On random minimal factorizations of large $n$-cycles

Mohamed Amine Bennouna, Yassine El Maazouz
supervisor: Igor Kortchemski
March 2019

Abstract

We study minimal factorizations of the $n$-cycle, which are factorizations of the permutation $(1, \ldots, n)$ into a product of $n - 1$ transpositions. We implement an algorithm that generates a uniformly distributed minimal factorization by using a bijection between these factorizations and Cayley trees. With this generator, we are able to observe behavior of random minimal factorizations predicted by Korchesmski & Feray [5]. We are also interested in primitive minimal factorizations, which are minimal factorizations where the sequence of the smallest elements of transpositions is non decreasing. We construct an algorithm that generates a random primitive minimal factorization uniformly by using bijections with Dyck paths and 231-avoiding sequences. With this generator, we observe the behaviour of these random factorizations and we establish an explicit formula for the law of the first transposition of this factorization.

1 Introduction and motivation

We study the geometric structure of minimal factorizations of the $n$-cycle represented as a compact subset of the unit disk in the plane $\mathbb{R}^2$. More precisely we denote by $\mathfrak{S}_n$ the symmetric group of permutations acting on $[n] := \{1, \ldots, n\}$ and $\mathfrak{T}_n$ the set of all transpositions of $\mathfrak{S}_n$. We denote by $(1, \ldots, n)$ the $n$-cycle that maps $i$ to $i + 1$ for $1 \leq i \leq n - 1$ and $n$ to $1$. This particular $n$-cycle will be referred to as of this point by: the $n$-cycle.

It is easy to see that the minimal number of transpositions needed to factorize the $n$-cycle $c = (1, 2, \ldots, n)$ is at least $n - 1$ since its orbit is $[n]$ i.e: $\{c^k(1) : 1 \leq k \leq n - 1\} = [n]$ (its graph consists of one connected component). And since $(1, 2, \ldots, n) = (1, 2)(2, 3)\ldots(n - 1, n)$ the minimal number of transpositions needed is exately $n - 1$. We denote by

$$\mathfrak{M}_n := \{ (\tau_1, \ldots, \tau_{n-1}) \in \mathfrak{T}_n^{n-1} : \tau_{n-1}\tau_{n-2} \ldots \tau_1 = (1, \ldots, n) \}$$

the set of all minimal factorizations of the $n$-cycle into transpositions. The cardinal of this set is $|\mathfrak{M}_n| = n^{n-2}$ as proved by Dénes in [3]. Bijection proofs are given by Moszkowski [11], Goulden & Pepper [6], Goulden & Yong [7] and Biane [1].

Remark 1. Let $G_{\mathfrak{S}_n}$ be the undirected graph with $\mathfrak{S}_n$ as a node set and $E_G := \{\{\sigma, \tau\} \subset \mathfrak{S}_n : \sigma\tau^{-1} \text{ is a transposition } \}$ as an edge set. Minimal factorizations of the $n$-cycle into transpositions can be seen a geodesics from the identity permutation to the $n$-cycle on this graph.
We denote by $\mathbb{D} := \{ z \in \mathbb{C}, |z| \leq 1 \}$ the closed unit disk of the complex plane, $S := \{ z \in \mathbb{C}, |z| = 1 \}$ the unit circle. For every $x, y \in S$, we denote by $[x, y]$ the line segment between $x$ and $y$ in $\mathbb{D}$. To any non-oriented graph $G$ with vertex set $[n]$ and edge set $E_G$ we associate a subset $\hat{G}$ of $\mathbb{D}$ defined as follows:

$$\hat{G} := \bigcup_{\{k,l\} \in E_G} [e^{2i\pi k/n}, e^{2i\pi l/n}]$$

Given a factorization $F^n = (\tau_1, \ldots, \tau_{n-1}) \in \mathfrak{M}_n$ and $1 \leq k \leq n - 1$ let $F^n_k = (\tau_1, \ldots, \tau_k)$ be the first $k$ transpositions of $F^n$. We can then define the graph associated to $F^n_k$ as the graph $G(F^n_k)$ with vertex set $[n]$ and edge set $E_{F^n_k} := \{ \{a, b\} : (a, b) = \tau_i \text{ for some } i \in [k] \}$ and $\hat{G}(F^n_k)$ is the subset of $\mathbb{D}$ associated to $G(F^n_k)$ as defined above. An example is given in Figure 1.

![Figure 1: An example of $G(F^n_k)$ for $F^n = ((5, 7), (6, 7), (1, 5), (4, 5), (2, 3), (2, 4))$ (numbers 1 to 7 are represented on the circle in trigonometric order).](image)

Let $\mathfrak{S}^n$ be a uniformly distributed random variable in $\mathfrak{M}_n$ for all $n \geq 1$. Féray and Kortchemski [5, Theorem 1.3] establish a limit theorem for the process $\hat{G}(\mathfrak{S}^n_c) \subset \mathbb{D}$ for different orders of magnitude of $c_n$. In particular their results predict a phase transition when $c_n \sim c\sqrt{n}$ for $c > 0$.

In section 2 we explore various methods to simulate a uniformly random labelled Cayley trees conditioned to have size $n$. We then use the bijection given by Goulden and Pepper [6] to simulate the variables $\mathfrak{S}^n$ in order to visualize the phase transition predicted in [5, Theorem 1.3].

We also study primitive minimal factorizations of the $n$-cycle which form a subset of $\mathfrak{M}_n$ and are defined as follows:

Let $F^n = (\tau_1, \ldots, \tau_{n-1}) \in \mathfrak{M}_n$ be a minimal factorization where $\tau_k = (a_k, b_k)$ and $a_k < b_k$ for $k \in [n - 1]$. $F^n$ is said to be primitive if the sequence $(a_k)_{1 \leq k \leq n-1}$ is non-decreasing. We denote by $\mathfrak{P}\mathfrak{M}_n$, the set of primitive minimal factorization of the $n$-cycle.

In section 3 we use the bijections in [8] and in [2] to simulate uniformly random primitive factorizations of the $n$-cycle, and we prove a limit theorem for the first transposition of these factorizations.
2 Generating a uniformly random minimal factorization

2.1 Minimal factorizations and labelled Cayley trees

In order to sample a uniformly random minimal factorization, we use a simple bijection established by Goulden and Pepper in [6] between minimal factorization and Cayley trees. We denote by \( \mathcal{GM}_n := \{ (\tau_1, \ldots, \tau_{n-1}) \in T_{n-1}^n : \tau_1\tau_2\ldots\tau_{n-1} = \text{some } n\text{-cycle} \} \) the set of minimal factorisations of all \( n \)-cycles of the symmetric group \( S_n \) (not only \( 1, \ldots, n \)). We can easily see that \( |\mathcal{GM}_n| = (n-1)! |\mathcal{M}_n| \) since every \( n \)-cycle has the same number of minimal factorizations as \( 1, \ldots, n \) and there are \( (n-1)! \) \( n \)-cycles in total.

There exists a natural bijection between the set \( \mathcal{GM}_n \) and the set of labelled trees of size \( n \) (vertices are labelled from 1 to \( n \) and edges from 1 to \( n-1 \)). More precisely, given a minimal factorization \( F_n = (\tau_1, \ldots, \tau_{n-1}) \in \mathcal{GM}_n \) where \( \tau_k = (a_k, b_k) \) for \( 1 \leq k \leq n-1 \), construct its corresponding labelled tree iteratively by reading the factorization from right to left as follows:

- Start with a graph of \( n \) vertices labeled from 1 to \( n \) and no edges.
- For \( 1 \leq k \leq n-1 \) add an edge between vertex \( a_k \) and vertex \( b_k \) and label the edge by \( k \).

We can easily verify as done in [6] that the application induced by this construction is a bijection between labelled Cayley trees of size \( n \) and \( \mathcal{GM}_n \).

Simulating a uniformly distributed random variable \( F_n \) in \( \mathcal{GM}_n \) is then equivalent to simulating a uniformly distributed random labelled Cayley tree of size \( n \).

Here is an example for \( n = 7 \) and \( F^7 = ((5,7), (6,7), (1,5), (4,5), (2,3), (2,4)) \):

![Labelled Cayley tree example]

Recall that our objective is to simulate a random variable in \( \mathcal{M}_n \subset \mathcal{GM}_n \). To do so we take advantage of the fact that all \( n \)-cycles have the same number of minimal factorisations \( n^{n-2} \) in other words the set \( \mathcal{GM}_n \) is the union of \( (n-1)! \) disjoint classes of factorizations (one for each \( n \)-cycle) that have the same cardinality. Given a factorization \( F^n \in \mathcal{GM}_n \) we denote by \( c_{F^n} \) it’s corresponding \( n \)-cycle and by \( c_{F^n}F^n c_{F^n}^{-1} \) the factorization obtained by conjugating all the transpositions in \( F^n \) by \( c_{F^n} \). One can verify that the resulting factorization \( c_{F^n}F^n c_{F^n}^{-1} \) is a minimal factorization of the \( n \)-cycle i.e \( c_{F^n}F^n c_{F^n}^{-1} \in \mathcal{M}_n \).

It can also be easily verified that if \( \mathfrak{F}^n \) is a uniformly distributed random variable in \( \mathcal{GM}_n \) then \( c_{\mathfrak{F}^n}\mathfrak{F}^n c_{\mathfrak{F}^n}^{-1} \) is a uniformly distributed random variable in \( \mathcal{M}_n \). We will focus
on generating a uniform random Cayley tree conditioned on having \( n \) vertices and then 
use the reciprocal of the previous bijection to generate our uniformly random minimal 
factorization in \( \mathfrak{S} \mathfrak{M}_n \) which we will transform by conjugation to a uniformly random 
variable in \( \mathfrak{M}_n \).

2.2 Simulation of uniformly random labelled Cayley tree conditioned to have a fixed size

2.2.1 Naive method

To simulate a uniformly random labelled Cayley tree, the first idea that comes to mind 
is to simulate the tree structure randomly and then label the vertices and the edges with 
uniformly random permutations. More precisely we proceed as follows:

- We start by considering \( n \) vertices \( \{1, \ldots, n\} \) with an empty set of edges \( E \).
- At each iteration we choose a first vertex uniformly randomly and a second vertex 
  that is not in the connected component of the first and we add the edge \( \{i, j\} \) to \( E \).
- At the end we obtain a random tree with \( n \) vertices and we relabel the vertices and 
  the edges uniformly randomly.

This algorithm allows us to generate a random labelled Cayley tree with \( n \) vertices in 
two steps: the first two points construct a random tree structure and the last one adds 
a random labelling (for both vertices and edges) to the structure. One might think that 
this method yields a uniformly random labelled Cayley tree with \( n \) vertices but it is not 
the case as we explain in the following example:

**Example 1.** For \( n = 4 \) there are \( (n - 1)!n^{n-2} = 3 \times 2^5 \) labelled trees with 4 vertices. 
We will calculate the probability of having a particular tree when simulated with the naive 
algorithm.

Consider following simple linear tree:

```
  1   2   3   4
```

On 4 vertices we have only 2 tree structures: either the linear tree structure (where all 
non-leaf vertices have degree 1), or the following tree structure

```
      a
     /|
    b  c  d
```

We can easily compute the probability that the naive algorithm above yields the linear 
tree structure. That computation gives us a probability of \( \frac{1}{3} \). There are only two permutations of \( \mathfrak{S}_4 \) that give us the correct vertices labelling to get the 
linear tree represented above. So that give us a probability of \( \frac{2}{7} \). That leave us with one 
choice of edge labelling and we get that with a probability of \( \frac{1}{3} \).

Then the probability of getting the linear tree above is \( p = \frac{1}{3} \times \frac{2}{7} \neq \frac{1}{2^4} \). We then conclude 
that the algorithm described above does not yield a uniform distribution on the labelled 
Cayley trees with size \( n \).
Remark 2. The reason why the naive algorithm fails to yield a uniform distribution is mainly the way it picks the next edge to be added to the tree structure at each iteration. One could fix this problem by proceeding as follows:

At each iteration, instead of choosing a uniformly random vertex from the $n$ vertices, we choose two connected components among all the present connected component at that iteration. Then choose a vertex from both components randomly and then connect the two vertices.

We next present a simulation method based on Bienayme-Galton-Watson trees.

### 2.2.2 Bienayme-Galton-Watson trees (BGW)

We first start by giving a simple definition of BGW trees.

**Definition 1.** Let $(\mu_k)_{k \in \mathbb{N}}$ a probability distribution on $\mathbb{N}$. A BGW tree with reproduction distribution $\mu$ (denoted $\text{BGW}_\mu$) is the random tree that starts with one vertex as a root and each vertex has a random number children with distribution $\mu$. More precisely if we denote by $X_n$ the number of children in generation $n$, there exists a collection of independent random variables $(\xi_{n,k})$ with integer values with the same distribution $\mu$ such that:

- $X_0 = 1$
- $\forall n \geq 0 : X_{n+1} = \sum_{k=1}^{X_n} \xi_{n,k}$

Devroye [4] gives a simple method to generate a random Cayley Tree conditioned on having $n$ vertices. It is based on the observation that a random Cayley tree of size $n$ has the same distribution of a $\text{BGW}_\mu$ conditioned to have size $n$ for a certain reproduction distribution $\mu$ on $\mathbb{N}$. It turns out that Poisson distributions ($\mu_k^\lambda = e^{-\lambda} \frac{\lambda^k}{k!}$) yield a uniformly random Cayley tree of size $n$. The parameter of Poisson distribution does not have any impact because of the conditioning, see [4] and [9] for details.

First we generate an ordered sequence $\Xi_r = (\xi_1, ..., \xi_n)$ verifying $\inf\{1 \leq t \leq n | \sum_{j=1}^{t} \xi_j = n - 1\} = n$.

- Generate $n - 1$ random variables $Z_i \sim \mathcal{U}([1, n])$ uniform in the set of $\{1, ..., n\}$.
- For all $i \in [1, n]$, set $\xi_i = \sum_{j=1}^{Z_i} 1_{Z_j = i}$ and $\Xi = (\xi_1, ..., \xi_n)$.
- Set $S_t(\Xi) = 1 + \sum_{j=1}^{t} (\xi_j - 1)$ for $1 \leq t \leq n$.
- Find $l = \arg\min\{S_t(\Xi) | 1 \leq t \leq n\}$.
- Set $\Xi_r = (\xi_{l+1}, ..., \xi_n, \xi_1, ..., \xi_l)$.

With the sequence $\Xi_r$, we construct the graph as follow. Start with a root node and put it in a queue. At the $i$th step, grab the first node from the queue, give it $\xi_i$ children, and place these in the queue. The process ends when the queue is empty. The condition over $\Xi_r$ ensures that the process ends with a tree $T$ of correct size $n$. By labeling the vertices and edges of $T$ randomly we obtain a uniformly generated random Cayley Tree.
2.3 Results and observations

In [5], it is proved (Theorem 1.3) that $G(F_{\lfloor n - \sqrt{n} \rfloor}^n)$ converges to the so-called Brownian triangulation which looks like the following:

![Figure 2: A realisation of $G(F_{\lfloor n - \sqrt{n} \rfloor}^n)$ for $n = 10000$](image)

In order to visualise the phase transition in $\sqrt{n}$ we need to generate $F^n$ for a large $n$ and plot the $c_n$ first transpositions for different order of magnitude $c_n$. In the following figures we have chosen $n = 100000$.

**Case $c_n = c n^{1/3}$ :**

![Figure 3: Drawing of $G(F_{\lfloor c_n \rfloor}^n)$ for $c_n$ of order $O(n^{1/3})$](image)

**Case $c_n = c n^{1/2}$ :**

![Figure 4: Drawing of $G(F_{\lfloor c_n \rfloor}^n)$ for $c_n$ of order $O(n^{1/3})$](image)
Case \( c_n = c \cdot n^{2/3} \):

![Image](image)

Figure 5: Drawing of \( G(F_{\lfloor c_n \rfloor}^n) \) for \( c_n \) of order \( O(n^{2/3}) \)

### 3 Primitive Factorizations and Dyck paths

In this section, our goal is to generate uniformly a primitive minimal factorization. We recall that a primitive minimal factorization is a minimal factorization where the sequence of smallest elements of each transposition is increasing.

We denote by \( \mathcal{PM}_n \) the set of primitive minimal factorization of \((1, ..., n+1)\). We will establish a bijection between \( \mathcal{PM}_n \) and the set of Dyck paths of length \( 2n \) denoted by \( \text{Dyck}_n \).

#### 3.1 231-avoiding permutations

We call a given permutation \( \sigma \) a 231-avoiding path if \( \sigma \) does not contain a subword \([\sigma_i, \sigma_j, \sigma_k]\) with \( \sigma_k < \sigma_i < \sigma_j \). We denote the set of 231-avoiding paths \( \mathcal{A}^\text{231}_n \) and the set of 132-avoiding paths by \( \mathcal{A}^\text{132}_n \). 231-avoiding paths are closely linked with primitive minimal factorizations. Indeed, Gewurz and Merola [2] exhibited a simple and intuitive bijection between \( \mathcal{PM}_n \) and \( \mathcal{A}^\text{132}_n \) and thus inducing a natural extention to \( \mathcal{A}^\text{231}_n \) (By taking a reflexion of the elements of \( \mathcal{A}^\text{132}_n \)). They proved that the map that associates with \((a_1, b_1)(a_2, b_2)...(a_n, b_n)\) the sequence \(b_1b_2...b_n\) is a bijection between \( \mathcal{PM}_n \) and \( \mathcal{A}^\text{231}_n \). They also gave an iterative algorithm that gives the antecedent of a 231-avoiding path by the map.

231-avoiding permutations will be our bridge from Dyck paths to primitive minimal factorization as we will now see a bijection between 231-avoiding permutations and Dyck paths.

#### 3.2 Dyck paths

A Dyck path of semilength \( n \) is a sequence of \( 2n \) containing \( n - 1 \)'s and \( n \)'s such that every prefix contains at least as many \( 1 \)'s as \(-1\)'s. Notice that if we draw a Dyck path in a graph, it will always start at \((0, 0)\), stay in the positive orthan and end at \((2n, 0)\). In fact, it is an equivalent definition of Dyck paths.

Krattenthaler gives a bijection between \( \text{Dyck}_n \) and \( \mathcal{A}^\text{231}_n \) [8]. Given \( \sigma \in \mathcal{A}^\text{231}_n \) we read the permutation \( \sigma \) from left to right and successively generate a Dyck path. When \( \sigma_j \) is read, then in the path we adjoin as many up-steps as necessary, followed by a down-step from height \( h_j + 1 \) to height \( h_j \) (measured from the \( x \)-axis), where \( h_j \) is the number of elements in \( \sigma_{j+1}...\sigma_n \) which are larger than \( \sigma_j \). This mapping is a bijection from \( \mathcal{A}^\text{231}_n \) to \( \text{Dyck}_n \).
As we use the inverse of this mapping for our simulation, we will explicit it. Given a Dyck path $D \in Dyck^n$ (which we see it as a sequence of $+1$ and $-1$) we read the path from left to right and successively generate a 231-avoiding path. Let $L_0 = (1, ..., n)$ and let $c_0 = n$ be a cursor we will iterate over $L$. We denote by $L[k]$ the $k$th element of $L$. At step $i$, when $D_i$ is read, we move the cursor by $-D_i$, i.e., $c_i = c_{i-1} - D_i$. If $D_i = -1$, we add $L_i[c_i]$ to the sequence $\sigma$ (being constructed from left to right) and we delete $L_i[c_i]$ from $L_i$ shifting all elements of $L_i$ to the left to fill the empty space, i.e, $L_i[1, ..., c_i - 1] = L_{i-1}[1, ..., c_i - 1]$ and $L_i[c_i, ...] = L_{i-1}[c_i + 1, ...]$.

### 3.3 Simulation of a Dyck path

To generate a uniformly random Dyck path in $Dyck^n$ we proceed as follows:

- We first generate a symmetric random walk $(S_k)_{k \leq 2n+1}$ with jumps in $\{\pm 1\}$ conditioned to stop in $-1$ (i.e: $S_{2n+1} = -1$) by using rejection sampling.
- We then use Vervaat transformation (see [10]) on this walk to get another walk $(V(S)_k)_{k \leq 2n+1}$. We then forget the last jump to get a uniformly random Dyck path $D_n$ in $Dyck^n$.

### 4 Simulations

Simulating a 231-avoiding sequence of $1, 2, ..., n$ using the bijection with Dyck paths allows us to get the simulate the second element of the first transposition easily. Generating a large sample of this element gives us an idea on how it is distributed (Figure 6).

![Figure 6: distribution of the second element of the 2\textsuperscript{nd} of the 1\textsuperscript{st} transposition of a primitive factorisation 1000](image)

From a 231-avoiding sequence in $A_231^n$, we easily access the number of transposition which contains 1 which corresponds to the first index of 1 in the sequence. We can then simulate this random variable and plot a histogram.
5 Results on the behaviors of random minimal factorization

In this section we prove some results on the behavior of random primitive minimal factorizations motivated by the results of our simulations.

**Proposition 1.** Let \( \pi \) be a random variable such that \( \pi \sim U(\mathfrak{PM}_n) \). Let \( \tau \) be its first transposition starting from left. Then \( \Pr(\tau = (1, 2)) = \Pr(\tau = (1, n)) = \frac{c_{n-1}}{c_n} \to \frac{1}{4} \).

**(Proof.** Using the bijection between \( \mathfrak{PM}_n \) and \( A_{231}^n \) we only need to show that if \( \sigma \sim U(S_n) \) (where \( S_n \) is the set of permutations), \( \Pr(\sigma_1 = 1|\sigma \in A_{231}^n) = \Pr(\sigma_1 = n|\sigma \in A_{231}^n) = \frac{c_{n-1}}{c_n} \).

We denote by \( \sigma^{(n-1)} \) the sequence \( \sigma_2, ..., \sigma_n \).

\[
\Pr(\sigma_1 = 1|\sigma \in A_{231}^n) = \frac{\Pr(\sigma_1 = 1)}{\Pr(A_{231}^n)} \Pr(\sigma \in A_{231}^n|\sigma_1 = 1) \\
= \frac{\Pr(\sigma_1 = 1)}{\Pr(A_{231}^n)} \Pr(\sigma^{(n-1)} \in A_{n-1}^{231}|\sigma_1 = 1) \\
= \frac{\Pr(\sigma_1 = 1)}{\Pr(A_{231}^n)} \Pr(\sigma^{(n-1)} \in A_{n-1}^{231}) \\
= \frac{1}{n} \frac{c_{n-1}}{c_n} = \frac{c_{n-1}}{c_n} \to \frac{1}{4}
\]

The proof for \( \tau = (1, n) \) is similar. \( \square \)

**Proposition 2.** Let \( \pi \) be a random variable such that \( \pi \sim U(\mathfrak{PM}_n) \). Let \( \tau \) be its first transposition starting from left. Then \( \Pr(\tau = (1, 3)) = \Pr(\tau = (1, n-1)) = \frac{c_{n-2}}{c_n} \to \frac{1}{16} \).
Proof.

\[ P(\sigma_1 = 2|\sigma \in A_{n}^{231}) = \frac{P(\sigma_1 = 2)}{P(A_{n}^{231})}P(\sigma \in A_{n}^{231}|\sigma_1 = 2) \]

and

\[ P(\sigma \in A_{n}^{231}|\sigma_1 = 2) = P(\sigma^{(n-1)} \in A_{n-1}^{231} \cap \sigma_1^{(n-1)} = 1|\sigma_1 = 2) \]

\[ = P(\sigma^{(n-1)} \in A_{n-1}^{231} \cap \sigma_1^{(n-1)} = 1) \]

\[ = P(\sigma_1^{(n-1)} = 1|\sigma^{(n-1)} \in A_{n-1}^{231}), P(A_{n-1}^{231}) \]

Then using proposition 1 for \( n - 1 \) we deduce the following:

\[ P(\sigma_1 = 2|\sigma \in A_{n}^{231}) = \frac{1/n}{c_n/n!} \frac{c_{n-1}}{c_{n-1}(n-1)!} \]

\[ = \frac{c_{n-2}}{c_n} \rightarrow \frac{1}{16} \]

The proof for \( \tau = (1, n-2) \) is similar. \( \square \)
References


