)! / k! \mu(\pi, a)$ if $a$ is any class of type $k$.

Let $g_\pi$ be the function on $S_n$, with values in $\mathbb{C}[x_2, x_3, \ldots]$, the polynomial algebra on infinitely many indeterminates $x_2, x_3, \ldots$, given by

$$g_\pi(\pi) = \sum_{k \in K} v(\pi, k) \frac{x^k}{k!}$$
Since \( (\xi^j, k) = 0 \) if \( n(k) \leq |\pi| \), there is only a finite number of terms in this sum.

**Lemma 8.** The function \( \mathcal{G}_e \) is central and multiplicative on \( S_\infty \).

**Proof.** That \( \mathcal{G}_e \) is central is obvious, so let us prove that it is multiplicative. Let \( \pi \in S_\infty \) be a permutation with cycles \( c_1, \ldots, c_r \). Let \( \pi = \xi_1 \cdots \xi_f \) be a minimal decomposition of \( \pi \), (so that \( |\pi| = |\xi_1| + \cdots + |\xi_f| \)). Applying Lemma 2, let, for \( j = 1, \ldots, r \), \( (\xi^j, k) \in \pi \) be the cycles whose support is contained in that of \( c_j \), ordered according to their order in the sequence \( \xi_1, \ldots, \xi_f \). Since cycles with disjoint support commute, one has \( \xi^{j,1}_1 \cdots \xi^{j,k} = c_j \), for all \( j \). One has \( |\xi_1| + \cdots + |\xi_f| = |c_1| + \cdots + |c_r| = |\pi| \), and \( |\xi^{j,1}_1 + \cdots + |\xi^{j,k}| \geq |c_j| \) so that there is equality for every \( j \). This implies that \( \xi^{j,1}_1 \cdots \xi^{j,k} = c_j \) is a minimal factorization of \( c_j \). To every minimal factorization of \( \pi \) we can thus associate a \( r \)-tuple of minimal factorizations of \( c_1 \cdots c_r \), thus we have a map from \( \gamma(\pi, k) \) to \( \bigcup \mathcal{K}^{r} = (\bigcup \mathcal{K})^r \). This map is not one to one; indeed, let \( (c^j, \mu) \in \bigcup \mathcal{K}^{r} = (\bigcup \mathcal{K})^r \) with \( k^1 + \cdots + k^r = k \), then, since cycles with disjoint supports commute, any total ordering \( \xi_1, \ldots, \xi_f \) of the cycles \( \xi^{j,1}_1 \cdots \xi^{j,k} \) compatible with the order on the second component \( s \), will give a minimal decomposition of \( \pi \). It follows that there are exactly \( r! \) ways of obtaining a minimal decomposition from the \( r \)-tuple \( (c^1 = \xi^{j,1}_1 \cdots \xi^{j,k}, \ldots, c^r) \). We deduce that

\[
v(\pi, k) = \sum_{k^1 + \cdots + k^r = k} \prod_{j=1}^{r} v(c_j, k^j) \frac{r!}{r(k^j)! \cdots r(k^r)!}.
\]

We can now prove Lemma 8. Let \( \pi \in S_\infty \), with cycles \( c_1, \ldots, c_r \), then

\[
\mathcal{G}_e(\pi) = \sum_{k \in \mathcal{K}} v(\pi, k) \frac{x^k}{r(k)!} = \sum_{k \in \mathcal{K}} \sum_{k^1 + \cdots + k^r = k} \prod_{j=1}^{r} v(c_j, k^j) \frac{r!}{r(k^j)! \cdots r(k^r)!} \frac{x^{k^1 + \cdots + k^r}}{r(k)!}.
\]

This proves that \( \mathcal{G}_e \) is multiplicative.
The characteristic series of \( G_x \) is

\[
G_x(z) = z + \sum_{j=2}^{\infty} \sum_{n, k \in K : j} v(k) \frac{x^k}{r(k)!} z^j.
\]

From Corollary 3 we infer that

\[
G_x(z) = z + \sum_{j=2}^{\infty} \sum_{n, k \in K : j} j^{r(k)} x^k \frac{z^j}{k!}.
\]

From Lemma 7 we deduce that \( G_x \) satisfies the equation

\[
G_x(z) = ze^{F_x(G_x(z))},
\]

where \( F(z) = \sum_{j=2}^{\infty} x_j z^{j-1} \).

Let now \( y_2, y_3, \ldots, y_n, \ldots \) be another set of indeterminates, and let \( G_{y} \) (respectively \( G_{y+x} \)) be the function obtained by substituting \( y_2, y_3, \ldots \) (respectively \( x_2, x_3, y_2, x_3, y_3, \ldots \)) for \( x_2, x_3, \ldots \) into the definition of \( G_y \).

Lemma 9. \( G_x \star G_y : G_{x+y} \).

Proof. Let \( k, k', k'' \in K \) such that \( k = k' + k'' \), \( r(k) = l, r(k') = m \), and \( a = (a_1, \ldots, a_l) \) be a class of type \( k \), such that \( a^m \equiv (a_1, \ldots, a_m) \) is of type \( k' \) (and hence \( a^{lm} \equiv (a_{m+1}', \ldots, a_l') \) is of type \( k'' \)). Clearly if \( \pi = \zeta_1 \cdots \zeta_l \) is a minimal factorization of class \((a_1, \ldots, a_l)\) then \( \theta = \zeta_1 \cdots \zeta_m \) is a minimal factorization of class \((a_1, \ldots, a_m)\), and \( \theta^{-1} \pi = \zeta_{m+1} \cdots \zeta_l \) is a minimal factorization of class \((a_{m+1}', \ldots, a_l')\). Conversely, if \( \theta = \zeta_1 \cdots \zeta_m \) is a minimal factorization of class \((a_1, \ldots, a_m)\), and \( \theta^{-1} \pi = \zeta_{m+1} \cdots \zeta_l \) is a minimal factorization of class \((a_{m+1}', \ldots, a_l')\), then \( \pi = \zeta_1 \cdots \zeta_l \) is a minimal factorization of type \((a_1', \ldots, a_l')\). It follows that \( \mu(\pi, a) = \sum_{\theta \in \{\pi, \varepsilon\}} \mu(\theta, a^m) \mu(\theta^{-1}, a^{lm}) \).

Using Corollary 4, we thus see that

\[
v(\pi, k) \frac{k!}{r(k)!} = \sum_{\theta \in \{\pi, \varepsilon\}} v(\theta, k') \frac{k'!}{r(k')!} v(\theta, k'') \frac{k''!}{r(k'')!} \quad (**)
\]

We can now compute

\[
G_{x+y}(\pi) = \sum_{k \in K} v(\pi, k) \frac{(x+y)^k}{r(k)!} = \sum_{k \in K} \sum_{k', k'' \in K : k + k' = k} v(\pi, k) \frac{x^k y^{k'} k!}{r(k)! k'! k''!}
\]
This proves Lemma 9.

The end of the Proof of Theorem 2. Let \( v_j, j \geq 2 \) and \( w_j, j \geq 2 \) be indeterminates, and consider the central multiplicative functions \( f \) and \( g \) on \( S_n \), with values in \( C[v_j, w_j; j \geq 2] \) with characteristic series \( z + \sum_{j=2}^n v^j z^j \) and \( z + \sum_{j=2}^n w^j z^j \). Let \( x_j = v_j + P_{v_j}(v_2, \ldots, v_{j-1}) \), and \( y_j = w_j + P_{w_j}(w_2, \ldots, w_{j-1}) \), and let \( F_x \) be the power series \( F_x(z) = \sum_{j=2}^n x_j z^{j-1} \). By Lemma 7, we see that \( f = g_x \) and \( g = g_y \). By Lemma 7 again, we have \( \varphi_f(z) e^{-F_x(z)} = z \); this implies that \( e^{-F_x} \) is the Fourier transform of \( f \) and, also, \( e^{-F_x} \) is the Fourier transform of \( g \). By Lemma 9, one sees that the Fourier transform of \( f \star g = g_y \) is equal to the Fourier transform of \( g_x \), which is \( e^{-F_{x+y}} = e^{-F_x-F_y} \); hence we have \( \varphi_f \star \varphi_g = \varphi_{f \star g} \). This proves the result for the functions \( f \) and \( g \). The proof for any functions with values in some complex commutative algebra with unit follows by substitution in \( C[v_j, w_j; j \geq 2] \). This finishes the proof of Theorem 2.

ACKNOWLEDGMENTS

I thank the referee for pointing out Ref. [G-J] and for making useful comments on the presentation of this paper. The author acknowledges partial support from the Human Capital and Mobility programme, Contract Number ERBCHRXCT93094.

REFERENCES


