On the number of indecomposable permutations with a given number of cycles

Robert Cori [*]

LaBRI, Université Bordeaux 1, F33405 Talence Cedex, France

robert.cori@labri.fr

Claire Mathieu [†]

Department of Computer Science, Brown University, Providence RI 02912, USA

claire@cs.brown.edu

John Michael Robson

LaBRI, Université Bordeaux 1, F33405 Talence Cedex, France

mike.robson@labri.fr

Submitted: May 17, 2011; Accepted: Feb 5, 2012; Published: Feb 29, 2012
Mathematics Subject Classification: 05A05

In memory of Philippe Flajolet

Abstract

Abstract. A permutation $a_1 a_2 \ldots a_n$ is *indecomposable* if there does not exist $p < n$ such that $a_1 a_2 \ldots a_p$ is a permutation of $\{1, 2, \ldots, p\}$. We consider the probability that a permutation of $\mathbb{S}_n$ with m cycles is indecomposable and prove that this probability is monotone non-increasing in n.

We compute also the asymptotic probability when n goes to infinity with m/n tending to a fixed ratio. The asymptotic probability is monotone in m/n, and there is no threshold phenomenon: it degrades gracefully from 1 to 0. When $n = 2m$, a slight majority (51.117... percent) of the permutations are indecomposable.

1 Introduction.

A permutation $a_1 a_2 \ldots a_n$ is called *decomposable* if there exists $p < n$ such that $a_1 a_2 \ldots a_p$ is a permutation of $\{1, 2, \ldots, p\}$, and is called *indecomposable* otherwise.

[*]The first author acknowledges the support of ERC under the agreement "ERC StG 208471 - ExploreMap" and that of ANR Magnum.

[†]The second author acknowledges the support of the NSF grant AF-0964037.

Let $\mathbb{S}_n$ denote the set of permutations of $\{1, 2, \ldots, n\}$. In [Com72], Comtet proved that almost all permutations of $\mathbb{S}_n$ are indecomposable, more precisely:

$$\Pr_{\mathbb{S}_n}\{\alpha \text{ indecomposable}\} = 1 - \frac{2}{n} + O(\frac{1}{n^2}).$$

Indecomposable permutations are also called connected or irreducible permutations, they have been considered by many authors.

Marshall Hall [Hal49] was probably the first to implicitly consider them while enumerating subgroups of finite index of the free group with 2 generators. They were studied in more detail about 20 years later by A. Lentin[Len72] and L. Comtet [Com72] and are quoted as examples or exercises in many classical books in Combinatorics and Algorithms (see for instance [Com74, FS09, GS95, GJ83, Knu05, Odl95, Sta99]).

More recently, a bijection between them and hypermaps (or equivalently bicolored maps) was given by P. Ossona de Mendez and P. Rosenstiehl in [dMR04]. This bijection is such that the number of cycles of the permutation is equal to the number of vertices of the hypermap (equivalently the number of vertices of a given color of the bicolored map). Hence in order to generate at random a hypermap with a fixed number m of vertices, a natural algorithm consists of generating permutations with m cycles until obtaining an indecomposable one, then building the hypermap in bijection with it. The efficiency of this algorithm depends on the value of the probability that a permutation with m cycles is indecomposable.

The event that α is decomposable depends heavily on the number of cycles of α. The permutation with n cycles (the identity) is decomposable, and among the $\binom{n}{2}$ permutations with $n-1$ cycles (the transpositions), all but one are decomposable. At the other extreme, a permutation with only one cycle is never decomposable. Intuitively, it seems clear that a permutation with more cycles is more likely to be decomposable. In this note

- we prove that in $\mathbb{S}_n$ the probability for a permutation with m cycles to be indecomposable is greater than for one with $m+1$ cycles to be indecomposable;
- for any $\mu \in (0, 1]$, we calculate the asymptotic probability that a permutation over $\{1, \ldots, n\}$ with approximately μn cycles is decomposable.
- Since the probability tends to 0 when μ tends to 1 and tends to 1 when μ tends to 0, one might expect that it could be 1/2 when $\mu = \frac{1}{2}$, surprisingly this is not exactly the case since our result shows that the asymptotic value is $0.511699676\ldots$

Let $\mathbb{S}_{n,m}$ denote the set of permutations of $\mathbb{S}_n$ with m cycles, then its number of elements $s_{n,m}$ is the unsigned Stirling number of the first kind. Let $c_{n,m}$ denote the number of indecomposable permutations of $\mathbb{S}_{n,m}$ and $p_{n,m} = \frac{c_{n,m}}{s_{n,m}}$.

A *left-to-right maximum* of a permutation $\alpha = a_1 \ldots a_n$ is an a_j such that for any $i < j$ one has $a_j > a_i$. A classical result states that the number of permutations of $\mathbb{S}_n$ with m cycles is equal to the number of those with m left-to-right maxima. Moreover the so called

First Fundamental Transform (see [Lot83] chap. 10) is a bijection between permutations of $\mathbb{S}_n$ which maps a permutation with m cycles to a permutation with m left-to right maxima. It is not difficult to prove (see [Cor09] Proposition 1) that the permutation is indecomposable if and only if its image under this transformation is indecomposable. Hence the probabilities obtained above are also those for a permutation with m left-to-right maxima to be indecomposable.

2 Decreasing fraction of decomposable permutations of $\mathbb{S}_{n,m}$.

In this section we prove that for a given n the numbers $p_{n,m}$ decrease when m increases. The proof uses inversion sequences; these are introduced here since there exists a bijection beteween the inversion sequences of length n and permutations in $\mathbb{S}_n$, moreover the set of these sequences is a sublattice of the lattice of integer sequences of length n.

We then proceed by induction, the key point is that the lattice of the inversion sequences of length n may be simply built from n copies of the lattice of sequences of length $n-1$.

2.1 Permutations and inversion sequences

A classical construction associates to each permutation $\alpha = a_1, a_2, \ldots, a_n$ the sequence often called the inversion table, (see for instance [Knu73] section 5.1.1):

$$Inv(\alpha) = x_1, x_2, \ldots, x_n$$

such that x_i is the number of j satisfying: $j < i$ and $a_j > a_i$.

It is well known that Inv is a bijection from permutations in $\mathbb{S}_n$ to the set of sequences $x_1, x_2, \ldots, x_n$ of integers such that:

$$0 \leq x_i < i \quad \text{for all } i,\ 1 \leq i \leq n \tag{1}$$

moreover the number of occurrences of 0 in $Inv(\alpha)$ is equal to the number of left-to-right maxima of α.

For two sequences of the same lengths $x = x_1, x_2, \ldots, x_n$ and $y = y_1, y_2, \ldots, y_n$ we write $x \preceq y$ if $x_i \leq y_i$ for all $1 \leq i \leq n$ and for two permutations α and β we write $\alpha \preceq \beta$ if $Inv(\alpha) \preceq Inv(\beta)$. Notice that this order on the symmetric group is weaker than the Bruhat order $\preceq_B$, since $2,1,3 \preceq_B 2,3,1$ and $Inv(2,1,3) = 0,1,0;\ Inv(2,3,1) = 0,0,2$ so that the two permutations $2,1,3$ and $2,3,1$ are incomparable for $\preceq$. However we have the same kind of result (see [Ten07] corollary 4.3):

Lemma 1 *Let α and β be two permutations such that $\beta \preceq \alpha$. If α is decomposable then so is β.*

Proof: Remark that α is decomposable if and only if $Inv(\alpha) = x_1, x_2, \ldots, x_n$ has a suffix $x_{i+1}, \ldots, x_n$ (where $i > 0$) which is the inversion table of a permutation of $\mathbb{S}_{n-i}$. The result follows from the fact that diminishing the value of x_i keeps the existence of such a suffix. $\square$

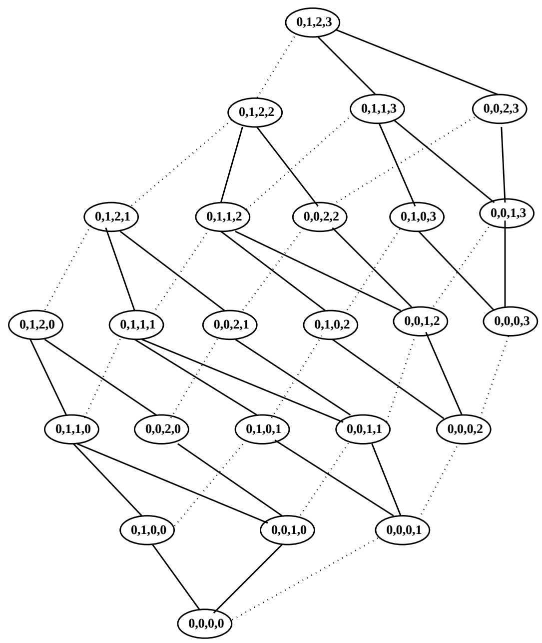

Figure 1: The Lattice of inversion sequences of length 4

2.2 On a bicoloring of the elements of the lattice

Generalizing the question of decomposability, we consider the following question on the lattice E_n of integer sequences of length n satisfying condition (1). Divide the lattice into n slices: the slice $E_{n,m}$ contains those sequences with exactly m elements equal to 0. The number of elements in slice m corresponds to the permutations of $\mathbb{S}_n$ having m left to right maxima, hence is equal to the Stirling number of the first kind $s_{n,m}$. Consider a coloring of the elements of $E_{n,m}$ in two colors, red and blue. We say that the coloring *respects the order* $\preceq$ if any predecessor of a blue vertex is also blue.

Lemma 2 *Given a bicoloring of the set E_n respecting the order $\preceq$, let r_m denote the number of red elements in slice m. Then:*

$$\frac{r_m}{s_{n,m}} \geq \frac{r_{m+1}}{s_{n,m+1}} \tag{2}$$

Proof: We proceed by induction on n. The case $n = 2$ is obvious since there are two slices with 1 element each. For the induction step, observe that the lattice E_n can be

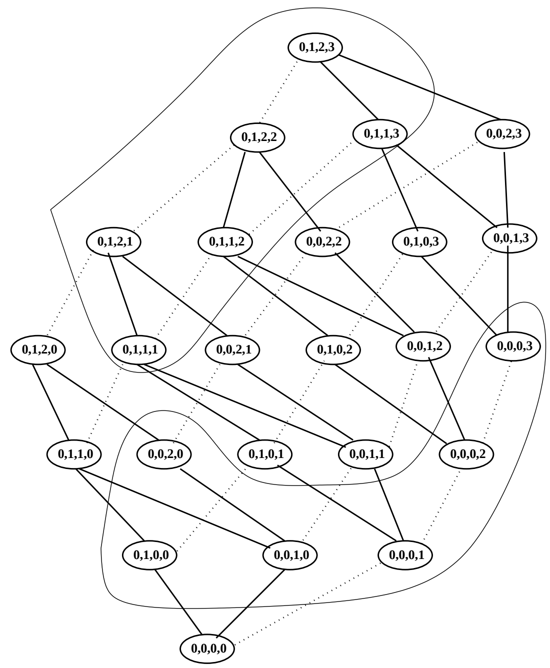

Figure 2: Divison of the lattice into 4 slices

divided in n subsets in a way different from that considered above. Indeed, E_n can be decomposed into the subsets E_n^i for $0 \leq i < n$, defined by:

$$E_n^i \quad = \quad \{(x_1, x_2, \ldots, x_n) \in E_n \mid x_n = i\}.$$

For this decomposition all the subsets have the same cardinality and each of the E_n^i is by deletion of the last coordinate isomorphic as a lattice to E_{n-1}; notice however that E_n^i for $i \geq 1$ and E_n^0 play different roles since the number of elements with m occurrences of 0 is equal to $s_{n-1,m}$ in E^i for $i \geq 1$ and to $s_{n-1,m-1}$ for E^0.

Each element $(x_1, x_2, \ldots, x_n)$ of E_n^i for $i < n-1$ is covered by exactly one element in E_n^{i+1}, namely, $(x_1, x_2, \ldots, x_n + 1)$.

Let us consider a bicoloring of the lattice E_n respecting the order $\preceq$ and let us compare the number of red elements in the two slices $E_{n,m}$ and $E_{n,m+1}$. These slices are divided into n subsets:

$$E_{n,m}^i \quad = \quad E_{n,m} \cap E_n^i$$

For each value of $i > 0$ we may consider that the coloring of E_n^i induces a bicoloring of E_{n-1} in which the subsets $E_{n,m}^i$ correspond to the slices $E_{n-1,m}$. Similarly the coloring of E_n^0 induces a coloring of E_{n-1} in which the slice $E_{n,m}^0$ corresponds to $E_{n-1,m-1}$. Hence we may apply the induction hypothesis for the bicoloring of the set E_{n-1} induced by that on E_n. For a subset S of E_n we denote by $\mathrm{r}(S)$ the number of red elements in S. Since the number of elements in $E^0_{n,m}$ is $s_{n-1,m-1}$, we have:

$$\frac{\mathrm{r}(E^0_{n,m})}{s_{n-1,m-1}} \quad \geq \quad \frac{\mathrm{r}(E^0_{n,m+1})}{s_{n-1,m}} \tag{3}$$

Similarly for each $i > 0$, since the number of elements of $E^i_{n,m}$ is $s_{n-1,m}$ we get:

$$\frac{\mathrm{r}(E^i_{n,m})}{s_{n-1,m}} \quad \geq \quad \frac{\mathrm{r}(E^i_{n,m+1})}{s_{n-1,m+1}} \tag{4}$$

The last set of inequalities (4) may be summed up since the denominators are equal, giving:

$$\frac{\mathrm{r}(\cup_{i>0}E^i_{n,m})}{s_{n-1,m}} \quad \geq \quad \frac{\mathrm{r}(\cup_{i>0}E^i_{n,m+1})}{s_{n-1,m+1}}. \tag{5}$$

Now, we turn to proving Equation (2). Let us denote $a_m = \mathrm{r}(E^0_{n,m})$, $b_m = \mathrm{r}(\cup_{i>0}E^i_{n,m})$, then $r_m = a_m + b_m$. We prove that $\Delta = r_m s_{n,m+1} - r_{m+1}s_{n,m} \geq 0$. Using inequalities (3) and (5) we have:

$$\begin{aligned}
\Delta &= (a_m + b_m)s_{n,m+1} - (a_{m+1} + b_{m+1})s_{n,m} \\
&\geq (a_{m+1}\frac{s_{n-1,m-1}}{s_{n-1,m}} + b_m)s_{n,m+1} - (a_{m+1} + \frac{s_{n-1,m+1}}{s_{n-1,m}}b_m)s_{n,m} \\
&= a_{m+1}(\frac{s_{n-1,m-1}}{s_{n-1,m}}s_{n,m+1} - s_{n,m}) + b_m(s_{n,m+1} - \frac{s_{n-1,m+1}}{s_{n-1,m}})
\end{aligned}$$

Applying the recurrence formula $s_{n,m+1} = s_{n-1,m} + (n-1)s_{n-1,m+1}$ and simplifying, yields:

$$\Delta \geq (b_m - (n-1)a_{m+1})(s_{n-1,m} - \frac{s_{n-1,m+1}s_{n-1,m-1}}{s_{n-1,m}}).$$

Notice that each element $x = (x_1, x_2, \ldots, x_{n-1}, 0)$ coloured red in $E^0_{n,m+1}$ is dominated by $y^i = (x_1, x_2, \ldots, x_{n-1}, i)$ in each of the $E^i_{n,m}$, and by Lemma 1 y^i is also of red color. Hence we have $\mathrm{r}(E^i_{n,m}) \geq \mathrm{r}(E_{n,m+1})$, and we get :

$$b_m \quad \geq \quad (n-1)a_{m+1}. \tag{6}$$

Recall the log-concavity of Stirling numbers:

$$s^2_{n-1,m} \geq s_{n-1,m-1}s_{n-1,m+1}.$$

This imples $\Delta \geq 0$. □

Theorem 1 *The numbers $c_{n,m}$ of indecomposable permutations of $\mathbb{S}_n$ having m cycles satisfy :*

$$\frac{c_{n,m}}{s_{n,m}} \quad \geq \quad \frac{c_{n,m+1}}{s_{n,m+1}}$$

Proof: The number $c_{n,m}$ counts also the number of indecomposable permutations of $\mathbb{S}_n$ with m left-to-right maxima. Consider the coloring of the lattice E_n of inversion sequences where red elements are those sequences $(x_1, \ldots, x_n)$ such that $(x_1, \ldots, x_n) = Inv(\alpha)$, for α indecomposable, and blue elements correspond to decomposable permutations. The result is a direct consequence of Lemma 2. $\square$

3 Asymptotic results

3.1 Proof overview

In this part, we state the main asymptotic result and the three lemmas which, together, imply the result.

Theorem 2 *Let μ be a positive real number less than 1. Let m and n be integers tending to infinity in such a way that the ratio m/n tends to μ. Then the probability $p_{n,m}$ that a permutation of $\mathbb{S}_{n,m}$ is indecomposable tends to $p(\mu)$ given by:*

$$p(\mu) = \left(\frac{u}{u+\mu}\right)^2, \tag{7}$$

where $u > 0$ is defined implicitly by the equation

$$\mu = \frac{u}{e^u - 1}. \tag{8}$$

Moreover, when $m/n = \mu$ then $|p_{n,m} - p(\mu)| = O(\log(n-m)/(n-m))$.

The proof of Theorem 2 follows directly from the following three lemmas. The first lemma states some simple facts and has a short proof.

Lemma 3 *If the following condition holds, then α is decomposable:*

$$(a_1 = 1) \quad \text{or} \quad (a_n = n) \tag{9}$$

If the following condition holds, then α is indecomposable:

$$(\exists i, i \leq a_1 \ \textit{and}\ a_i > a_n) \tag{10}$$

Proof: If condition (9) holds then either a_1 is a permutation of $\mathbb{S}_1$ or $a_1 \ldots a_{n-1}$ is a permutation of $\mathbb{S}_{n-1}$.

If α is decomposable then there exist $p < n$ such that $a_1 a_2 \ldots a_p$ is a permutation of $\mathbb{S}_p$, this implies $a_n > a_i$ for all $1 \leq i \leq p$. Moreover all i such that $p < i \leq n$ satisfy $i > a_1$ contradicting (10). Note that there is a simple way to represent indecomposability as a simple drawing: put n points on a horizontal segment numbered 1 to n from left to right draw a half circle from i to a_i when $a_i \neq i$ then the permutation is decomposable if and only if there is no vertical line intersecting the segment but not any of the half circles. As an example the proof of the above Lemma is illustrated on Figure 3. $\square$

The second Lemma will be proved in the next section using an evaluation of the asymptotics of Stirling numbers due to Moser and Wyman [MW58]

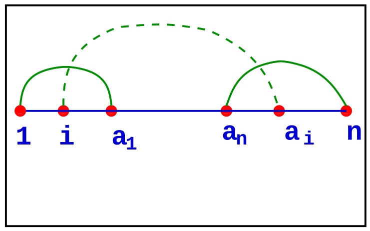

Figure 3: Illustration of Condition 10 guaranteeing indecomposability.

Lemma 4 *Let m, n, μ, u be defined as in Theorem 2. Let $A_{n,m}$ denote the event that a permutation of $\mathbb{S}_{n,m}$ satisfies condition (9). Then the probability of $A_{n,m}$ tends to*

$$\frac{2e^u - 1}{e^{2u}} = \frac{2u\mu + \mu^2}{(u+\mu)^2}.$$

The third lemma, is the main technical point in our paper and will be proved in the second part of the following section:

Lemma 5 *The probability that a permutation of $\mathbb{S}_{n,m}$ satisfies neither condition (9) nor condition (10) is $O(\frac{\log(n-m)}{n-m})$.*

Remark The solution of equation (8) can be expressed by the so called Lambert function W_{-1}. The Lambert function W is the inverse relation of the function $f(W) = We^W$. When $-\frac{1}{e} < x = f(W) < 0$ there are two branches for $W(x)$ classically denoted W_0 and W_{-1}. Equation (8) can be written:

$$-(u+\mu)e^{-(u+\mu)} \;=\; -\mu e^{-\mu}$$

Since for $0 < \mu < 1$ we have $-1/e < -\mu e^{-\mu} < 0$ there are two solutions to the above

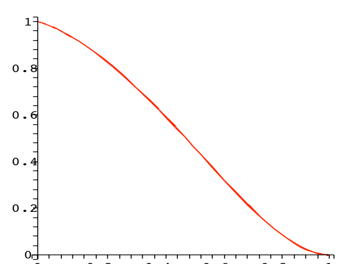

Figure 4: Asymptotic probability $p(\mu)$ that a permutation of $\mathbb{S}_n$ with $\lfloor \mu n \rfloor$ cycles is indecomposable, as a function of μ.

equation. The first one is $-(u+\mu) = W_0(-\mu e^{-\mu}) = -\mu$ giving $u = 0$ which should be discarded and the second one is $-(u+\mu) = W_{-1}(-\mu e^{-\mu})$ giving :

$$p(\mu) = \left(1 + \frac{\mu}{W_{-1}(-\mu e^{-\mu})}\right)^2$$

Using this formula the asymptotic probability of indecomposability of a permutation as a function of μ can be computed, its graph is depicted in Figure 4.

The value for $\mu = 1/2$ computed with Maple is 0.511699676.

3.2 Proofs

3.2.1 Asymptotics of Stirling numbers of the first kind

We use two results on those asymptotics.

The first one, due to Moser and Wyman ([MW58] Equation (5.7)) gives the following formula for Stirling numbers of the first kind in the asymptotic regime where n and m tend to infinity such that $m/n = \mu$ is fixed:

$$s_{n,m} \sim b \frac{n!}{a^n \sqrt{n}} \frac{u^m}{m!}. \tag{11}$$

Here, u is such that $\mu = u/(e^u - 1)$, $a = 1 - e^{-u}$, and $b = \sqrt{\frac{u}{2\pi(ue^u - e^u + 1)}}$ (note that since $\mu < 1$, we have $u > 0$ and b is well defined.)

The second one is due to Temme ([Tem93] Equation (3.5)) and the author shows that his approximation is uniformly valid with respect to m when $n \to \infty$. He introduces the following function:

$$\phi(x) = \ln(x+1)(x+2)\cdots(x+n) - m \ln x.$$

He considers x_0, the unique positive root of $\phi'(x) = 0$. Note that, letting $u = m/x_0$, we can check that $u/(e^u - 1) \sim \mu$, showing the relation between the two results. Indeed, x_0 satisfies

$$\frac{m}{x_0} = \sum_{i=1}^{n} \frac{1}{x_0 + i}.$$

The left hand side equals u. The right hand side can be approximated by $\int_{x_0}^{x_0+n} dt/t = \ln(1 + n/x_0)$, giving $u \sim \ln(1 + u/\mu)$, hence $\mu \sim u/(e^u - 1)$.

From there, substituting m/u for x_0 in ([Tem93] Equation (3.5)), using Stirling's approximation for $(n-m)!$, and approximating sums by integrals, we recover Equation (11), showing its uniformity. More precisely we have:

Lemma 6

$$\forall \epsilon\ \exists \alpha, N_0 \ \text{ such that } \forall \mu \text{ if } n > N_0 \text{ and } 1 - \alpha \leq \frac{m}{n\mu} \leq 1 + \alpha \text{ then :}$$

$$1 - \epsilon \leq \frac{s_{n,m}}{b \frac{n!}{a^n \sqrt{n}} \frac{u^m}{m!}} \leq 1 + \epsilon.$$

3.2.2 Proof of Lemma 4.

We use the inclusion-exclusion formula. The number of permutations of $\mathbb{S}_{n,m}$ such that $a_1 = 1$ is equal to $s_{n-1,m-1}$, the number of those such that $a_n = n$ is also equal to $s_{n-1,m-1}$, and the number of those such that $a_1 = 1$ and $a_n = n$ is equal to $s_{n-2,m-2}$. Hence:

$$\Pr(A_{n,m}) = \frac{2s_{n-1,m-1} - s_{n-2,m-2}}{s_{n,m}}.$$

In order to conclude we evaluate the limit of $\frac{s_{n-1,m-1}}{s_{n,m}}$.

Lemma 7 *The quotient $\frac{s_{n,m}}{s_{n-1,m-1}}$ tends to $\frac{a\mu}{u}$ when n and m tend to infinity with $\frac{m}{n}$ close to μ.*

Proof: Denote $\mu_1 = \frac{m-1}{n-1}$ and let u_1 be given by $\mu_1 = \frac{u_1}{(e^{u_1}-1)}$ and $a_1 = 1 - e^{-u_1}$ then:

$$\frac{s_{n,m}}{s_{n-1,m-1}} \sim \frac{b_1}{b}\sqrt{\frac{n-1}{n}}\frac{m}{n}\left(\frac{u_1}{u}\right)^m\left(\frac{a}{a_1}\right)^n\frac{a_1}{u_1} \tag{12}$$

The first two of these terms tend to 1, and $\frac{ma_1}{nu_1}$ tends to $\frac{\mu a}{u}$ when n, m tend to infinity. It remains to evaluate the limit of the function ϕ of m, n given by:

$$\phi(m,n) = \left(\frac{u_1}{u}\right)^m\left(\frac{a}{a_1}\right)^n \tag{13}$$

To compute this limit we evaluate the logarithm of this expression which is equal to $n(\log(a) - \log(a_1)) - m(\log(u) - \log(u_1))$. By Rolle's standard theorem we have:

$$\frac{\log(\phi(m,n))}{\mu - \mu_1} = \frac{d(n\log(a) - m\log(u))}{d\mu} \tag{14}$$

where the derivative is taken as some point μ_2 (with corresponding values u_2 and a_2) between μ_1 and μ. We write:

$$\frac{d(n\log a - m\log(u))}{d\mu} = \frac{n}{a_2}\frac{da}{d\mu} - \frac{m}{u_2}\frac{du}{d\mu}. \tag{15}$$

Since $a = 1 - e^{-u}$ the derivatives of a and of u at μ_2 are related by:

$$\frac{da}{d\mu} = e^{-u_2}\frac{du}{d\mu}$$

Dividing the two members of the equation by $e^{u_2} - 1$ gives:

$$\frac{1}{1-e^{-u_2}}\frac{da}{d\mu} = \frac{1}{e^{u_2}-1}\frac{du}{d\mu}$$

Hence, using $\mu_2 = \frac{u_2}{e^{u_2}-1}$ and $a_2 = 1 - e^{-u_2}$ we have:

$$\frac{da}{d\mu} = \frac{a_2\mu_2}{u_2}\frac{du}{d\mu}$$

Substituting that in (14) and (15) gives:

$$\frac{\log(\phi(m,n))}{\mu-\mu_1} \;=\; \frac{n}{u_2}(\mu_2-\mu)\frac{du}{d\mu}.$$

Noting that

$$\mu-\mu_1=\frac{1-\mu}{n-1},$$

and using continuity of the derivative $du/d\mu$ in $[\mu_1,\mu]$, we obtain

$$\log(\phi(m,n))=\frac{1-\mu}{(1-1/n)u_2}(\mu_2-\mu)\frac{du}{d\mu}=O(\mu-\mu_2)=O(1/n),$$

and so:

$$\left(\frac{u_1}{u}\right)^m\left(\frac{a}{a_1}\right)^n\sim 1.$$

□

We now return to prove Lemma 4 Since n/m tends to μ, by uniformity (Lemma 6) we obtain applying Lemma 7 twice:

$$\Pr(A_{n,m})=\frac{2s_{n-1,m-1}}{s_{n,m}}-\frac{s_{n-2,m-2}}{s_{n-1,m-1}}\frac{s_{n-1,m-1}}{s_{n,m}}\sim\frac{2a\mu}{u}-\frac{a^2\mu^2}{u^2}.$$

Since $a=1-e^{-u}$, and $\mu=\frac{u}{e^u-1}$, the result follows. □

3.2.3 Proof of Lemma 5.

Let $T_{n,m}$ denote the set of permutations of $\mathbb{S}_{n,m}$ such that neither condition (9) nor condition (10) holds. We will partition the permutations of $\mathbb{S}_{n,m}$ according to their *shape*, defined below, and prove by probabilistic arguments that within each class of permutations having the same shape, the fraction of those which are in $T_{n,m}$ is negligible.

To each permutation α in $\mathbb{S}_{n,m}$, we associate a shape $(n_1,\ldots,n_m;p,q,b,r)$ defined as follows. $n_1\geq n_2\geq\cdots\geq n_m$ are the lengths of the m cycles of α; p and q are the lengths of the cycles containing 1 and n; when $p=q$, b is a boolean indicating whether 1 and n are in the same cycle; and when b is true, $r>1$ is the smallest integer such that $\alpha^r(1)=n$. The shape of a permutation in $\mathbb{S}_{n,m}$ may be represented by a directed graph with n vertices of indegree and outdegree 1, consisting of the union of m (directed) cycles of lengths $n_1,n_2,\ldots,n_m$, and of two distinguished edges, that are not loops and that are called the *initial* and the *last* edges. We identify a shape and the associated graph.

Lemma 8 *In the graph representing a shape σ there exist $(n-m)/2-4$ edges, that are pairwise disjoint, and disjoint from the initial and last edges. We say that those edges are* marked.

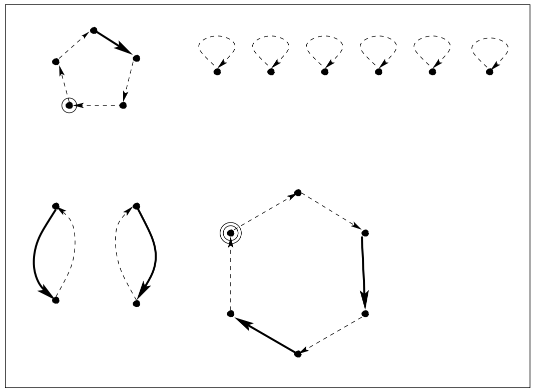

Figure 5: The shape $(6, 5, 2, 2, 1, 1, 1, 1, 1; 5, 6)$, the initial vertex is indicated by a circle and the last one by a double circle; the marked edges are in bold.

Proof: There are m cycles, of which m_1 have length 1. In each of the cycles of length n_i, we can mark at least $(n_i - 1)/2$ disjoint edges, for a total of $[(n - m_1) - (m - m_1)]/2$ marked edges. Discounting the marked edges that touch the initial or the last edge yields the result. $\square$

Lemma 5 follows by summing Equation (16) below over all shapes.

Lemma 9 *Given a shape σ, let $s^\sigma_{n,m}$ and $t^\sigma_{n,m}$ be the number of permutations with shape σ in $\mathbb{S}_{n,m}$ and in $T_{n,m}$. Then*

$$t^\sigma_{n,m} \leq s^\sigma_{n,m} \frac{1 + \ln((n - m - 8)/2)}{n - m - 8}. \tag{16}$$

Proof: Let $\alpha = a_1, a_2, \ldots, a_n$ be a permutation of shape $\sigma = (n_1, \ldots, n_m; p, q, b, r)$, and let $(j_1, a_{j_1}), (j_2, a_{j_2}, \ldots, (j_\ell, a_{j_\ell})$ denote the $\ell = (n - m)/2 - 4$ marked edges. We may suppose $p, q > 1$ since this means $a_1 \neq 1, a_n \neq n$. If α is in $T_{n,m}$, then the following condition holds

$$\forall i = 1, 2, \ldots, \ell, \quad \neg(j_i \leq a_1 \text{ and } a_{j_i} > a_n). \tag{17}$$

Consider the set of points

$$(a_1, a_n), (j_1, a_{j_1}), \ldots, (j_\ell, a_{j_\ell}).$$

The rank of a_1 among $\{a_1, j_1, \ldots j_\ell\}$ is uniform in $\{1, 2, \ldots, \ell + 1\}$. If a_1 has rank r then Property (17) is satisfied if and only if a_n is maximum among $\{a_n, a_{j_1}, \ldots, a_{j_{r-1}}\}$. This event has probability $1/r$, giving $t^\sigma_{n,m}/s^\sigma_{n,m} \leq \sum_{r=1}^{\ell+1}(1/\ell + 1)(1/r)$. Using the well-known inequality $H_n \leq 1 + \ln(n)$ gives the statement of the lemma. $\square$

4 Remarks

4.1 Numerical results

It is well-known that $(s_{n,m})$ satisfies $s_{n,m} = 0$ for $m = 0$ or $m > n$, $s_{1,1} = 1$, and:

$$s_{n,m} = s_{n-1,m-1} + (n-1)s_{n-1,m} \tag{18}$$

The numbers $c_{n,m}$ of indecomposable permutations of $\mathbb{S}_{n,m}$, can be computed by a formula similar to that giving the number of those in $\mathbb{S}_n$, (see for instance [Cor09], Proposition 2)

$$c_{n,m} = s_{n,m} - \sum_{p=1}^{n-1} \sum_{i=1}^{min(m,p)} c_{p,i} s_{n-p,m-i} \tag{19}$$

Thus the value of $p_{n,m} = \frac{c_{n,m}}{s_{n,m}}$ can be computed exactly by using the above formulas inductively for small n.

We have proved that the error term $|p_{n,m} - p(\mu)|$ is bounded by $O(\log(n-m)/(n-m))$. The error is actually very small. The table below gives some values of $\frac{c_{n,m}}{s_{n,m}}$ for $n = 20, n = 100$ and for some values of m/n. The last row shows the values of the fonction $p(m/n)$ allowing the comparison.

m/n	0.05	0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80	0.90	0.95	1
$p_{20,m}$	1	0.968	0.883	0.774	0.644	0.5	0.35	0.207	0.090	0.02	0.005	0
$p_{100,m}$	0.981	0.95	0.868	0.764	0.643	0.51	0.371	0.236	0.116	0.03	0.006	0
$p(m/n)$	0.978	0.946	0.865	0.762	0.642	0.511	0.374	0.241	0.122	0.035	0.009	0

4.2 Comments

- The majority (51.1... percent) of permutations of $\mathbb{S}_{2m}$ with m cycles are indecomposable.

- Since there is a bijection between indecomposable permutations and hypermaps (see [dMR04]) our result shows that the probability for an ordered pair of permutations σ, α on $\mathbb{S}_n$ to generate a transitive group when σ is supposed to have m cycles is about the same as the probability for a permutation of $\mathbb{S}_{n+1,m}$ to be indecomposable. Hence this probability is about 0.511 when $n = 2m$.

- It would be interesting to know the structure of the group generated by two permutations when their number of cycles is given. When these numbers are not fixed then Dixon (see [Dix05]) proved that the probability that they generate the symmetric or alternating group is near to 1, using the fact that they generate a transitive group with probability 1. But as we saw transitivity cannot be assumed when the number of cycles is given and large.

References

[Com72] L. Comtet. Sur les coefficients de l'inverse de la série formelle $\sum n!t^n$. *C. R. Acad. Sci. (Paris)*, A275:569—572, 1972.

[Com74] L. Comtet. *Advanced combinatorics, the art of finite and infinite expansions*. Reidel publishing, 1974.

[Cor09] R. Cori. Indecomposable permutations, hypermaps and labeled Dyck paths. *J. Combin. Theory Ser. A*, 116:1326—1343, 2009.

[Dix05] J. D. Dixon. Asymptotics of generating the symmetric and alternating groups. *Electronic J. Comb.*, 12, R56, 2005.

[dMR04] P. Ossona de Mendez and P. Rosenstiehl. Transitivity and connectivity of permutations. *Combinatorica*, 24:487—502, 2004.

[FS09] Ph. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

[GJ83] I. P. Goulden and D. J. Jackson. *Combinatorial Enumeration,*. John Wiley and Sons, New York, 1983.

[GS95] I. Gessel and R. Stanley. Algebraic enumerations. In R. Graham, M. Grötschel, and L. Lovász, editors, *Handbook of Combinatorics*, pages 1021–1062. North Holland, 1995.

[Hal49] M. Hall. Subgroups of finite index in free groups. *Canadian J. Math.*, 1:187—190, 1949.

[Knu73] D. E. Knuth. *The Art of Computer Programming, Vol 3*. Addison-Wesley, 1973.

[Knu05] D. E. Knuth. *The Art of Computer Programming, Vol 4, Fascicle 2, Generating all Tuples and Permutations*. Addison-Wesley, 2005.

[Len72] A. Lentin. *Equations dans les monoïdes libres*. Gauthier-Villars, Paris, 1972.

[Lot83] Lothaire. *Combinatorics on words*. Addison-Wesley, Paris, 1983.

[MW58] L. Moser and M. Wyman. Asymptotic development of the Stirling numbers of the first kind. *J. London. Math. Soc*, 33:133—146, 1958.

[Odl95] A. Odlyzko. Asymptotic enumeration methods. In R. Graham, M. Grötschel, and L. Lovász, editors, *Handbook of Combinatorics*, pages 1063–1230. North Holland, 1995.

[Sta99] R. P. Stanley. *Enumerative Combinatorics, Volume 2*. Cambridge University Press, 1999.

[Tem93] N. Temme. Asymptotic estimates of Stirling numbers. *Studies in Appl. Math*, 89:233—243, 1993.

[Ten07] B. E. Tenner. Pattern avoidance and the Bruhat order. *J. Comb. Theory (A)*, 114:888—905, 2007.