Indecomposable permutations with a given number of cycles

Robert Cori[1][†] and Claire Mathieu[2]

[1]*Labri, Université Bordeaux 1, F-33405, Talence Cedex, France*
[2]*Computer Science Department, Brown University, Providence RI 02912, USA*

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 compute the asymptotic probability that a permutation of $\mathbb{S}_n$ with m cycles is indecomposable as n goes to infinity with m/n fixed. The error term is $O(\frac{\log(n-m)}{n-m})$. 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 (51.1... percent) of the permutations are indecomposable. We also consider indecomposable fixed point free involutions which are in bijection with maps of arbitrary genus on orientable surfaces, for these involutions with m left-to-right maxima we obtain a lower bound for the probability of being indecomposable.

Résumé. Une permutation $a_1 a_2 \ldots a_n$ est *indécomposable*, s'il n'existe pas de $p < n$ tel que $a_1 a_2 \ldots a_p$ est une permutation de $\{1, 2, \ldots, p\}$. Nous calculons la probabilité pour qu'une permutation de $\mathbb{S}_n$ ayant m cycles soit indécomposable et plus particulièrement son comportement asymptotique lorsque n tend vers l'infini et que m/n est fixé. Cette valeur décroît régulièrement de 1 à 0 lorsque m/n croît, et il n'y a pas de phénomène de seuil. Lorsque $n = 2m$, une faible majorité (51.1... pour cent) des permutations sont indécomposables. Nous considérons aussi les involutions sans point fixe indécomposables qui sont en bijection avec les cartes de genre quelconque plongées dans une surface orientable, pour ces involutions ayant m maxima partiels (ou records) nous obtenons une borne inférieure pour leur probabilité d'êtres indécomposables.

Keywords: Permutations, enumeration, asymptotics.

1 Introduction.

Indecomposable permutations (also often called connected) have been considered by many authors trying to show that they play the same role for permutations as connected graphs play in graph theory. 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 20 years later by A. Lentin[Len72] and L. Comtet [Com72] and are quoted in good place in many classical books in Combinatorics and Algorithms (see for instance [Com74], [Knu05], [GJ83], and [Sta99]). More recently, a bijection was given by P. Ossona de Mendez and P. Rosenstiehl in [dMR04] with hypermaps (or equivalently bicolored maps) is such a way that the number of cycles of the permutation is equal to the number

---

[†]Work done while visiting the CS Department at Brown University.

of vertices of the hypermap (equivalently the number of vertices of a given color of the bipartite map). Hence in order to generate at random a hypermap with a fixed number m of vertices, a natural algorithm consists in generating permutations with m cycles until obtaining an indecomposable one, then to build the hypermap in bijection with it. The efficiency of this algorithm depends on the value of the probability for a permutation with m cycles to be indecomposable. Intuitively this probability is expected to be a decreasing function of $\frac{m}{n}$; we will prove this fact asymptotically in this paper and give a precise description of the asymptotic limit of this function when n and m tend to infinity keeping $\frac{n}{m}$ constant.

In a second part of the paper we restrict these permutations to be involutions with no fixed points and take as parameter the number of left-to-right maxima instead of the number of cycles, note that these two statistics are equal for general permutations. Similarly the above bijection associates to indecomposable involutions maps on orientable surfaces having the same number of vertices as the involution has left-to-right maxima. We obtain a lower bound on the probability for an involution with no fixed points and a given number of let-to-right maxima to be indecomposable. We use combinatorial arguments and a coding of these involutions by labeled Dyck words, often called *histoires d'Hermite*, (see [dMV94], [Dra09]).

Notation

A permutation will be denoted $a_1 a_2 \ldots a_n$, it 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. 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:

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

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 this statement, up to lower order terms; we prove that a permutation with $n/2$ cycles is indecomposable with probability about $.5117\ldots$; and for any $\mu \in (0, 1]$, we calculate the asymptotic probability that a permutation over $\{1, \ldots, n\}$ with approximatively μn cycles is decomposable.

Let $\mathbb{S}_{n,m}$ denote the set of permutations of $\mathbb{S}_n$ with m cycles, $s_{n,m}$, the unsigned Stirling number of the first kind, denote the cardinality of $\mathbb{S}_{n,m}$, and $\mu = m/n$. Let $\alpha = a_1 a_2 \ldots a_n$ denote a permutation of $\{1, 2, \ldots n\}$.

2   Main result and proof overview

Theorem 1 *Let μ be a rational number less than 1. If m and n tend to infinity while keeping their ratio fixed at $m/n = \mu$, then the probability $p_{n,m}$ that a permutation of $\mathbb{S}_{n,m}$ is indecomposable tends to $p(\mu)$,*

$$p(\mu) = \frac{(e^u - 1)^2}{e^{2u}}, \tag{1}$$
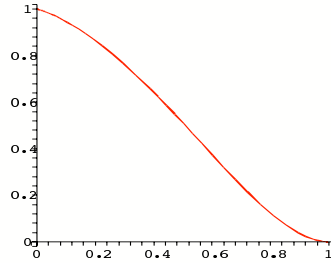
Fig. 1: Asymptotic probability $p_\infty(\mu)$ that a permutation of $\mathbb{S}_n$ with μn cycles is indecomposable, as a function of μ.

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

$$\mu = \frac{u}{e^u - 1}. \tag{2}$$

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

The asymptotic probability of indecomposability of a permutation as a function of μ is depicted in Figure 1.

The value for $\mu = 1/2$ computed with Maple is 0.511699676. The proof of Theorem 1 follows directly from the following three lemmas. The first lemma states some simple facts and has a short proof.

Lemma 1 *If the following condition holds, then α is decomposable:*

$$(a_1 = 1) \quad \text{or} \quad (a_n = n) \tag{3}$$

*If the following condition holds, then α is indecomposable:*

$$(\exists i, i \leq a_1 \text{ and } a_i > a_n) \tag{4}$$

Proof: If condition (3) 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 $p < i \leq n$ either $i \leq p$ satisfies $a_i > a_1$ contradicting (4). 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 2.

$\square$

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]
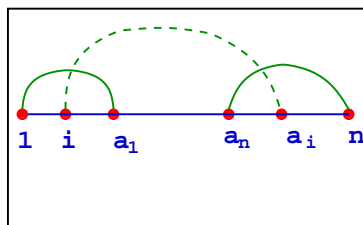
Fig. 2: Illustration of Condition 4 guaranteeing indecomposability.

Lemma 2 *Let m, n, μ, u be defined as in Theorem 1. Then the probability that a permutation of $\mathbb{S}_{n,m}$ satisfies condition (3) tends to*

$$\frac{2e^u - 1}{e^{2u}}.$$

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

Lemma 3 *The probability that a permutation of $\mathbb{S}_{n,m}$ satisfies neither condition (3) nor condition (4) is $O(\frac{\log(n-m)}{n-m})$.*

3   Proofs

3.1   Proof of Lemma 2.

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 the number satisfying condition (3) is equal to

$$t_{n,m} = 2s_{n-1,m-1} - s_{n-2,m-2}.$$

Moser and Wyman ([MW58] Equation (5.7)) give 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:

$$s_{n,m} = b\frac{n!}{a^n\sqrt{n}}\frac{u^m}{m!}(1 + O_\mu(1/m)), \tag{5}$$

where u satisfies Equation (2) with $\mu = m/n$, $a = 1 - e^{-u}$, $b = \sqrt{\frac{u}{2\pi(ue^u - e^u + 1)}}$ (note that since $\mu < 1$, we have $u > 0$ and b is well defined,) and the constants in the $O_\mu(1/m)$ are continuous functions of μ.

Using continuity, it is easy to prove that $\frac{t_{n,m}}{s_{n,m}}$ tends to $\frac{2e^u - 1}{e^{2u}}$. The details will be given in the extended version of the paper.

3.2 Proof of Lemma 3.

Let $S_{n,m}$ denote the set of permutations of $\mathbb{S}_{n,m}$ such that neither condition (3) nor condition (4) hold. 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 $E_{n,m}$ is negligeable.

To each permutation α in $E_{n,m}$, 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 vertices, belonging to cycles of length not less than 2 and called the "initial" and the "last" vertices. We identify a shape and the associated graph.
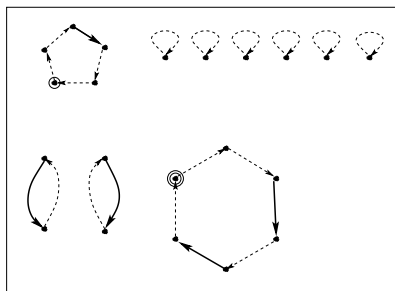
Fig. 3: The shape $(6, 5, 2, 2, 1, 1, 1, 1, 1; 5, 6)$, the initial vertex is indicated by a circle and the last one by a double circle; the marked edges are in bold.

Given any shape σ, the following process defines a permutation drawn uniformly at random among the permutations of $\mathbb{S}_{n,m}$ with shape σ:

- To each undistinguished vertex, independently assign a real number drawn uniformly at random from the interval $[0, 1]$; assign 0 to the initial vertex and 1 to the last vertex.

- Give integer labels $1, 2, \ldots n$ to the n vertices of the diagram in such a way that the labels are in the same order as the reals assigned to them. This defines the permutation $a_1, a_2, \ldots, a_n$ such that the edge with head labeled i has tail labeled a_i.

Lemma 4 *In the graph representing a shape σ there exist $(n - m)/2 - 2$ edges, called* marked *edges, such that no head of a marked edge is the tail of another marked edge and such that the initial and the last vertex are neither a head nor a tail of a marked edge.*

Proof: There are m cycles, of which m_1 have length 1. In each of the cycles of length $n_i \geq 2$, 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 vertex yields the result. $\qquad\square$

Lemma 3 follows by summing Equation (6) below over all shapes.

Lemma 5 *Given a shape σ, let $s_{n,m}^\sigma$ and $e_{n,m}^\sigma$ be the number of permutations with shape σ in $\mathbb{S}_{n,m}$ and in $E_{n,m}$. Then*

$$e_{n,m}^\sigma \leq s_{n,m}^\sigma \frac{4\log((n-m-4)/2)}{n-m-4}(1+o(1)). \tag{6}$$

Proof: (of Lemma 5.) Let $\alpha = a_1, a_2, \ldots, a_n$ be a permutation of shape $\sigma = (n_1, \ldots, n_m; p, q, b, r)$ obtained by the process. We may suppose $p, q > 1$ since this means $a_1 \neq 1, a_n \neq n$. Then α in $E_{n,m}$, if for all i the following condition holds

$$\neg(i \leq a_1 \ \text{and} \ a_i > a_n)$$

The probability of this event is less than if the condition holds only for the i corresponding to the heads of marked edges. But since the marked edges have no common end points, the conditions on each marked edges are independent. Hence an upper bound for the probability of decomposability is the ℓ-th power of the satisfaction of one of the conditions.

Let x and y be the real numbers assigned to the tails of the edges which heads are the first and the last vertex respectively. For every marked edge, the values x_i and y_i associated to its head and tail respectively are such that we do not have $(x_i < x$ and $y_j > y)$.

Fix x, y; for each marked edge, the probability of the event $(x_i < x$ and $y_i > y)$ is $x(1-y)$. By definition of the marked edges, the values x_i, y_i are independent, and so the probability that no (x_i, y_i) among the $(n-m-4)/2$ marked edges has $(x_i < x$ and $y_i > y)$ is : $(1-x(1-y))^{(n-m-4)/2}$. Then, denoting $\ell = (n-m-4)/2$, the proportion $\varepsilon_{n,m}$ of permutations with shape σ in $E_{n,m}$ is bounded by:

$$\varepsilon_{n,m} \leq \int_0^1 \int_x^1 (1-x(1-y))^\ell dy dx.$$

Using the well known inequality $1 - z \leq e^{-\frac{z}{2}}$ for $z \in [0,1]$ (with $z = x(1-y)$) we obtain:

$$\varepsilon_{n,m} \leq \int_0^1 \int_x^1 e^{-\frac{x(1-y)\ell}{2}} dy dx \;=\; \int_0^1 \int_0^{1-x} e^{-\frac{xy\ell}{2}} dy dx \;=\; \int_0^1 \frac{2}{x\ell}(1 - e^{-\frac{x(1-x)}{2}}) dx.$$

We decompose $[0,1]$ in two intervals $[0, \frac{1}{\ell}]$ and $[\frac{1}{\ell}, 1]$. When $x \geq 1/\ell$ the function inside the integral can be bounded by $2/(x\ell)$. When $x < 1/\ell$ we use again $1 - e^{-\frac{z}{2}} \leq z$ for $z \in [0,1]$ (with $z = x(1-x)$) and write:

$$\varepsilon_{n,m} \leq \int_0^{\frac{1}{\ell}} \frac{2(1-x)}{\ell} dx + \int_{\frac{1}{\ell}}^1 \frac{2}{x\ell} dx \leq \frac{2\log\ell}{\ell} + \frac{2}{\ell^2} = \frac{2\log\ell}{\ell}(1+o(1)).$$

Substituting $\ell = (n-m-4)/2$, the lemma follows.   □

4 Remarks

4.1 Numerical results

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

$$s_{n,p} = s_{n-1,p-1} + (n-1)s_{n-1,p} \tag{7}$$

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)

$$c_{n,k} = s_{n,k} - \sum_{p=1}^{n-1} \sum_{i=1}^{min(k,p)} c_{p,i} s_{n-p,k-i} \tag{8}$$

Thus the exact value of $\frac{c_{n,k}}{s_{n,k}}$ 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. For instance we find for $n = 20$ and $n = 100$:

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
$p_\infty(m/n)$	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 Left-to-right maxima

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. Hence the probabilities obtained above are also those for a permutation with m left-to-right maxima to be indecomposable.

4.3 Comments

- The majority ($51.1 \ldots$ 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, his proof uses 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.

5   Fixed point free involutions.

We now consider involutions with no fixed points (which we will call fpf-involutions for short in the sequel), that is, permutations of $\mathbb{S}_{2m}$ with m cycles, all of length 2, hence belonging the subset of $\mathbb{S}_{2m}$ for which the probability of being indecomposable is close to 0.51. However assuming that the cycles are all of length 2 implies that the probability increases to $1 - \frac{1}{m}$. This can easely be proved using the recursion formula giving the number c_m of indecomposable fpf-involutions namely :

$$c_m = (2m - 1)!! - \sum_{k=1}^{m-1} c_k (2m - 2k - 1)!!$$

where $(2k - 1)!! = \prod_{i=1}^{k} (2i - 1)$ is the total number of fpf-involutions of $\mathbb{S}_{2k}$.

Ossona de Mendez and Rosenstiehl in [dMR05] gave a bijection between rooted maps on orientable surfaces with $m - 1$ edges, and indecomposable fpf-involutions of $\mathbb{S}_{2m}$; in this bijection the number of vertices of the map is equal to the number of left-to-right maxima of the corresponding involution. This allows a new proof of the results in [AB00], see also: [BJ02], [Dra09].

Hence it is interesting to find the number $a_{m,k}$ of fpf-involutions of length m having k left-to-right maxima. No simple formula for these numbers are known unlike for Stirling numbers, which the statistics of the same parameter for general permutations.

Let $c_{m,k}$ be the number of indecomposable fpf-involutions of $\mathbb{S}_{2m}$ with k lef-to-right maxima; it is also the number of rooted maps with $m - 1$ edges and k vertices.

In order to calculate the numbers $a_{n,k}$ and $c_{n,k}$ we use a bijection between these involutions and labeled Dyck words which will be recalled in Section 6. The values obtained allowed us to conjecture that the probability for an fpf-involution to be indecomposable increases smoothly when the number of left-to-right maxima decreases.

We are not able to prove this conjecture, but we obtain as a partial result a lower bound for the the proportion of indecomposable fpf-involutions with a given number of left-to-right maxima:

Theorem 2 *The numbers of decomposable fpf-involutions $d_{m,k} = a_{m,k} - c_{m,k}$ of $\mathbb{S}_{2m}$, having k left-to-right maxima satisfy:*

$$d_{m,k} \leq \frac{4k}{m} c_{m,k}$$

Hence the probability that a random fpf-involution of $\mathbb{S}_{2m}$ with λm left-to-right maxima is decomposable is at most $4\lambda/(1 + 4\lambda)$.

In Section 6 we recall the bijection between fixed point free involutions and labeled Dyck words. In Section 7 we give a sketch of the proof of Theorem 2.

6   Labeled Dyck words.

Dyck words.

We consider words over the two letters alphabet $\{a, b\}$. We denote the length of a word w by $|w|$, and the number of occurrences of the letter x by $|w|_x$. A Dyck word u is a word such that $|u|_a = |u|_b$ and $|u'|_a \geq |u'|_b$ for any of its prefixes u' (i. e. $u = u'u''$). The *height* of the occurrence of a letter x in

$w = w'xw"$ is defined as $|w'x|_a - |w'x|_b$. A Dyck word is *decomposable* if there exist two non-empty Dyck words u', $u"$ such that $u = u'u"$. It is indecomposable otherwise.

Labeling

We consider the infinite alphabet $\{a, b_0, b_1, b_2, \ldots, b_i, \ldots\}$, and use the notation $|w|_b = \sum_{i \geq 0} |w|_{b_i}$ allowing to define the heights of occurence of letters as above. A *labeled Dyck word* is a word f on this alphabet such that

1. Replacing every b_i for $i \geq 0$ by b in f gives a Dyck word, and

2. Every occurrence of b_i in f has height at least i.

A labeled Dyck word is decomposable if replacing every b_i for $i \geq 0$ by b gives a decomposable Dyck word. Let L_m denote the set of labeled Dyck words of length $2m$, and $L_{m,k}$ denote the subset of those having k occurrences of b_0. Let $a_{m,k}$ be the number of words of $L_{m,k}$ and $c_{m,k}$ the number of indecomposable ones. We define the polynomials A_m and C_m by :

$$A_m(x) = \sum_{k=0}^{m} a_{m,k} x^k \qquad C_m(x) = \sum_{k=0}^{m} c_{m,k} x^k \tag{9}$$

Then we have, where A_0 is set equal to 1 :

Proposition 1 *For any $m \geq 1$ the polynomials A_m and C_m satisfy the following recursion equations:*

$$C_m(x) \quad = \quad x A_{m-1}(x+1) \qquad A_m(x) \quad = \quad \sum_{k=1}^{m} C_k(x) A_{m-k}(x) \tag{10}$$

Proof: For the first equations note that an indecomposable Labeled Dyck word w is equal to avb_0 where v is obtained from a a labbeled Dyck word u by choosing a subset of occurrences of b_i and replacing them by b_{i+1}. The seoncd one follows from the fact that any labeled Dyck word is the concatenation of an indecomposable one and another labeled Dyck word (possibly empty). $\square$
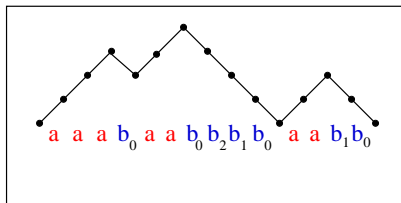
Bijection.

The following algorithm describes a well-known bijection between fpf-involutions of $\mathbb{S}_m$ and labeled Dyck words of length $2m$, such that the labeled Dyck word is indecomposable if and only if the involution is indecomposable. Less known is the fact that the number of left-to-right maxima of α is equal to the number of occurrences of b_0 in the corresponding word. It takes as input a fpf-involution $\alpha \in \mathbb{S}_{2m}$ and outputs the labeled Dyck word $f = f_1 f_2 \cdots f_{2m}$. It uses an ordered list Q.

for i = 1 to 2m do
  if $(\alpha(i) > i)$
    then { add i at the end of Q, and set $f_i = a$; }
    else { let j be the position of $\alpha(i)$ in Q; set $f_i = b_{j-1}$, and remove $\alpha(i)$ from Q; }
  For instance, for the involution $\alpha = (1,4)(2,7)(3,10)(5,9)(6,8)(11,14)(12,13)$, we get

$$f = a\ a\ a\ b_0\ a\ a\ b_0\ b_2\ b_1\ b_0\ a\ a\ b_1\ b_0$$

Fig. 4: Labeled Dyck word corresponding to the involution
$(1, 4)(2, 7)(3, 10)(5, 9)(6, 8)(11, 14)(12, 13)$

6.0.1   Enumeration

A consequence of this bijection is that the number of fpf-involutions of $\mathbb{S}_{2m}$ with k left-to-right maxima is $a_{m,k}$ and that of indecomposable ones is $c_{m,k}$. These numbers can be computed thanks to Equation (10). Moreover we have $a_{m,1} = c_{m,1} = (2m - 3)!!$ since any fpf-involution with one left-to-right maximum is indecomposable and is equal to $(1, 2m)\beta$, where β is any fpf-involutions over $2, \dots 2m - 1$ a. We also have: $a_{m,m} = C_m$ and $c_{m,m} = C_{m-1}$ where C_k denotes the k-th Catalan number since the fpf-involutions with of $\mathbb{S}_{2m}$ with m left-to-right maxima correspond to labbelled Dyck words with all the b_i equal to b_0 and the indecomposable ones to indecomposable Dyck words with the same property.

This gives some values for this numbers and allows to compare our result in Theorem 2 with values of $\frac{c_{m,k}}{a_{m,k}}$ for $m = 100$ showing an important gap except when k is close to 1 or close to m.

k/m	0.001	0.10	0.20	0.30	0.40	0.50	0.60	0.70	0.80	0.90	1
$m/(m + 4k)$	0.96	0.71	0.55	0.45	0.38	0.33	0.29	0.26	0.24	0.22	0.20
$c_{m,k}/a_{m,k}$	1	0.98	0.95	0.90	0.86	0.80	0.74	0.67	0.58	0.46	0.25

7   Sketch of proof of Theorem 2

In order to explain this proof we consider a much simple result for Dyck words which we will try to genralise for labeled Dyck words.

7.1   A simpler result

Proposition 2 *The number of decomposable Dyck words of length $2m$ is less than 4 times the number of indecomposable ones.*

Proof: There is a very simple proof since we know that the number of decomposable Dyck words of length $2m$ is $C_m - C_{m-1}$ and that of indecomposable ones is C_{m-1}.   □

Note that this simple proof shows also that we could have a better result replacing 4 by 3 in the Proposition. But it is impossible to generalize this simple proof in ordrer to obtain a result for labeled Dyck words with k occurrences of b_0, since we do not know a nice formula for the number of such words of length $2m$. Hence we need another proof which do not uses any formula and which has a bijective flavour. For that we define *admissible factorisations* of decomposable Dyck words and prooced in three steps.

An *admissible factorisation* of a decomposable Dyck word w consists of a pair of words (u, v) such that $uv = w$, u ends with an a and contains a prefix which is an indecomposable (hence non empty) Dyck word. So that we can write $u = u_1 u' a$ where u_1 is an indecomposable Dyck word.

Let d_m and c_m be the number of decomposable and indecomposable Dyck words of length $2m$. Denote F_m the set of all admissible factorisations of decomposable ones and f_m the number of elements of F_m

Step 1: $md_m \leq 2f_m$

Proof: A decomposable Dyck word w writes $w = u_1 u_2 \ldots u_k$ where the u_i are indecomposable Dycl words. Let $2m_i$ denote the length of u_i for $i = 1, k$, the number of admissible factorisations of w is $m - m_1$. If this number is less than $m/2$ then the word $w = u_k u_1 u_2 \ldots u_{k-1}$ has $m - m_k$ admissible factorisations and the sum of these two numbers is greater or equal to m. Hence proving the result. $\quad\square$

Step 2: factorisations of indecomposable Dyck words

Consider the set F'_m of pair of words (u, v) such that uv is an indecomposable Dyck word of length $2m$ and u ends with an occurrence of a. Then the number f'_m of elements of F'_m is equal to mc_m.

Step 3: $f_m < 2f'_m$

We build a mapping Φ from the set F_m into F'_m such that each element of F'_m is the image of at most 2 elements of F_m. Let $(u_1 w' a, v) \in F_m$ be such that u_1 is an indecomposable Dyck word and $u_1 w' a v$ is a decomposable one.

- If $u_1 = ab$ then we set $\Phi((u_1 w' a, v)) = (a w' a, vb)$

- If $u_1 \neq ab$ then $u_1 = aa w_1 b w_2 b$ where w_1, w_2 are (not necessarily indecomposable) Dyck words. In that case we set $\Phi((u_1 w' a, v)) = (a w_1 a w' a, v b w_2 b)$.

It is clear that for any factorisation (u', v') in F'_m there are only two candidates (u, v) to be such that $\Phi(u, v) = (u', v')$.

Putting all together we obtain :

$$md_m \;\leq\; 2f_m \;<\; 4f'_m \;=\; 4mc_m$$

Ingredients for the generalisation

In order to prove Theorem 2 we consider the set $L_{2m,k}$ of Dyck words of length $2m$ on the alphabet with 3 letters: $\{a, b_0, b\}$, having k occurrences of b_0 and such that no occurrence of b has height less than 1. For each word $w \in L_{2m,k}$ denote $\lambda(w)$ the number of labeled Dyck words that are obtained from w by replacing the occurrences of b by a b_i. Then the numbers $c_{m,k}$ and $d_{m,k}$ in Theorem 2 are the sums of the $\lambda(w)$ for indecomposable and decomposable words of $L_{2m,k}$ respectively. Then we modify the proof in three steps above to make it work for words in $L_{2m,k}$. The main difficulty is in Step 3, since the mapping Φ has to be modified in such a way that $\Phi((u, v)) = (u', v')$ implies $\lambda(uv) \leq \frac{m}{k} \lambda(u'v')$.

The detailed construction of such a mapping Φ will be given in the extended version of this paper.

References

[AB00]   D. Arques and J-F. Béraud. Rooted maps on orientable surfaces, Riccati's equation and contin-
          ued fractions. *Discrete Math.*, 215:1—12, 2000.

[BJ02]   D. Brown and D. Jackson. The quadrangulation conjecture for orientable surfaces. *Journal of
          Combinatorial Theory (B)*, 86:54–79, 2002.

[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. Comb. Theory
          (A), to appear*, 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. *Com-
          binatorica*, 24:487—502, 2004.

[dMR05]   P. Ossona de Mendez and P. Rosenstiehl. Encoding pointed maps by double occurence words.
          KAM-DIMATIA Series, 752:487—502, 2005.

[dMV94]   A de Medicis and X. G. Viennot. Moments des polynômes de Laguerre et la bijection de
          Foata-Zeilberger. *Adv. Appl. Math*, 15:262—304, 1994.

[Dra09]   D. Drake. The combinatorics of associated Hermite polynomials. *European J. Combin*,
          30:1005–1021, 2009.

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

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

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

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

[Lot83]   M. Lothaire. *Combinatorics on Words*. Encyclopedia of Math. and its Apl, (Vol 17). Addison-
          Wesley, London, 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.

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