

On the Cut-Off Phenomenon for the Transitivity of Randomly Generated Subgroups

André Galligo,¹ Laurent Miclo²

¹Laboratoire J.-A. Dieudonné, UMR 6621, Université de Nice-Sophia Antipolis and CNRS, France; e-mail: Andre.Galligo@unice.fr

²Institut de Mathématiques de Toulouse, UMR 5219, Université de Toulouse and CNRS, France; e-mail: miclo@math.univ-toulouse.fr

Received 15 August 2009; accepted 11 February 2011; received in final form 14 September 2010

Published online 2 June 2011 in Wiley Online Library (wileyonlinelibrary.com).

DOI 10.1002/rsa.20369

ABSTRACT: Consider $K \geq 2$ independent copies of the random walk on the symmetric group S_N starting from the identity and generated by the products of either independent uniform transpositions or independent uniform neighbor transpositions. At any time $n \in \mathbb{N}$, let G_n be the subgroup of S_N generated by the K positions of the chains. In the uniform transposition model, we prove that there is a cut-off phenomenon at time $N \ln(N)/(2K)$ for the non-existence of fixed point of G_n and for the transitivity of G_n , thus showing that these properties occur before the chains have reached equilibrium. In the uniform neighbor transposition model, a transition for the non-existence of a fixed point of G_n appears at time of order $N^{1+\frac{2}{K}}$ (at least for $K \geq 3$), but there is no cut-off phenomenon. In the latter model, we recover a cut-off phenomenon for the non-existence of a fixed point at a time proportional to N by allowing the number K to be proportional to $\ln(N)$. The main tools of the proofs are spectral analysis and coupling techniques. © 2011 Wiley Periodicals, Inc. *Random Struct. Alg.*, 40, 182–219, 2012

Keywords: random walks on symmetric groups; uniform transposition model; uniform neighbor transposition model; cut-off phenomenon; flared transition phenomenon; existence of a fixed point for random subgroups; transitivity for random subgroups; spectral analysis; coupling techniques; exclusion processes; isoperimetric bounds

1. INTRODUCTION

The cut-off phenomenon usually describes the fast transition of the time-marginal distributions of a Markov chain from being far from the equilibrium to being close to it. This subject has been introduced and investigated by Persi Diaconis and his coauthors, see for

Correspondence to: Laurent Miclo

© 2011 Wiley Periodicals, Inc.

instance [1, 5, 6] and the references therein. Here we will study the cut-off phenomenon not for the convergence to stationarity, which requires to consider all possible events, but only for particular events such as the transitivity of the subgroup generated by some elements from a symmetric group obtained by a Monte-Carlo Markov chain procedure. In general this kind of property occurs before the underlying Markov chain reaches equilibrium and we will see that depending on how the Markov chain is generated, there will be or not a cut-off phenomenon.

Let us describe more precisely the kind of questions we are interested in. Let μ be a probability measure on S_N the set of permutations of $E_N := \{1, \dots, N\}$, with $N \in \mathbb{N} \setminus \{0, 1\}$ which corresponds to the size of the problem. We consider $Z := (Z_n)_{n \in \mathbb{N}}$ a corresponding random walk starting from the identity. The simplest way to construct such a Markov chain is to use a family $(\tilde{Z}_n)_{n \in \mathbb{N}^*}$ of independent random variables distributed according to μ and to begin with $Z_0 = \iota$, the identity element of S_N , and next to take iteratively for any $n \in \mathbb{N}$, $Z_{n+1} = \tilde{Z}_{n+1}Z_n$. For $K \in \mathbb{N} \setminus \{0, 1\}$, which we will sometimes call the multiplicity of the problem, let $Z^{(1)}, \dots, Z^{(K)}$ be K independent chains distributed as Z (the possibility $K = 1$ is excluded from our study, indeed the following results are not true in this case). Our main object of investigation is the subgroup $G_n^{(K)}$ of S_N generated by $Z_n^{(1)}, \dots, Z_n^{(K)}$ at time $n \in \mathbb{N}$, and we are particularly interested in two features of its natural action of $G_n^{(K)}$ on E_N : transitivity and the existence of a fixed point. The latter property asks for the existence of $x \in E_N$ such that for any $g \in G_n^{(K)}$, $g(x) = x$, while the former property means that for any $x \in E_N$, there exists $g \in G_n^{(K)}$ such that $g(1) = x$ (i.e. the permutation g has moved the element at position 1 to position x and the product of permutations will be interpreted as the composition of the corresponding mappings), in particular there is no fixed point. Let us denote respectively $A_n^{(K)}$ and $B_n^{(K)}$ the events that $G_n^{(K)}$ acts transitively on E_N and that $G_n^{(K)}$ admits at least one fixed point. The purpose of this paper is to study the mappings

$$\mathbb{N} \ni n \mapsto \mathbb{P}[A_n^{(K)}] \quad \text{and} \quad \mathbb{N} \ni n \mapsto \mathbb{P}[B_n^{(K)}] \tag{1}$$

(where \mathbb{P} is the underlying probability measure) as N grows to infinity. This will be done for two particular choices of μ , or more precisely of sequences of such probability distributions, since for any $N \in \mathbb{N} \setminus \{0, 1\}$ we have to be given a probability measure μ on S_N . We don't know a priori if these mappings are monotonous in $n \in \mathbb{N}$, contrary to the quantities of interest in the study of convergence to equilibrium, such as the total variation distance between the time marginal distribution and the invariant measure. Indeed, if the support of μ is a generating set for the group S_N and if it contains ι , then Z is an irreducible and aperiodic Markov chain, so its invariant measure ν has S_N for support. Applying the ergodic theorem to the Markov chain $(Z^{(1)}, \dots, Z^{(K)})$, which admits $\nu^{\otimes K}$ for its attracting measure, it follows that almost surely,

$$\begin{aligned} \liminf_{n \rightarrow \infty} \mathbb{1}_{A_n^{(K)}} &= 0 \\ \limsup_{n \rightarrow \infty} \mathbb{1}_{A_n^{(K)}} &= 1 \end{aligned}$$

so we cannot assert in a deterministic way that the subgroup will eventually become transitive. In addition, for n large, $\mathbb{P}[A_n^{(K)}]$ will converge to the probability that K independent elements sampled according to ν generate a transitive subgroup of S_N , a quantity which is strictly smaller than 1 (similar remarks hold for the existence of a fixed point). Nevertheless, we conjecture that the above mappings are respectively increasing and decreasing under our assumption that $(Z_0^{(1)}, \dots, Z_0^{(K)}) = (\iota, \dots, \iota)$. Of course such monotonicity properties

depend on the initial configuration, for instance the situation would have been completely different if we had started with (σ, \dots, σ) where σ is a cycle of order N .

For any size $N \in \mathbb{N} \setminus \{0, 1\}$, multiplicity $K \in \mathbb{N} \setminus \{0, 1\}$ and time $n \in \mathbb{N}$, let $C_{K,n}$ be either $A_n^{(K)}$ or the complementary event of $B_n^{(K)}$. We say there is a cut-off phenomenon for $(C_{K,n})_{n \in \mathbb{N}}$, if we can find a time $T(N, K) \in \mathbb{R}_+$ such that

$$\begin{aligned} \forall \alpha \in [0, 1), \quad \lim_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &= 0 \\ \forall \alpha \in (1, +\infty), \quad \lim_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &= 1 \end{aligned}$$

where for any $t \in \mathbb{R}_+ \setminus \mathbb{N}$, we took $C_{K,t} := C_{K, \lfloor t \rfloor}$, with $\lfloor \cdot \rfloor$ designating the integer part (this convenient embedding of discrete time into continuous time will be implicitly enforced in the whole paper to simplify notations). Such a result would give a rigorous probabilistic meaning to the assertion that the subgroup $G_n^{(K)}$ becomes transitive at time $T(N, K)$. Of course such a time $T(N, K)$ can only be defined up to an equivalence relation as N becomes large.

More generally, we say that a transition phenomenon occurs at times of order $T(N, K) \in \mathbb{R}_+^*$, if

$$\begin{aligned} \lim_{\alpha \rightarrow 0_+} \limsup_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &= 0 \\ \lim_{\alpha \rightarrow +\infty} \liminf_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &= 1 \end{aligned}$$

A priori this definition does not forbid that several transition phenomena can occur at times of different orders. So to avoid this possibility, we will speak of a unique transition phenomenon at times of order $T(N, K) \in \mathbb{R}_+^*$, if furthermore for any sequence of positive numbers $(\alpha_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ converging to zero, we have

$$\lim_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha_N T(N,K)}] = 0 \tag{2}$$

and for any sequence of positive numbers $(\alpha_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ diverging to infinity, we have

$$\lim_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha_N T(N,K)}] = 1 \tag{3}$$

The cut-off phenomenon is an example of a transition phenomena, but at the opposite side of this notion, we will speak of a flared transition phenomenon if there is a transition at times of order $T(N, K) \in \mathbb{R}_+^*$ which is not sharp: we can find a non-empty interval $(\alpha_*, \alpha^*) \subset \mathbb{R}_+^*$ such that for any $\alpha \in (\alpha_*, \alpha^*)$, we have

$$\begin{aligned} \liminf_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &> 0 \\ \limsup_{N \rightarrow \infty} \mathbb{P}[C_{K,\alpha T(N,K)}] &< 1 \end{aligned}$$

However there is still hope for a cut-off phenomenon in this situation, if we allow the number of chains K to depend on N . So we will say there is as (K, T) -sharp transition, if we can find a sequence $(K, T) := (K(N), T(N))_{N \in \mathbb{N} \setminus \{1,2\}}$ from $\mathbb{N} \setminus \{0, 1\} \times \mathbb{R}_+$ such that

$$\begin{aligned} \forall \alpha \in [0, 1), \quad \lim_{N \rightarrow \infty} \mathbb{P}[C_{K(N),\alpha T(N)}] &= 0 \\ \forall \alpha \in (1, +\infty), \quad \lim_{N \rightarrow \infty} \mathbb{P}[C_{K(N),\alpha T(N)}] &= 1 \end{aligned}$$

The first case we will investigate is that of uniform generating transpositions, which corresponds to

$$\mu = \frac{2}{N(N-1)} \sum_{i < j \in E_N} \delta_{(i,j)}$$

where (i, j) is the transposition exchanging i and j . The probability μ does not satisfy the assumption that ι belongs to its support and in fact the Markov chain Z is periodic of period 2, going from even to odd permutations and vice-versa. But this is not important for our purposes and if μ is replaced by $(1 - \epsilon_N)\mu + \epsilon_N\delta_\iota$ with $\lim_{N \rightarrow \infty} \epsilon_N = 0$ (if one considers for instance the probability measure $\tilde{\mu} := \frac{1}{N^2} \sum_{i,j \in E_N} \delta_{(i,j)}$, with $(i, i) = \iota$ for any $i \in E_N$), then the next result remains true (see Remark 10 at the end of Section 3 for the links with the continuous time setting).

Theorem 1. *In the above model of uniform generating transpositions, there is a cut-off for transitivity as well as for the non-existence of a fixed point at time*

$$T(N, K) := \frac{1}{2K} N \ln(N)$$

The fact that the cut-off occurs at the same time for both events suggests that a fixed point is the last resort against transitivity in this model. This will be confirmed by the simulations of Section 6. Let us recall (see for instance the book of Diaconis [5]), that for the model of uniform generating transpositions with $\tilde{\mu}$ as distribution of the increments of the random walk, the cut-off phenomenon for the convergence to equilibrium in the total variation sense occurs at time $\frac{1}{2} N \ln(N)$. This is valid for the Markov chain Z but also for its K -product $(Z^{(1)}, \dots, Z^{(K)})$. So for the latter Markov chain, the properties of transitivity and of the non-existence of a fixed point appear strictly before the equilibrium is reached. Nevertheless, note that for any time $n \in \mathbb{N}$, $Z_n^{(1)} Z_n^{(2)} \dots Z_n^{(K)}$ has the same law as Z_{Kn} . It follows that for any $\alpha > 1$,

$$\lim_{N \rightarrow \infty} \mathbb{P}[G_{\alpha T(N,K)}^{(K)} = S_N \text{ or } A_N] = 1$$

where A_N is the alternating group (knowing that $G_{n,K}$ is either S_N or A_N , to decide between this two possibilities it is sufficient to check if there exists an odd permutation among $\{Z_n^{(1)}, \dots, Z_n^{(K)}\}$ or not). Indeed, this a consequence of a result due to Łuczak and Pyber [12], stating that the minimal transitive subgroup containing a permutation chosen uniformly in S_N (role essentially played here by the product $Z_{\alpha T(N,K)}^{(1)} Z_{\alpha T(N,K)}^{(2)} \dots Z_{\alpha T(N,K)}^{(K)}$) is either S_N or A_N with probability going to 1 as N goes to infinity.

The second case we will investigate is that of neighbor generating transpositions, which corresponds to

$$\mu = \frac{1}{N} \sum_{i \in E_N} \delta_{(i,i+1)}$$

where E_N has to be seen as $\mathbb{Z}/N\mathbb{Z}$, so that $N + 1 = 1$.

The situation is now different from the previous one, since we have:

Theorem 2. *At least as soon as $K \geq 3$, there is a flared transition for the non-existence of a fixed point in the model of neighbor generating transpositions, at times of order*

$$T(N, K) := N^{1+\frac{2}{K}}$$

Replacing μ by $\tilde{\mu} := (\delta_i + \sum_{i \in \mathbb{Z}/(N\mathbb{Z})} \delta_{(i,i+1)})/(N+1)$, it is known that the convergence to equilibrium occurs at times of order $N^3 \ln(N)$ (see for instance the survey of Jonasson [10] for a precise statement), so again the property of non-existence of a fixed point appears before equilibrium is reached.

One may consider both the uniform generating transpositions and the neighbor generating transpositions as Monte-Carlo ways to sample sets of K generators of subgroups of the symmetric group without fixed point (even if we don't know which laws one would get by following these procedures) and hopefully of transitive subgroups. Assuming that it is possible to sample according to μ within a time of order 1, the complexity of these algorithms (namely the required computational time) is heuristically $KT(N, K)$. So for the uniform generating transposition chain we get $N \ln(N)/2$ as complexity, while we get $KN^{1+\frac{2}{K}}$ for neighbor generating transposition chain. Optimizing the latter expression in $K \in \mathbb{N} \setminus \{0, 1\}$, it appears that the better choice is $K = 2 \ln(N)$, so we get a complexity of the same order in both cases (if one wants to be more precise at the level of constant factor, one should first remember that at each elementary step, to sample uniformly over a set of cardinality N^2 asks a priori twice the time necessary to sample uniformly over a set of cardinality N). One may think that the first algorithm has the advantage that it admits a cut-off phenomenon, which enables to stop more sharply the algorithm. But this is also true for the second algorithm: consider the decreasing function defined by

$$J : \mathbb{R}_+ \ni \alpha \mapsto \int_0^1 \exp(-2\alpha(1 - \cos(2\pi s))) ds \quad (4)$$

which is going from 1 to 0. Let $\tilde{\alpha} \in \mathbb{R}_+^*$ be the unique value such that $J(\tilde{\alpha}) = \exp(-1/2)$. Then we have

Theorem 3. *In the model of neighbor generating transpositions, there is a (K, T) -sharp transition for the non-existence of a fixed point with*

$$\begin{aligned} K(N) &:= 2 \ln(N) \\ T(N) &:= \tilde{\alpha} N \end{aligned}$$

We conjecture that both Theorems 2 and 3 (with another constant $\tilde{\alpha}$, see Section 6) hold for transitivity. We have not yet been able to prove them, but this is also suggested by simulations, see Section 6.

In fact our motivation for the above results comes from the design of algorithms for bivariate polynomials factorization, relying on combinatorial invariants attached to union of random Riemann surfaces. Let us briefly sketch the link with the transitivity of subgroups generated by products of transpositions. The set of zeros of a "generic" bivariate polynomial $f \in \mathbb{C}[x, y]$ of degree N defines a smooth Riemann surface $X \subset \mathbb{C}^2$, let $\pi : X \rightarrow \mathbb{C}$ denote the first projection $(x, y) \mapsto x$. In this case, X has $N(N-1)$ points with a vertical tangent and their projections by π form a subset Δ of $N(N-1)$ points in \mathbb{C} called the discriminant.

Then, $\pi : X \setminus \pi^{-1}(\Delta) \rightarrow \mathbb{C} \setminus \Delta$ is a connected N -covering, i.e. for each $a \in \mathbb{C} \setminus \Delta$ the fiber above a , namely $\{y \in \mathbb{C} : f(a, y) = 0\}$, consists of N distinct points. Suppose $0 \notin \Delta$ and denote by $E := \{y_1, \dots, y_N\}$, the fiber above 0. Now consider a loop $\gamma \subset \mathbb{C} \setminus \Delta$ starting and ending at 0, and lift it by π^{-1} to N paths in $X \setminus \pi^{-1}(\Delta)$. Each path starts at some $y_i \in E$ and ends at another (possibly the same) $y_j \in E$ and this process defines a permutation p_γ on E ; this permutation only depends on the homotopical class of γ in $\mathbb{C} \setminus \Delta$. The subgroup of S_N generated by all such permutations is called the monodromy group of X , with respect to π . When γ is a “small” loop circling around only one discriminant point, then the permutation p_γ is a transposition. Furthermore, some numerical calculations, reinforced by heuristic arguments, suggest that there exists an ordering of E such that these transpositions are close to uniform neighbor transpositions when N is large and when the discriminant point is chosen uniformly. Anyway when γ is a “large” loop circling around a set of n discriminant points, then γ is homotopic to the concatenation of n “small” loops, and the permutation p_γ is equal to the product of the corresponding transpositions. The question is to predict when a subgroup generated by K permutations of type p_γ has the same connecting effect on E as the whole monodromy group. See e.g. [3] and [14].

The plan of the paper is as follows. In the next two sections we investigate the uniform generating transposition model, first by establishing the cut-off phenomenon for the non-existence of a fixed point for $G_n^{(K)}$ in Section 2 and next for transitivity in Section 3. The two main underlying tools of this proof of Theorem 1 are spectral analysis and coupling techniques, which enable to come back to Markov chains whose spectral decomposition is well-known. The following two sections concerns the neighbor generating transposition model. In Section 4 we prove Theorem 2, namely we show that there is a flared transition for the non-existence of a fixed point. The lack of strong symmetries leads to more involved computations. Section 5 is devoted to the proof of Theorem 24, which is an extension of Theorem 3. It will be a relatively direct consequence of the estimates deduced in Section 4. Finally to illustrate the obtained results and to support our conjectures, we give some simulations in the last Section 6.

2. FIXED POINTS FOR THE UNIFORM GENERATING TRANSPOSITIONS

We prove here the simplest part of Theorem 1, namely we investigate the cut-off phenomenon for the non-existence of a fixed point for the generated subgroup, in the uniform generating transposition model.

Since in this section and the two following ones the multiplicity $K \in \mathbb{N} \setminus \{0, 1\}$ won't depend on the size N of the problem, we remove it from our notation when this doesn't lead to confusion. Thus for instance for any time $n \in \mathbb{N}$, G_n designates the subgroup of S_N generated by $Z_n^{(1)}, \dots, Z_n^{(K)}$, where recall that $Z^{(1)}, \dots, Z^{(K)}$ are K independent random walks on S_N whose increments are uniform transpositions as described in the introduction. For any $x \in E_N$, consider

$$B_n(x) := \{\forall i \in \llbracket 1, K \rrbracket, \quad Z_n^{(i)}(x) = x\}$$

the event saying that x is a fixed point for the action of G_n on E_N , so we can write $B_n = \cup_{x \in E_N} B_n(x)$. As it was announced, our goal here is to prove the

Proposition 4. *In the model of uniform generating transpositions, starting with $(Z_0^{(1)}, \dots, Z_0^{(K)}) = (\iota, \dots, \iota)$, we have*

$$\begin{aligned} \forall \alpha \in [0, 1), \quad \lim_{N \rightarrow \infty} \mathbb{P}[B_{\alpha T(N,K)}] &= 1 \\ \forall \alpha > 1, \quad \lim_{N \rightarrow \infty} \mathbb{P}[B_{\alpha T(N,K)}] &= 0 \end{aligned}$$

where

$$T(N, K) := \frac{1}{2K} N \ln(N)$$

The second convergence is the easiest to prove, since it is a consequence of the rough bound

$$\begin{aligned} \forall n \in \mathbb{N}, \quad \mathbb{P}[B_n] &\leq \sum_{x \in E_N} \mathbb{P}[B_n(x)] \\ &= N \mathbb{P}[B_n(1)] \\ &= N \mathbb{P}[Z_n(1) = 1]^K \end{aligned}$$

where $(Z_n)_{n \in \mathbb{N}}$ is a random walk starting from ι and whose increments are uniform transpositions. Indeed, the next result is quite immediate:

Lemma 5. *If $T(N, K)$ is as in the previous proposition, we have, for any $\alpha \geq 0$,*

$$\lim_{N \rightarrow \infty} N \mathbb{P}[Z_{\alpha T(N,K)}(1) = 1]^K = \begin{cases} +\infty, & \text{if } \alpha < 1 \\ 1, & \text{if } \alpha = 1 \\ 0, & \text{if } \alpha > 1 \end{cases}$$

Proof. Let us denote for any $n \in \mathbb{N}$, $X_n := Z_n(1)$. It appears that $(X_n)_{n \in \mathbb{N}}$ is a Markov chain on E_N , starting from 1 and whose transition matrix P is given by

$$P = \frac{2}{N-1} M + \left(1 - \frac{2}{N-1}\right) \text{Id}$$

where M is the transition matrix whose all entries are $1/N$ and Id is the identity matrix. It follows that for any $n \in \mathbb{N}$,

$$P_n = \left(1 - \frac{2}{N-1}\right)^n \text{Id} + \left(1 - \left(1 - \frac{2}{N-1}\right)^n\right) M$$

(as it is usual in Markovian semi-group theory, we rather denote by P_n the n -th power P^n of matrix P), so we get that

$$\begin{aligned} \mathbb{P}[Z_n(1) = 1] &= P_n(1, 1) \\ &= \left(1 - \frac{2}{N-1}\right)^n + \left(1 - \left(1 - \frac{2}{N-1}\right)^n\right) \frac{1}{N} \\ &= \frac{1}{N} + \frac{N-1}{N} \left(1 - \frac{2}{N-1}\right)^n \end{aligned}$$

We deduce that

$$N\mathbb{P}[Z_{\alpha T(N,K)}(1) = 1]^K = N \left(\frac{1}{N} + \frac{N-1}{N} \left(1 - \frac{2}{N-1} \right)^{\lfloor \alpha N \ln(N)/2K \rfloor} \right)^K$$

Note that for $\alpha > 0$, we have for N large

$$\left(1 - \frac{2}{N-1} \right)^{\lfloor \alpha N \ln(N)/2K \rfloor} \sim \frac{1}{N^{\frac{\alpha}{K}}}$$

(this is even true for $\alpha = 0$). The announced result follows at once since $K \geq 2$. ■

We now come to the first convergence of Proposition 4. As it was noticed by a referee, it is an immediate consequence of the coupon collector theorem. In a first version of this paper (still available at <http://hal.archives-ouvertes.fr/hal-00384188/fr/>), we proved it via an estimate of the variance of the number of fixed points. This was a simple version of the approach that will be used in Sections 4 and 5 to deal with the successive generating transpositions model.

We begin by recalling a statement of the coupon collector theorem. Let $(X_n)_{n \in \mathbb{N}}$ be independent variables uniformly distributed on $\llbracket 1, N \rrbracket$ and let τ_N be the first time $n \in \mathbb{N}$ such that $\{X_0, \dots, X_n\} = \llbracket 1, N \rrbracket$. Then for any $\epsilon > 0$, we have

$$\lim_{N \rightarrow \infty} \mathbb{P}[(1 - \epsilon)N \ln(N) \leq \tau_N \leq (1 + \epsilon)N \ln(N)] = 1 \tag{5}$$

(see for instance Theorem 3.8 of the book of Motwani and Raghavan [13] for a more precise result).

Consider now the case where the law of the increments of Z is the probability $\tilde{\mu}$ described above Theorem 1 (it is equivalent to prove Proposition 4 either with μ or with $\tilde{\mu}$, see Remark 10 below). For any $n \in \mathbb{N}$ and $k \in \llbracket 1, K \rrbracket$, denote $(I_n^{(k)}, J_n^{(k)})$ the transposition enabling to pass from $Z_n^{(k)}$ to $Z_{n+1}^{(k)}$. Next define

$$\forall n \in \mathbb{N}, \forall k \in \llbracket 0, 2K - 1 \rrbracket, \quad X_{2Kn+k} := \begin{cases} J_n^{(1+\lfloor k/2 \rfloor)}, & \text{if } k \text{ is even} \\ J_n^{(1+\lfloor k/2 \rfloor)}, & \text{if } k \text{ is odd} \end{cases}$$

The variables $(X_n)_{n \in \mathbb{N}}$ are independent and uniformly distributed on $\llbracket 1, N \rrbracket$ and let τ_N as above. Clearly for $n < \lfloor \tau_N / (2K) \rfloor$, $G_n^{(k)}$ admits a fixed point, since there is a point which has not been touched by any of the transpositions used up to this time. The first convergence of Proposition 4 then follow from (5).

It is not so immediate to deduce the second part of Proposition 4 from the coupon collector theorem. It is also interesting to remark that this argument will not be sufficient in the situation of successive transpositions: some fixed points will exist for quite a long time after that all the positions have been touched by the random successive transpositions used to construct the chains $Z^{(1)}, \dots, Z^{(K)}$.

3. TRANSITIVITY FOR THE UNIFORM GENERATING TRANSPOSITIONS

Our goal here is to complete the proof of Theorem 1 by establishing the cut-off phenomenon for transitivity. The basic ingredient will be the knowledge of whole spectra of the exclusion process associated to a complete graph random walk.

First we note that if G_n admits a fixed point, it cannot be transitive, so with the notations of the previous section, we have $\mathbb{P}[A_n] \leq \mathbb{P}[B_n^c]$. Proposition 4 then implies that

$$\forall \alpha \in [0, 1), \quad \lim_{N \rightarrow \infty} \mathbb{P}[A_{\alpha T(N,K)}] = 0$$

and to prove Theorem 1 it remains to show that

$$\forall \alpha > 1, \quad \lim_{N \rightarrow \infty} \mathbb{P}[A_{\alpha T(N,K)}] = 1 \tag{6}$$

To simplify notations, we assume for the remaining part of this section that $\alpha > 1$ is fixed and we denote $n_N := \lfloor \alpha T(N, K) \rfloor$.

The proof of (6) begins with very simple bounds. Let \mathcal{R} be the set of nonempty subsets of E_N whose cardinality is less than $N/2$. We have

$$A_{n_N}^c = \{ \exists R \in \mathcal{R} : \forall k \in \llbracket 1, K \rrbracket, Z_{n_N}^{(k)}(R) = R \}$$

so by symmetry (see the proof of Lemma 6 below for a formal justification of the last identity) we get

$$\begin{aligned} \mathbb{P}[A_{n_N}^c] &\leq \sum_{R \in \mathcal{R}} \mathbb{P}[\forall k \in \llbracket 1, K \rrbracket, Z_{n_N}^{(k)}(R) = R] \\ &= \sum_{R \in \mathcal{R}} \mathbb{P}[Z_{n_N}(R) = R]^K \\ &= \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} \mathbb{P}[Z_{n_N}(\{1, \dots, r\}) = \{1, \dots, r\}]^K \end{aligned} \tag{7}$$

This leads us to introduce, for $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$, the set $E_N^{(r)}$ of subsets of E_N whose cardinality is r and the $E_N^{(r)}$ -valued stochastic chain $(R_m^{(r)})_{m \in \mathbb{N}}$ defined by

$$\forall m \in \mathbb{N}, \quad R_m^{(r)} := Z_m(\{1, \dots, r\}) \tag{8}$$

(for $r = 2$, these objects do not coincide exactly with $E_N^{(2)}$ and $(X_m, Y_m)_{m \in \mathbb{N}}$ considered in the previous section, because the latter were related to ordered pairs and not to subsets of cardinality two).

It is not difficult to see that $(R_m^{(r)})_{m \in \mathbb{N}}$ is a Markov chain, whose transition matrix $P^{(r)}$ is given by

$$\forall A, B \in E_N^{(r)}, \quad P^{(r)}(A, B) = \begin{cases} \frac{2}{N(N-1)}, & \text{if } |A \cap B| = r - 1 \\ \frac{N(N-1) - 2(N-r)r}{N(N-1)}, & \text{if } A = B \\ 0, & \text{otherwise} \end{cases}$$

Thus we can write

$$P^{(r)} = \frac{2}{N(N-1)} M^{(r)} + \frac{N(N-1) - 2(N-r)r}{N(N-1)} \text{Id}$$

where $M^{(r)}$ is the $E_N^{(r)} \times E_N^{(r)}$ -matrix given by

$$\forall A, B \in E_N^{(r)}, \quad M^{(r)}(A, B) = \begin{cases} 1, & \text{if } |A \cap B| = r - 1 \\ 0, & \text{otherwise} \end{cases}$$

This is the adjacency matrix of a distance transitive graph (called the Johnson graph $J(N, r)$), so its spectrum is known: the eigenvalues are the quantities $(r - l)(N - r - l) - l$, for $l \in \llbracket 0, r \rrbracket$, with multiplicities $\binom{N}{l} - \binom{N}{l-1}$ (with $\binom{N}{-1} = 0$), cf. the book of Bannai and Ito [2] (see also Diaconis [9] and Donnelly, Lloyd and Sudbury [7]). It follows that the eigenvalues of $P^{(r)}$ are the $\theta_l = 1 - \frac{2l(N-l+1)}{N(N-1)}$ for $l \in \llbracket 0, r \rrbracket$ with multiplicities $\binom{N}{l} - \binom{N}{l-1}$.

This knowledge and the fact that $P^{(r)}$ admits a lot of symmetries enables us to give an explicit formula for the quantity we are interested in:

Lemma 6. *For any time $n \in \mathbb{N}$, we have*

$$\begin{aligned} \mathbb{P}[Z_n(\{1, \dots, r\}) = \{1, \dots, r\}] &= \binom{N}{r}^{-1} \sum_{l \in \llbracket 0, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \theta_l^n \\ &\leq \binom{N}{r}^{-1} \sum_{l \in \llbracket 0, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp\left(-n \frac{2l(N-l+1)}{N(N-1)}\right) \end{aligned}$$

Proof. A one-to-one mapping $g : E_N^{(r)} \rightarrow E_N^{(r)}$ is called a symmetry for $P^{(r)}$ if

$$\forall x, y \in E_N^{(r)}, \quad P^{(r)}(g(x), g(y)) = P^{(r)}(x, y)$$

The set of all such symmetries is a group under the composition law. In our situation this group acts transitively on $E_N^{(r)}$, since it contains all mappings of the form g_h , where h is a one-to-one mapping $h : E_N \rightarrow E_N$ and where g_h is defined by

$$\forall A := \{x_1, \dots, x_r\} \in E_N^{(r)}, \quad g_h(A) := \{h(x_1), \dots, h(x_r)\}$$

Note that for any $n \in \mathbb{N}$, the symmetries for $P^{(r)}$ are also symmetries for $P_n^{(r)}$, so we get that for any $A, B \in E_N^{(r)}$, $P_n^{(r)}(A, A) = P_n^{(r)}(B, B)$ and finally

$$\begin{aligned} \mathbb{P}[Z_n(\{1, \dots, r\}) = \{1, \dots, r\}] &= \frac{1}{|E_N^{(r)}|} \text{tr}(P_n^{(r)}) \\ &= \binom{N}{r}^{-1} \sum_{l \in \llbracket 0, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \theta_l^n \\ &\leq \binom{N}{r}^{-1} \sum_{l \in \llbracket 0, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp\left(-n \frac{2l(N-l+1)}{N(N-1)}\right) \end{aligned}$$

where the last bound is a consequence of the concavity inequality $\ln(1 - x) \leq -x$, valid for any $x < 1$. ■

Now via (7), to end the proof of (6), we have to show that

$$\lim_{N \rightarrow \infty} \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} \left(\binom{N}{r}^{-1} \sum_{l \in \llbracket 0, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp\left(-n_N \frac{2l(N-l+1)}{N(N-1)}\right) \right)^K = 0 \tag{9}$$

To do so, let $\eta \in (0, 1)$ be small enough so that $\gamma := (1 - \eta)\alpha > 1$ (recall that $\alpha > 1$ is the fixed number entering in the definition of n_N), we denote $\beta := (\gamma + 1)/2 > 1$, $p := \lfloor (\beta - 1)^{-1} \rfloor + 1$ and $r_N := \lfloor \eta N \rfloor$. For $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$, we introduce the quantities

$$\begin{aligned}
 H_N(r) &:= \binom{N}{r}^{-1} \sum_{l \in \llbracket 0, p \wedge r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp \left(-n_N \frac{2l(N-l+1)}{N(N-1)} \right) \\
 I_N(r) &:= \binom{N}{r}^{-1} \sum_{l \in \llbracket (p \wedge r) + 1, r_N \wedge r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp \left(-n_N \frac{2l(N-l+1)}{N(N-1)} \right) \\
 J_N(r) &:= \binom{N}{r}^{-1} \sum_{l \in \llbracket (r_N \wedge r) + 1, r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp \left(-n_N \frac{2l(N-l+1)}{N(N-1)} \right)
 \end{aligned}$$

(of course such a quantity is null if the domain of the corresponding sum is empty). We also consider

$$\begin{aligned}
 H(N) &:= \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} H_N^K(r) \\
 I(N) &:= \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} I_N^K(r) \\
 J(N) &:= \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} J_N^K(r)
 \end{aligned}$$

Taking into account with $p = 3$ the bound

$$\forall p \in \mathbb{N}^*, \forall (t_i)_{i \in \llbracket 1, p \rrbracket} \in \mathbb{R}_+^p, \left(\sum_{i \in \llbracket 1, p \rrbracket} t_i \right)^K \leq p^{K-1} \sum_{i \in \llbracket 1, p \rrbracket} t_i^K \tag{10}$$

the next three technical results complete the proof of Theorem 1.

Lemma 7. *We have*

$$\lim_{N \rightarrow \infty} H(N) = 0$$

Proof. Since p is a fixed integer, by using (10), we can write that for any $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$,

$$\begin{aligned}
 H_N^K(r) &\leq \left(\binom{N}{r}^{-1} \sum_{l \in \llbracket 0, p \wedge r \rrbracket} \binom{N}{l} \exp \left(-n_N \frac{2l(N-l+1)}{N(N-1)} \right) \right)^K \\
 &\leq p^{K-1} \binom{N}{r}^{-K} \sum_{l \in \llbracket 0, p \wedge r \rrbracket} \binom{N}{l}^K \exp \left(-Kn_N \frac{2l(N-l+1)}{N(N-1)} \right)
 \end{aligned}$$

Since $\beta < \alpha$, there exists a $N_0 \in \mathbb{N} \setminus \{0, 1\}$ (depending only on α, β and slightly on K) large enough such that for all integers $N \geq N_0$,

$$\forall l \in \llbracket 0, p \rrbracket, \quad Kn_N \frac{2l(N-l+1)}{N(N-1)} \geq l\beta \ln(N)$$

Thus for such N , we get

$$\begin{aligned} H(N) &\leq p^{K-1} \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r}^{1-K} \sum_{l \in \llbracket 0, p \wedge r \rrbracket} \binom{N}{l}^K N^{-\beta l} \\ &= p^{K-1} \sum_{l \in \llbracket 0, p \rrbracket} \binom{N}{l}^K N^{-\beta l} \sum_{r \in \llbracket 1 \vee l, \lfloor N/2 \rfloor \rrbracket} \binom{N}{r}^{1-K} \end{aligned}$$

To go on, we need to evaluate the last sum and the simplest way seems to divide it into two parts. Consider first $\sum_{r \in \llbracket \lfloor N/4 \rfloor + 1, \lfloor N/2 \rfloor \rrbracket} \binom{N}{r}^{1-K}$. Using Stirling's formula, it appears that we can find a constant $h > 0$ independent from N such that for any $r \in \llbracket \lfloor N/4 \rfloor + 1, \lfloor N/2 \rfloor \rrbracket$, $\binom{N}{r} \geq \exp(hN)$, so we get

$$\sum_{r \in \llbracket \lfloor N/4 \rfloor + 1, \lfloor N/2 \rfloor \rrbracket} \binom{N}{r}^{1-K} \leq N \exp(-(K-1)hN)$$

For the remaining sum, we note that since for any $r \in \llbracket 0, N \rrbracket$, we have $\binom{N}{r+1} = \frac{N-r}{r+1} \binom{N}{r}$, it appears that for N large enough and $r \in \llbracket 0, \lfloor N/4 \rfloor \rrbracket$, $\binom{N}{r+1} \geq 2 \binom{N}{r}$, so we get

$$\begin{aligned} \sum_{r \in \llbracket 1 \vee l, \lfloor N/4 \rfloor \rrbracket} \binom{N}{r}^{1-K} &\leq \binom{N}{1 \vee l}^{1-K} \sum_{r \in \llbracket 1 \vee l, \lfloor N/4 \rfloor \rrbracket} 2^{-(r-1 \vee l)(K-1)} \\ &\leq 2 \binom{N}{1 \vee l}^{1-K} \end{aligned}$$

Since for N large the quantity $N \exp(-(K-1)hN)$ is negligible with respect to $\binom{N}{1 \vee l}^{1-K}$, we get that the whole sum $\sum_{r \in \llbracket 1 \vee l, \lfloor N/2 \rfloor \rrbracket} \binom{N}{r}^{1-K}$ is also of order $\binom{N}{1 \vee l}^{1-K}$. By consequence to obtain the convergence announced in the above lemma, it is sufficient to show that

$$\lim_{N \rightarrow \infty} \binom{N}{1}^{1-K} + \sum_{l \in \llbracket 1, p \rrbracket} \binom{N}{l} N^{-\beta l} = 0$$

and this is immediate because for any fixed l , $\binom{N}{l}$ is of polynomial order N^l and $\beta > 1$. ■

Lemma 8. *We have*

$$\lim_{N \rightarrow \infty} I(N) = 0$$

Proof. Applying the Hölder inequality to the probability on $\llbracket 0, r \rrbracket$ given by

$$\left(\binom{N}{r}^{-1} \left(\binom{N}{l} - \binom{N}{l-1} \right) \right)_{l \in \llbracket 0, r \rrbracket}$$

we obtain that for any $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$,

$$\begin{aligned} I_N^K(r) &\leq \binom{N}{r}^{-1} \sum_{l \in \llbracket (p \wedge r) + 1, r_N \wedge r \rrbracket} \left(\binom{N}{l} - \binom{N}{l-1} \right) \exp \left(-Kn_N \frac{2l(N-l+1)}{N(N-1)} \right) \\ &\leq \binom{N}{r}^{-1} \sum_{l \in \llbracket (p \wedge r) + 1, r_N \wedge r \rrbracket} \binom{N}{l} \exp \left(-Kn_N \frac{2l(N-l+1)}{N(N-1)} \right) \end{aligned}$$

Due to our choice of β , for N large enough, we have

$$\forall l \in \llbracket 1, r_N \rrbracket, \quad Kn_N \frac{2l(N-l+1)}{N(N-1)} \geq \beta l \ln(N)$$

and thus we get for N such that $r_N \geq p$,

$$\begin{aligned} I(N) &\leq \sum_{r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket} \sum_{l \in \llbracket (p \wedge r) + 1, r_N \wedge r \rrbracket} \binom{N}{l} \exp(-\beta l \ln(N)) \\ &\leq \lfloor N/2 \rfloor \sum_{l \in \llbracket p+1, r_N \rrbracket} a_N(l) \end{aligned}$$

with $a_N(l) := \binom{N}{l} N^{-\beta l}$. We compute that for $l \in \llbracket p+1, r_N \rrbracket$,

$$\begin{aligned} \frac{a_N(l+1)}{a_N(l)} &= \frac{N-l}{l+1} N^{-\beta} \\ &\leq N^{1-\beta} \\ &\leq \frac{1}{2} \end{aligned}$$

again for N large enough. It follows that for all such N ,

$$\begin{aligned} I(N) &\leq \frac{N}{2} 2a_N(p+1) \\ &\leq N \frac{N^{p+1}}{(p+1)!} N^{-\beta(p+1)} \end{aligned}$$

and the wanted convergence follows from the fact that $(\beta - 1)(p + 1) > 1$. ■

Lemma 9. *We have*

$$\lim_{N \rightarrow \infty} J(N) = 0$$

Proof. Let $\chi \in (0, \alpha\eta(1 - \eta))$ be fixed (recall that $\eta \in (0, 1)$), we have for all N large enough,

$$\begin{aligned} \forall l \in \llbracket r_N, \lfloor N/2 \rfloor \rrbracket, \quad Kn_N \frac{2l(N-l+1)}{N(N-1)} &\geq Kn_N \frac{2r_N(N-r_N+1)}{N(N-1)} \\ &= 2K \left\lfloor \frac{\alpha N \ln(N)}{2K} \right\rfloor \frac{\lfloor \eta N \rfloor (N+1 - \lfloor \eta N \rfloor)}{N(N-1)} \\ &\geq \chi N \ln(N) \end{aligned}$$

Thus we get that for all such N and all $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$, $J_N(r) \leq \exp(-\chi N \ln(N))$ ($J_N(r)$ is even null if $r \leq r_N$). It follows that

$$\begin{aligned} J(N) &\leq \exp(-\chi N \ln(N)) \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} \\ &\leq \exp(-\chi N \ln(N)) \sum_{r \in \llbracket 0, N \rrbracket} \binom{N}{r} \\ &= 2^N \exp(-\chi N \ln(N)) \end{aligned}$$

and the announced convergence is immediate. ■

We end this section with three remarks.

Remark 10. Note that the last expression in Lemma 6 is the one we would have got if we had decided to work with continuous time Markov processes (where the time periods $[n, n + 1]$, $n \in \mathbb{N}$ are replaced by independent exponential waiting times) instead of discrete time Markov chains. More precisely, for $k \in \llbracket 1, K \rrbracket$, let $(\xi_n^{(k)})_{n \in \mathbb{N}^*}$ be independent sequences of independent exponential variables of parameter 1 (which are furthermore assumed to be independent from the chains $Z^{(1)}, \dots, Z^{(k)}$). We denote

$$\forall k \in \llbracket 1, K \rrbracket, \forall n \in \mathbb{N}, \quad \tau_n^{(k)} := \sum_{m \in \llbracket 1, n \rrbracket} \xi_m^{(k)}$$

(in particular $\tau_0^{(k)} = 0$) and we consider the Markov processes $\bar{Z}^{(1)}, \dots, \bar{Z}^{(K)}$ constructed via

$$\forall k \in \llbracket 1, K \rrbracket, \forall t \geq 0, \quad \bar{Z}_t^{(k)} := Z_n^{(k)} \quad \text{if } t \in [\tau_n^{(k)}, \tau_{n+1}^{(k)})$$

All notions discussed in the introduction can be extended to this continuous time setting and then Theorems 1 and 2 are also satisfied. Indeed it is easy to pass directly from discrete to continuous times (and conversely), using the strong law of large numbers which asserts that a.s.

$$\forall k \in \llbracket 1, K \rrbracket, \quad \lim_{n \rightarrow \infty} \frac{\tau_n^{(k)}}{n} = 1$$

The same kind of considerations enables us to justify the assertion made before Theorem 1. Assume more generally that Theorem 1 is satisfied with some times $T(N, K)$ by the chains constructed with the help of some probability measures μ . Next modify the latters through the transformations $\tilde{\mu} := (1 - \epsilon_N)\mu + \epsilon_N \delta_l$ with $\epsilon_N \in [0, 1]$. Suppose that the limit $l := \lim_{N \rightarrow \infty} \epsilon_N$ exists in $[0, 1)$. Then Theorem 1 is also valid for the chains constructed by rather using $\tilde{\mu}$, but with the times $\tilde{T}(N, K) := T(N, K)/(1 - l)$. In particular if $l = 0$, we obtain what was announced before Theorem 1 for the slightly slowed down uniform transposition generating chains. □

Remark 11. To estimate the quantity (7), we used the $E^{(r)}$ -valued Markov chains defined in (8). But a priori one could have thought of simpler Markov chains: for $r \in \llbracket 1, \lfloor N/2 \rfloor \rrbracket$ define

$$\forall n \in \mathbb{N}, \quad V_n^{(r)} := \text{card}(\{1, \dots, r\} \cap Z_n(\{1, \dots, r\}))$$

It is a birth and death chain on $\llbracket(2r - N)_+, r\rrbracket$ and let $Q^{(r)}$ be its transition matrix. Then the quantity we are interested in can be written as

$$\begin{aligned} \mathbb{P}[Z_{n_N}(\{1, \dots, r\}) = \{1, \dots, r\}] &= \mathbb{P}[V_{n_N}^{(r)} = r] \\ &= Q_{n_N}^{(r)}(r, r) \end{aligned}$$

Unfortunately, due to the lack of symmetry of this chain, the latter term is not so easy to evaluate in term of the spectrum of $Q^{(r)}$, in particular it is not equal to $\text{tr}(Q_{n_N}^{(r)})/N$, at least if $2r \leq N$. To be convinced by this assertion, note that since $Q^{(r)}$ is an irreducible birth and death transition matrix, it is diagonalizable and its eigenvalues have multiplicity one. Furthermore since the Markov chain $V^{(r)}$ is a function of the Markov chain $R^{(r)}$, the eigenvalues of $Q^{(r)}$ are also eigenvalues of $P^{(r)}$. It follows that if $2r \leq N$, the $r+1$ eigenvalues of $Q^{(r)}$ are exactly those of $P^{(r)}$. \square

Remark 12. The arguments given in this section and in the previous one can be slightly extended to show that the cut-off phenomena for the non-existence of a fixed point and transitivity are indeed unique transitions in the sense given in (2) and (3). \square

4. FIXED POINTS FOR THE NEIGHBOR GENERATING TRANSPOSITIONS

The goal of this section is to prove Theorem 2, namely that there is a flared transition phenomenon for the existence of a fixed point in the neighbor generating transposition model. Our approach is very simple in its principle: try to extract as much information as possible from the evaluation of the expectation and the variance of the sum of the indicator functions associated to fixed points.

So the sums defined by

$$\forall n \in \mathbb{N}, \quad S_n := \sum_{x \in E_N} \mathbb{1}_{B_n(x)}$$

will play an important role here. Their expectations are not difficult to compute:

Lemma 13. *We have at any time $n \in \mathbb{N}$,*

$$\mathbb{E}[S_n] = N \left(\frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \left(1 + \frac{2}{N} \left(\cos \left(\frac{2\pi l}{N} \right) - 1 \right) \right)^n \right)^K$$

and in particular for $N \geq 4$, the mapping $\mathbb{N} \ni n \mapsto \mathbb{E}[S_n]$ is nonincreasing.

Proof. By definition, we have

$$\begin{aligned} \mathbb{E}[S_n] &= \sum_{x \in E_N} \mathbb{P}[B_n(x)] \\ &= \sum_{x \in E_N} \mathbb{P}[Z_n(x) = x]^K \end{aligned}$$

Fix $x \in E_N$ and consider the stochastic chain $(X_n)_{n \in \mathbb{N}} := (Z_n(x))_{n \in \mathbb{N}}$. It is indeed a Markov chain on $\mathbb{Z}/(N\mathbb{Z})$ starting from x and whose transition matrix P is given by

$$\forall x, y \in E_N, \quad P(x, y) := \begin{cases} \frac{1}{N}, & \text{if } d(x, y) = 1 \\ 1 - \frac{2}{N}, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases}$$

where d is the natural graph distance on the discrete circle $\mathbb{Z}/(N\mathbb{Z})$. So we can write $P = \frac{2}{N}M + (1 - \frac{2}{N})\text{Id}$ where M is the transition matrix of the usual random walk on $\mathbb{Z}/(N\mathbb{Z})$. Its spectral decomposition is well-known (see for instance the book of Diaconis [5]): the eigenvalues are the quantities $\cos\left(\frac{2\pi l}{N}\right)$, for $l \in \llbracket 0, \lfloor N/2 \rfloor \rrbracket$. For $l \neq 0, N/2$, the corresponding multiplicity is 2 and the eigenspace is generated by the real and imaginary parts of the complex-valued function $E_N \ni x \mapsto \exp(i2\pi lx/N)$. For $l = 0$ and $l = N/2$ (which occurs only if N is even, then M is periodic with period 2), the multiplicity is 1. We deduce that the eigenvalues of P , with multiplicity, are the numbers $1 + \frac{2}{N} \left(\cos\left(\frac{2\pi l}{N}\right) - 1\right)$, for $l \in \llbracket 0, N - 1 \rrbracket$.

Note furthermore that P is space-homogeneous (namely, is invariant by the translations of $\mathbb{Z}/(N\mathbb{Z})$), so we get that for any $n \in \mathbb{N}$ and $x \in E_N$,

$$\begin{aligned} \mathbb{P}[Z_n(x) = x] &= P_n(x, x) \\ &= \frac{1}{N} \sum_{y \in E_N} P_n(y, y) \\ &= \frac{1}{N} \text{tr}(P_n) \\ &= \frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \left(1 + \frac{2}{N} \left(\cos\left(\frac{2\pi l}{N}\right) - 1\right)\right)^n \end{aligned}$$

and this leads to the formula of the above lemma. The monotonicity is a consequence of the fact that the eigenvalues of P are nonnegative for N larger than 4. ■

Next result shows that it is at times n of order $N^{1+\frac{2}{K}}$ that something interesting is happening for $\mathbb{E}[S_n]$.

Lemma 14. *Let fix $\alpha \in (0, +\infty)$ and define $n_N := \lfloor \alpha N^{1+\frac{2}{K}} \rfloor$. Then we have*

$$\lim_{N \rightarrow \infty} \mathbb{E}[S_{n_N}] = I^K(\alpha)$$

with

$$I(\alpha) := \frac{1}{2\sqrt{\pi\alpha}}$$

Proof. According to the previous lemma, we have to show that

$$\lim_{N \rightarrow \infty} \frac{1}{N^{1-\frac{1}{K}}} \sum_{l \in \llbracket 0, N-1 \rrbracket} \left(1 + \frac{2}{N} \left(\cos\left(\frac{2\pi l}{N}\right) - 1\right)\right)^{n_N} = I(\alpha)$$

Reinterpreting $\llbracket 0, N - 1 \rrbracket$ as $\mathbb{Z}/(N\mathbb{Z})$, we decompose the above sum into

$$I_1(N) := \frac{1}{N^{1-\frac{1}{k}}} \sum_{l \in Z_1(N)} \left(1 + \frac{2}{N} \left(\cos \left(\frac{2\pi l}{N} \right) - 1 \right) \right)^{nN}$$

$$I_2(N) := \frac{1}{N^{1-\frac{1}{k}}} \sum_{l \in Z_2(N)} \left(1 + \frac{2}{N} \left(\cos \left(\frac{2\pi l}{N} \right) - 1 \right) \right)^{nN}$$

with

$$Z_1(N) := \{l \in \mathbb{Z}/(N\mathbb{Z}) : d(0, l) \leq \epsilon_N N\}$$

$$Z_2(N) := \{l \in \mathbb{Z}/(N\mathbb{Z}) : d(0, l) > \epsilon_N N\}$$

where the sequence $(\epsilon_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ has been chosen such that

$$\lim_{N \rightarrow \infty} \epsilon_N = 0$$

$$\lim_{N \rightarrow \infty} \epsilon_N N^{\frac{1}{k}} = +\infty$$

The first condition insures that for large N , $I_1(N)$ is equivalent to

$$\frac{1}{N^{1-\frac{1}{k}}} \sum_{l \in Z_1(N)} \exp(-4\pi^2 \alpha l^2 N^{\frac{2}{k}-2})$$

and we recognize a Riemann type sum. More precisely, we bound this sum below and above respectively by

$$\frac{1}{N^{1-\frac{1}{k}}} + 2 \int_{N^{\frac{1}{k}-1}}^{(\lfloor \epsilon_N N \rfloor + 1) N^{\frac{1}{k}-1}} \exp(-4\pi^2 \alpha s^2) ds$$

and

$$\frac{1}{N^{1-\frac{1}{k}}} + 2 \int_0^{\lfloor \epsilon_N N \rfloor N^{\frac{1}{k}-1}} \exp(-4\pi^2 \alpha s^2) ds$$

Due to our second assumption on the sequence $(\epsilon_N)_{N \in \mathbb{N} \setminus \{0,1\}}$, both quantities converge for large N toward

$$\int_{\mathbb{R}} \exp(-4\pi^2 \alpha s^2) ds = \frac{1}{2\sqrt{\pi\alpha}}$$

So to prove the announced result, it is sufficient to see that

$$\lim_{N \rightarrow \infty} I_2(N) = 0$$

Using the concavity inequality $\ln(1 + s) \leq s$, valid for all $s \in (-1, +\infty)$ and the fact that there exists a constant $c > 0$ such that $\cos(s) - 1 \leq -cs^2$ for all $s \in [0, \pi]$, we have

$$I_2(N) \leq 2 \sum_{l \in \llbracket \lfloor \epsilon_N N \rfloor + 1, \lfloor N/2 \rfloor + 1 \rrbracket} \exp(-8\pi^2 \alpha c l^2 N^{\frac{2}{k}-2})$$

$$\leq 2 \int_{\lfloor \epsilon_N N \rfloor N^{1-\frac{1}{k}}}^{+\infty} \exp(-8\pi^2 \alpha c s^2) ds$$

and it is clear that the latter integral goes to zero as N becomes large. ■

We deduce the following result on the existence of a fixed point at large times with respect to the order $N^{1+\frac{2}{k}}$, which corresponds to the easy part of Theorem 2:

Corollary 15. *Consider for $N \in \mathbb{N} \setminus \{0, 1\}$, times of the type $n_N := \lfloor \alpha_N N^{1+\frac{2}{k}} \rfloor$, with $\alpha_N > 0$, and denote $\underline{\alpha} := \liminf_{N \rightarrow \infty} \alpha_N$. Then we have*

$$\limsup_{N \rightarrow \infty} \mathbb{P}[B_{n_N}] \leq I^K(\underline{\alpha})$$

with the convention $I(+\infty) = 0$, so that $\lim_{N \rightarrow \infty} \mathbb{P}[B_{n_N}] = 0$ if $\underline{\alpha} = +\infty$. Furthermore under the assumption $\underline{\alpha} > \alpha' := \frac{1}{4\pi}$, we get

$$\limsup_{N \rightarrow \infty} \mathbb{P}[B_{n_N}] < 1$$

Proof. Since we have for any time $n \in \mathbb{N}$,

$$\begin{aligned} \mathbb{P}[B_n] &\leq \sum_{x \in E_N} \mathbb{P}[B_n(x)] \\ &= \mathbb{E}[S_n] \end{aligned}$$

the first bound will be proven if we show that

$$\lim_{N \rightarrow \infty} \mathbb{E}[S_{n_N}] \leq I^K(\underline{\alpha}) \tag{11}$$

Consider $\alpha < \underline{\alpha}$ and define $n_N(\alpha) := \alpha N^{1+\frac{2}{k}}$. Due to Lemma 14 and to the monotonicity property alluded to in Lemma 13, we have

$$\begin{aligned} \limsup_{N \rightarrow \infty} \mathbb{E}[S_{n_N}] &\leq \limsup_{N \rightarrow \infty} \mathbb{E}[S_{n_N(\alpha)}] \\ &= I^K(\alpha) \end{aligned}$$

Next letting $\alpha \rightarrow \underline{\alpha}$ by below, (11) follows.

Concerning the last assertion, it comes from the fact that defining

$$\alpha' := \inf\{\alpha > 0 : I(\alpha) = 1\} = \frac{1}{4\pi}$$

we have $I(\alpha) < 1$ for any $\alpha > \alpha'$. ■

To proceed with our program, we also need to evaluate the variance of S_n and this amounts to get estimates on $\mathbb{P}[Z_n(x) = x, Z_n(y) = y]$ for $x \neq y \in E_N$. Indeed, we have for any time $n \in \mathbb{N}$,

$$\begin{aligned} \text{Var}(S_n) &= \mathbb{E}[S_n^2] - \mathbb{E}^2[S_n] \\ &= \sum_{x, y \in E_N} \mathbb{P}[B_n(x) \cap B_n(y)] - \mathbb{E}^2[S_n] \\ &= \sum_{x \neq y \in E_N} \mathbb{P}[B_n(x) \cap B_n(y)] + \sum_{x \in E_N} \mathbb{P}[B_n(x)] - \mathbb{E}^2[S_n] \\ &= \sum_{x \neq y \in E_N} \mathbb{P}^K[Z_n(x) = x, Z_n(y) = y] + \mathbb{E}[S_n] - \mathbb{E}^2[S_n] \end{aligned} \tag{12}$$

Contrary to the uniform generating transposition model, the quantity $\mathbb{P}[Z_n(x) = x, Z_n(y) = y]$ now depends on $x \neq y \in E_N$, but only through the distance $d(x, y)$, due to the underlying space homogeneity of our present model.

First we try to obtain a bound via a coupling argument. Fix $x \neq y \in E_N$ and denote $(X_n, Y_n)_{n \in \mathbb{N}} := (Z_n(x), Z_n(y))_{n \in \mathbb{N}}$ which is a stochastic chain starting from (x, y) and taking values in $E_N^{(2)} := E_N^2 \setminus \{(x, x) : x \in E_N\}$. Recalling that $Z_n(x) = z$ means that x is in position z , it appears that $(X_n, Y_n)_{n \in \mathbb{N}}$ is a Markov chain whose transition matrix $P^{(2)}$ is given by

$$\forall (x, y), (x', y') \in E_N^{(2)}, \quad P^{(2)}((x, y), (x', y')) = \begin{cases} \frac{1}{N}, & \text{if } d(x, x') = 1 \text{ and } y' = y \\ \frac{1}{N}, & \text{if } x' = x \text{ and } d(y, y') = 1 \\ \frac{1}{N}, & \text{if } d(x, y) = 1, x' = y \text{ and } y' = x \\ 1 - \frac{4}{N}, & \text{if } d(x, y) > 1, x' = x \text{ and } y' = y \\ 1 - \frac{3}{N}, & \text{if } d(x, y) = 1, x' = x \text{ and } y' = y \\ 0, & \text{otherwise} \end{cases}$$

The form of this matrix suggests to consider another transition matrix $\tilde{P}^{(2)}$ where the main interaction between the two components has been removed, namely

$$\forall (x, y), (x', y') \in E_N^2, \quad \tilde{P}^{(2)}((x, y), (x', y')) = \begin{cases} \frac{1}{N}, & \text{if } d(x, x') + d(y, y') = 1 \\ 1 - \frac{4}{N}, & \text{if } x' = x \text{ and } y' = y \\ 0, & \text{otherwise} \end{cases}$$

Its interest is that we can evaluate its powers:

Lemma 16. *We have for any $N \geq 9$, any $(x, y) \in E_N^2$ and $n \in \mathbb{N}$,*

$$\left(1 + \frac{144}{N^2}\right)^{-n} \left(\frac{\mathbb{E}[S_n]}{N}\right)^{\frac{2}{K}} \leq \tilde{P}_n^{(2)}((x, y), (x, y)) \leq \left(\frac{\mathbb{E}[S_n]}{N}\right)^{\frac{2}{K}}$$

In particular in the time scale we are interested in, since $K \geq 3$, we have for any given $\alpha > 0$, as N goes to infinity,

$$\tilde{P}_{\lfloor \alpha N^{1+\frac{2}{K}} \rfloor}^{(2)}((x, y), (x, y)) \sim I^2(\alpha) \frac{1}{N^{\frac{2}{K}}}$$

Proof. The evolution according to $\tilde{P}^{(2)}$ can be described in the following way: first we choose one of the factor of E_N^2 with a chance one half each, next we make the corresponding coordinate evolve according to the kernel \hat{P} defined by

$$\forall x, y \in E_N, \quad \hat{P}(x, y) := \begin{cases} \frac{2}{N}, & \text{if } d(x, y) = 1 \\ 1 - \frac{4}{N}, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases}$$

So conditioning on the number of times the first factor has been chosen, we get that for any $m \in \mathbb{N}$,

$$\forall (x, y), (x', y') \in E_N^2, \quad \tilde{P}_n^{(2)}((x, y), (x', y')) = \frac{1}{2^n} \sum_{p=0}^n \binom{n}{p} \widehat{P}_p(x, x') \widehat{P}_{n-p}(y, y')$$

with the convention $\widehat{P}_0 := \text{Id}$. In particular, for any $m \in \mathbb{N}$ and $(x, y) \in E_N^2$,

$$\tilde{P}_n^{(2)}((x, y), (x, y)) = \frac{1}{2^n} \sum_{p=0}^n \binom{n}{p} \widehat{P}_p(x, x) \widehat{P}_{n-p}(y, y)$$

Due to the space-homogeneity of the transition matrix \widehat{P} (with E_N identified with $\mathbb{Z}/(N\mathbb{Z})$), for any $p \in \mathbb{N}$, the quantity $P_p(x, x)$ does not depend on the choice of $x \in \mathbb{Z}/(N\mathbb{Z})$ and thus we have

$$\begin{aligned} \forall x \in \mathbb{Z}/(N\mathbb{Z}), \quad \widehat{P}_p(x, x) &= \frac{1}{N} \text{tr}(\widehat{P}_p) \\ &= \frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \widehat{\theta}_l^p \end{aligned}$$

where $(\widehat{\theta}_l)_{l \in \llbracket 0, N-1 \rrbracket}$ are the eigenvalues (with multiplicities) of \widehat{P} . The proof of Lemma 13 shows that we can take

$$\forall l \in \llbracket 0, N-1 \rrbracket, \quad \widehat{\theta}_l = 1 + \frac{4}{N} \left(\cos\left(\frac{2\pi l}{N}\right) - 1 \right)$$

Putting together these considerations, it appears that for any $n \in \mathbb{N}$ and $(x, y) \in E_N^2$,

$$\begin{aligned} \tilde{P}_n^{(2)}((x, y), (x, y)) &= \frac{1}{2^n} \sum_{p=0}^n \binom{n}{p} \frac{1}{N^2} \sum_{k, l \in \llbracket 0, N-1 \rrbracket} \widehat{\theta}_k^p \widehat{\theta}_l^{n-p} \\ &= \frac{1}{N^2} \sum_{k, l \in \llbracket 0, N-1 \rrbracket} \frac{1}{2^n} \sum_{p=0}^n \binom{n}{p} \widehat{\theta}_k^p \widehat{\theta}_l^{n-p} \\ &= \frac{1}{N^2} \sum_{k, l \in \llbracket 0, N-1 \rrbracket} \left(\frac{\widehat{\theta}_k + \widehat{\theta}_l}{2} \right)^n \end{aligned}$$

For $l \in \llbracket 0, N-1 \rrbracket$, let $\lambda_l := 2(\cos(2\pi l/N) - 1)/N$, so that $\widehat{\theta}_l = 1 + 2\lambda_l$. These quantities are nonpositive, so we get that for any $k, l \in \llbracket 0, N-1 \rrbracket$, $1 + \lambda_k + \lambda_l \leq (1 + \lambda_k)(1 + \lambda_l)$ and

$$\begin{aligned} \tilde{P}_n^{(2)}((x, y), (x, y)) &= \frac{1}{N^2} \sum_{k, l \in \llbracket 0, N-1 \rrbracket} (1 + \lambda_k + \lambda_l)^n \\ &\leq \left(\frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} (1 + \lambda_l)^n \right)^2 \\ &= \left(\frac{\mathbb{E}[S_n]}{N} \right)^2 \end{aligned}$$

according to Lemma 13.

Furthermore, since we have for any $l \in \llbracket 0, N - 1 \rrbracket$, $-\frac{4}{N} \leq \lambda_l \leq 0$, it appears that for any $k, l \in \llbracket 0, N - 1 \rrbracket$,

$$\begin{aligned} (1 + \lambda_k)(1 + \lambda_l) &= 1 + \lambda_l + \lambda_k + \lambda_k \lambda_l \\ &\leq 1 + \lambda_l + \lambda_k + \frac{16}{N^2} \\ &\leq \left(1 + \frac{16}{N^2} \left(1 - \frac{8}{N}\right)^{-1}\right) (1 + \lambda_l + \lambda_k) \\ &\leq \left(1 + \frac{16 \times 9}{N^2}\right) (1 + \lambda_l + \lambda_k) \end{aligned}$$

and the wanted lower bound follows.

The announced equivalence is an immediate consequence of Lemma 14 and of the fact that for fixed $K \geq 3$ and $\alpha > 0$,

$$\lim_{N \rightarrow \infty} \left(1 + \frac{144}{N^2}\right)^{\lfloor \alpha N^{1+\frac{2}{K}} \rfloor} = 1$$

■

Note that if in (12) we could replace the term $\mathbb{P}[Z_n(x) = x, Z_n(y) = y] = P_n^{(2)}((x, y), (x, y))$ by $\tilde{P}_n^{(2)}((x, y), (x, y))$, we could bound below and above the variance by

$$\begin{aligned} -\left(1 - \frac{N(N-1)(N-8)}{N^3}\right) \mathbb{E}^2[S_n] + \mathbb{E}[S_n] &\leq \text{Var}(S_n) \\ &\leq -\left(1 - \frac{N(N-1)}{N^2}\right) \mathbb{E}^2[S_n] + \mathbb{E}[S_n] \end{aligned}$$

(at least for $N \geq 9$). Taking into account Lemma 14, we could then conclude to the

Proposition 17. *Take $K \geq 3$ and consider times of the kind $n_N := \lfloor \alpha_N N^{1+\frac{2}{K}} \rfloor$, where $(\alpha_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ is a sequence of positive numbers converging to $\alpha \in [0, +\infty)$. Assume that*

$$\lim_{N \rightarrow \infty} \alpha_N N^{\frac{2(K-2)}{(4K-1)K}} = +\infty \tag{13}$$

(in particular this is automatic if $\alpha > 0$), then we have

$$\lim_{N \rightarrow \infty} \frac{\text{Var}(S_{n_N})}{\mathbb{E}^2[S_{n_N}]} = I^{-K}(\alpha)$$

with the convention $I^{-K}(0) = 0$.

This result will be the crucial estimate to complete the proof of the transition phenomenon alluded to in Theorem 2.

But let us first prove the above proposition by comparing the powers of $P^{(2)}$ with those of $\tilde{P}^{(2)}$. To go in this direction, it is convenient to introduce $(\tilde{X}_n, \tilde{Y}_n)_{n \in \mathbb{N}}$ a Markov chain on E_N^2 starting from (x, y) and admitting $\tilde{P}^{(2)}$ as transition matrix. Consider

$$\tilde{\tau} := \inf\{n \in \mathbb{N} : d(\tilde{X}_n, \tilde{Y}_n) \leq 1\} \quad \text{and} \quad \tau := \inf\{n \in \mathbb{N} : d(X_n, Y_n) \leq 1\}$$

Since $P^{(2)}$ and $\tilde{P}^{(2)}$ coincide on the lines corresponding to couples $(x', y') \in E_N^2$ such that $d(x', y') > 1$ and since the chains $(X_n, Y_n)_{n \in \mathbb{N}}$ and $(\tilde{X}_n, \tilde{Y}_n)_{n \in \mathbb{N}}$ start from the same couple (x, y) , the laws of $(\tau, (X_n, Y_n)_{n < \tau})$ and $(\tilde{\tau}, (\tilde{X}_n, \tilde{Y}_n)_{n < \tilde{\tau}})$ are the same. It follows that

$$\begin{aligned} & \sum_{(x', y') \in E_N^2} |P_n^{(2)}((x, y), (x', y')) - \tilde{P}_n^{(2)}((x, y), (x', y'))| \\ &= \sum_{(x', y') \in E_N^2} |\mathbb{P}[(X_n, Y_n) = (x', y')] - \mathbb{P}[(\tilde{X}_n, \tilde{Y}_n) = (x', y')]| \\ &= \sum_{(x', y') \in E_N^2} |\mathbb{P}[(X_n, Y_n) = (x', y'), \tau \leq n] - \mathbb{P}[(\tilde{X}_n, \tilde{Y}_n) = (x', y'), \tilde{\tau} \leq n]| \\ &\leq \sum_{(x', y') \in E_N^2} \mathbb{P}[(X_n, Y_n) = (x', y'), \tau \leq n] + \mathbb{P}[(\tilde{X}_n, \tilde{Y}_n) = (x', y'), \tilde{\tau} \leq n] \\ &= \mathbb{P}[\tau \leq n] + \mathbb{P}[\tilde{\tau} \leq n] \\ &= 2\mathbb{P}[\tilde{\tau} \leq n] \end{aligned} \tag{14}$$

The next result enables to evaluate the r.h.s. in the time scale we are interested in:

Lemma 18. *There exists a universal constant $c > 0$ such that $\tilde{\tau}$ is stochastically bounded below by an exponential random variable of parameter $c/(L^2N)$, where $N \geq 8$ and $L := d(x, y) \geq 2$.*

Proof. Define for $n \in \mathbb{N}$, $V_n := d(\tilde{X}_n, \tilde{Y}_n)$. It appears easily that $V := (V_n)_{n \in \mathbb{N}}$ is a birth and death Markov chain on $\llbracket 0, \lfloor N/2 \rfloor \rrbracket$, starting from $L \geq 2$. If $N \geq 8$ is even, its transition matrix \check{P} is given by

$$\forall x, y \in \llbracket 0, N/2 \rrbracket, \quad \check{P}(x, y) := \begin{cases} \frac{2}{N}, & \text{if } x \notin \{0, N/2\} \text{ and } |y - x| = 1 \\ \frac{4}{N}, & \text{if } x \in \{0, N/2\} \text{ and } |y - x| = 1 \\ 1 - \frac{4}{N}, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases}$$

(if $N \geq 8$ is odd, this transition matrix has to be slightly modified: $\check{P}((N-1)/2, (N-3)/2) = 2/N$ and $\check{P}((N-1)/2, (N-1)/2) = 1 - 2/N$). Then we have

$$\tilde{\tau} := \inf\{n \in \mathbb{N} : V_n = 1\}$$

To come back to a well-known absorbing problem, consider the new transition matrix \check{P} on $\llbracket 1, L \rrbracket$ given by

$$\forall x, y \in \llbracket 1, L \rrbracket, \quad \check{P}(x, y) := \begin{cases} \frac{2}{N}, & \text{if } x \notin \{1, L\} \text{ and } |y - x| = 1 \\ \frac{4}{N}, & \text{if } x = L \text{ and } y = L - 1 \\ 1 - \frac{4}{N}, & \text{if } x = y \neq 1 \\ 0, & \text{otherwise} \end{cases}$$

Let $U := (U_n)_{n \in \mathbb{N}}$ be a corresponding Markov chain starting from L (note that it is absorbed at 1). It is not difficult to construct a coupling of V and U such that

$$\forall n \leq \tilde{\tau}, \quad U_n \leq V_n$$

This shows that $\tilde{\tau}$ is stochastically bounded below by

$$\check{\tau} := \inf\{n \in \mathbb{N} : U_n = 1\}$$

The advantage of the latter absorption time is that its distribution is well-known (see Karlin and McGregor [11]): let $(\check{\theta}_l)_{l \in \llbracket 1, L-1 \rrbracket}$ be the nonzero eigenvalues of \check{P} , if they are all nonnegative then $\check{\tau}$ is distributed as a sum of independent geometric random variables of respective parameters the family $(\check{\theta}_l)_{l \in \llbracket 1, L-1 \rrbracket}$. In our situation these eigenvalues are known (see for instance the last example of Diaconis and Miclo [8]):

$$\forall l \in \llbracket 1, L-1 \rrbracket, \quad \check{\theta}_l = 1 + \frac{4}{N} \left(\cos \left(\frac{\pi(2l-1)}{2(L-1)} \right) - 1 \right)$$

It follows that $\check{\tau}$ is stochastically bounded below by $\check{\tau}_1$ geometric random variable of parameter $\check{\theta}_1$, which means that

$$\forall n \in \mathbb{N}^*, \quad \mathbb{P}[\check{\tau}_1 = n] = (1 - \check{\theta}_1)\check{\theta}_1^{n-1}$$

The random variable $\check{\tau}_1$ is itself stochastically bounded below by an exponential random variable of parameter $\ln(1/\check{\theta}_1)$.

The result announced in the above lemma then comes from the existence of a constant $c > 0$ such that for any $N \geq 8$ and $L \geq 2$,

$$\ln(1/\check{\theta}_1) \leq \frac{c}{L^2 N}$$

■

The next result gives an evaluation of the error made by replacing $P^{(2)}$ by $\tilde{P}^{(2)}$ on the time interval we are interested in.

Lemma 19. *Let $c > 0$ be the constant defined in the previous lemma and let $n \in \mathbb{N}$ and $L \in \llbracket 2, \lfloor N/2 \rfloor \rrbracket$ be given. For $N \geq 8$, we have*

$$\max_{m \in \llbracket 0, n \rrbracket, x, y \in \mathbb{Z}/(N\mathbb{Z}) : d(x, y) \geq L} \left| P_m^{(2)}((x, y), (x, y)) - \tilde{P}_m^{(2)}((x, y), (x, y)) \right| \leq \frac{2cn}{NL^2}$$

Consider times of the kind $n_N := \lfloor \alpha_N N^{1+\frac{2}{k}} \rfloor$, where $(\alpha_N)_{N \in \mathbb{N} \setminus \{0, 1\}}$ is a sequence of positive numbers, and take $L_N := \alpha_N^{\frac{1}{4}} N^{\frac{1}{2} + \frac{1}{k}}$. Assume either that $\lim_{N \rightarrow \infty} \alpha_N = 0$ or that $K \geq 3$ and that the sequence $(\alpha_N)_{N \in \mathbb{N} \setminus \{0, 1\}}$ converges to some $\alpha > 0$, then we have for large N ,

$$\sum_{x, y \in \mathbb{Z}/(N\mathbb{Z}) : d(x, y) \geq L_N} (P_{n_N}^{(2)}((x, y), (x, y)))^K \sim \sum_{x \neq y \in \mathbb{Z}/(N\mathbb{Z})} (\tilde{P}_{n_N}^{(2)}((x, y), (x, y)))^K$$

Proof. According to (14), we have for any $m \in \llbracket 0, n \rrbracket$ and any $x, y \in \mathbb{Z}/(N\mathbb{Z})$ such that $d(x, y) \geq L$,

$$\begin{aligned} |P_m^{(2)}((x, y), (x, y)) - \tilde{P}_m^{(2)}((x, y), (x, y))| &\leq 2\mathbb{P}[\tilde{\tau} \leq m] \\ &\leq 2\mathbb{P}[\tilde{\tau} \leq n] \\ &\leq 2\mathbb{P}\left[\frac{L_N^2 N}{c} \mathcal{E} \leq n\right] \end{aligned}$$

where the constant $c > 0$ is defined in Lemma 18 and where \mathcal{E} is an exponential random variable of parameter 1. So the latter probability is

$$\begin{aligned} \mathbb{P}\left[\mathcal{E} \leq \frac{c}{L_N^2 N} n\right] &= 1 - \exp\left(-\frac{c}{L_N^2 N} n\right) \\ &\leq \frac{c}{L_N^2 N} n \end{aligned}$$

where we used the convexity inequality $\exp(-s) \geq 1 - s$ valid for any $s \in \mathbb{R}$, and this leads to the announced bound.

Concerning the wanted equivalence, recall that in the r.h.s. the quantity $\tilde{P}_{n_N}^{(2)}((x, y), (x, y))$ does not depend on the couple $(x, y) \in E_N^2$. Lemma 16 shows that for large N ,

$$\begin{aligned} \tilde{P}_{n_N}^{(2)}((x, y), (x, y)) &= \tilde{P}_{n_N}^{(2)}((0, 0), (0, 0)) \\ &\sim \left(\frac{\mathbb{E}[S_{n_N}]}{N}\right)^{\frac{2}{k}} \end{aligned}$$

By our assumption on the times n_N , for $N \in \mathbb{N} \setminus \{0, 1\}$, we can find a constant $a > 0$ such that for any $N \in \mathbb{N} \setminus \{0, 1\}$, $n_N \leq aN^{1+\frac{2}{k}}$, and Lemma 13 and Lemma 14 imply that

$$\begin{aligned} \liminf_{N \rightarrow \infty} N^{\frac{2}{k}} \tilde{P}_{n_N}^{(2)}((0, 0), (0, 0)) &= \liminf_{N \rightarrow \infty} \mathbb{E}^{\frac{2}{k}}[S_{n_N}] \\ &\geq \liminf_{N \rightarrow \infty} \mathbb{E}^{\frac{2}{k}}[S_{aN^{1+\frac{2}{k}}}] \\ &= I^2(a) \end{aligned}$$

Thus by the choice of $L_N := \alpha_N^{\frac{1}{4}} N^{\frac{1}{2} + \frac{1}{k}}$, our assumptions implies that for large N ,

$$\tilde{P}_{n_N}^{(2)}((0, 0), (0, 0)) \gg \frac{c}{L_N^2 N} n_N$$

so that uniformly in $x, y \in \mathbb{Z}/(N\mathbb{Z})$ such that $d(x, y) \geq L_N$, we have

$$P_{n_N}^{(2)}((x, y), (x, y)) \sim \tilde{P}_{n_N}^{(2)}((x, y), (x, y))$$

The announced equivalence is then a consequence of

$$\text{card}(\{(x, y) : d(x, y) \geq L_N\}) \sim N^2$$

because our assumptions also imply that $\lim_{N \rightarrow \infty} L_N/N = 0$. ■

So in the time scale we are interested in, we can replace in (12) most of the terms $\mathbb{P}[Z_n(x) = x, Z_n(y) = y]$ by $\tilde{P}_n^{(2)}((x, y), (x, y))$. To end the proof of Proposition 17, it remains to show that, with the notations of Lemma 19 and under the assumptions of Proposition 17,

$$\begin{aligned} \lim_{N \rightarrow \infty} \sum_{x \neq y \in E_N : d(x,y) \leq L_N} (P_{n_N}^{(2)}((x, y), (x, y)))^K &= \lim_{N \rightarrow \infty} 2N \sum_{x \in \llbracket 1, L_N \rrbracket} (P_{n_N}^{(2)}((0, x), (0, x)))^K \\ &= 0 \end{aligned} \tag{15}$$

To do so, we will produce a direct bound on $P_{n_N}^{(2)}((x, y), (x, y))$, but it won't be so sharp. The underlying idea is to use heat kernel type estimates deduced from isoperimetric information (for a well-written introduction to this subject, see for instance Coulhon [4]). So let us consider the transition kernel $Q^{(2)}$ which is defined by the same formulas as $P^{(2)}$, except that $E_N^{(2)}$ is replaced by $\mathcal{V}^{(2)} := \mathbb{Z}^2 \setminus \Delta(\mathbb{Z}^2)$ (where $\Delta(\mathbb{Z}^2) := \{(x, x) : x \in \mathbb{Z}\}$ is the diagonal of \mathbb{Z}^2). We endow $\mathcal{V}^{(2)}$ with a graph structure by introducing the set of edges

$$\mathcal{E}^{(2)} := \{\{x, y\} : x \neq y \in \mathcal{V}^{(2)} \text{ and } Q^{(2)}(x, y) > 0\}$$

We denote respectively by λ and λ_∂ the counting measures on $\mathcal{V}^{(2)}$ and on $\mathcal{E}^{(2)}$. Let us also designate by \mathcal{R} the set of nonempty finite subsets of $\mathcal{V}^{(2)}$. If $R \in \mathcal{R}$, its boundary is the finite subset of $\mathcal{E}^{(2)}$ defined by

$$\partial R := \{\{x, y\} \in \mathcal{E}^{(2)} : x \in R \text{ and } y \notin R\} \tag{16}$$

Lemma 20. *There exists a constant $c > 0$ such that the 2-dimensional isoperimetric inequality is satisfied:*

$$\forall R \in \mathcal{R}, \quad \frac{\lambda_\partial(\partial R)}{\sqrt{\lambda(R)}} \geq c$$

Proof. The typical example of a 2-dimensional isoperimetric inequality is that of $\bar{\mathcal{V}} := \mathbb{Z}^2$ endowed with its traditional nearest neighborhood graph structure. More rigorously, consider the set of edges $\bar{\mathcal{E}} := \{\{x, y\} \subset \mathbb{Z}^2 : |x - y| = 1\}$ and denote respectively by $\bar{\lambda}$ and $\bar{\lambda}_\partial$ the counting measures on $\bar{\mathcal{V}}$ and on $\bar{\mathcal{E}}$. For any $R \in \bar{\mathcal{R}}$, the set of nonempty finite subsets of $\bar{\mathcal{V}}$, we define the boundary set $\bar{\partial}R$ by the same formula (16), with $\mathcal{E}^{(2)}$ replaced by $\bar{\mathcal{E}}$. It is well-known (see for instance Coulhon [4]), that there exists a constant $\bar{c} > 0$ such that

$$\forall R \in \bar{\mathcal{R}}, \quad \frac{\bar{\lambda}_\partial(\bar{\partial}R)}{\bar{\lambda}^{\frac{1}{2}}(R)} \geq \bar{c}$$

(more generally and with obvious notations, a similar result is true for the d -dimensional lattice \mathbb{Z}^d , with $d \in \mathbb{N}^*$, except that in the l.h.s., $\bar{\lambda}^{\frac{1}{2}}(R)$ has to be replaced by $\bar{\lambda}^{\frac{d-1}{d}}(R)$, this corresponds to the d -dimensional isoperimetric inequality).

Let us come back now to the graph $(\mathcal{V}^{(2)}, \mathcal{E}^{(2)})$ which can be seen (from ‘‘far away’’) as a slight modification of $(\bar{\mathcal{V}}, \bar{\mathcal{E}})$. First consider $R \in \mathcal{R}$ which is symmetrical, in the sense that if $x = (x_1, x_2) \in R$ then $\tilde{x} := (x_2, x_1)$ also belongs to R . Define

$$\bar{R} := R \sqcup \{(x_1, x_1) \in \mathbb{Z}^2 : \exists x_2 \in \mathbb{Z} \text{ with } |x_1 - x_2| = 1 \text{ and } (x_1, x_2) \in R\}$$

and let us show that

$$\lambda_\partial(R) \geq \frac{\bar{\lambda}_\partial(\bar{R})}{2} \tag{17}$$

Indeed, let $\{x, y\} \in \bar{\partial}\bar{R}$ be given, with $x \in R$ and $y \notin R$ and consider the different possibilities which can occur:

- If $x \in \mathcal{V}^{(2)}$ and $y \in \mathcal{V}^{(2)}$, then $\{x, y\} \in \partial R$.
- If $x = (x_1, x_1) \in \Delta(\mathbb{Z}^2)$ and $y = (y_1, y_2) \in \mathcal{V}^{(2)}$, for instance if $y_1 = x_1$ and $y_2 = x_1 + 1$. By definition of \bar{R} , it is easy to check that either $\{(x_1 - 1, x_1), (x_1 - 1, x_1 + 1)\} \in \partial R$ or $\{(x_1 - 1, x_1 + 1), (x_1, x_1 + 1)\} \in \partial R$ (depending on the belonging or not of the point $(x_1 - 1, x_1 + 1)$ to R).
- The possibility $y \in \Delta(\mathbb{Z}^2)$ is not permitted by our definition of \bar{R} .

So to any edge of $\bar{\partial}\bar{R}$, we can associate an edge of ∂R and through this relation any edge of ∂R can be associated only twice to an edge of $\bar{\partial}\bar{R}$. The bound (17) then follows.

Note that trivially we also have $\lambda(R) \leq \bar{\lambda}(\bar{R})$, so we get

$$\frac{\lambda_\partial(\partial R)}{\lambda^{\frac{1}{2}}(R)} \geq \frac{1}{2} \frac{\bar{\lambda}_\partial(\bar{\partial}\bar{R})}{\bar{\lambda}^{\frac{1}{2}}(\bar{R})}$$

and

$$\forall R \in \tilde{\mathcal{R}}, \quad \frac{\lambda_\partial(\partial R)}{\sqrt{\lambda(R)}} \geq \frac{\bar{c}}{2}$$

where $\tilde{\mathcal{R}}$ is the subset of \mathcal{R} consisting of symmetrical sets.

Next consider $R \in \mathcal{R}$ and let $\bar{R} \in \tilde{\mathcal{R}}$ be its symmetrized set:

$$\bar{R} := \{x \in \mathcal{V}^{(2)} : x \in R \text{ or } \tilde{x} \in R\}$$

We will show that

$$\frac{\lambda_\partial(\partial R)}{\lambda^{\frac{1}{2}}(R)} \geq \frac{1}{2} \frac{\lambda_\partial(\partial\bar{R})}{\lambda^{\frac{1}{2}}(\bar{R})}$$

so the above lemma will be proven with $c := \bar{c}/4$.

Since we have clearly $\lambda(R) \leq \lambda(\bar{R})$, it is sufficient to see that $\lambda_\partial(R) \geq \frac{\lambda_\partial(\bar{R})}{2}$. To do so, let $\{x, y\} \in \partial\bar{R}$, with $x \in \bar{R}$ and $y \notin \bar{R}$. If $x \in R$ then we have $\{x, y\} \in \partial R$, because $\bar{R}^c \subset R^c$. If $\tilde{x} \in R$, then $\{\tilde{x}, \tilde{y}\} \in \partial R$, because we also have $\tilde{y} \in \bar{R}^c \subset R^c$. Thus an argument similar to the one leading to (17) enables us to conclude the desired result. ■

Let us define a new transition kernel $\tilde{Q}^{(2)}$ on $\mathcal{V}^{(2)}$, by imposing that

$$\forall x \neq y \in \mathcal{V}^{(2)}, \quad \tilde{Q}^{(2)}(x, y) := \begin{cases} \frac{1}{4}, & \text{if } \{x, y\} \in \mathcal{E}^{(2)} \\ 0, & \text{otherwise} \end{cases}$$

The link with the boundary measure λ_∂ is that

$$\forall x \neq y \in \mathcal{V}^{(2)}, \quad \lambda_\partial(\{x, y\}) = 4\lambda(x)\tilde{Q}^{(2)}(x, y)$$

The isoperimetric inequality of the above lemma then implies the following upper bound on the diagonal (see Theorem 4.2 of Coulhon [4]): there exists a constant $c' > 0$ such that

$$\forall x \in \mathcal{V}^{(2)}, \forall n \in \mathbb{N}, \quad \tilde{Q}_n^{(2)}(x, x) \leq \frac{c'}{1+n}$$

(a d -dimensional isoperimetric inequality will lead to a Gaussian bound of the type $c'(1+n)^{-d/2}$). Note that for $N \geq 4$, the kernel $Q^{(2)}$ is strongly related to $\tilde{Q}^{(2)}$: with probability $4/N$ the transition is the same and otherwise the current state does not make a move. In particular we get that

$$\begin{aligned} \forall x \in \mathcal{V}^{(2)}, \forall n \in \mathbb{N}, \quad Q_n^{(2)}(x, x) &= \sum_{p \in \llbracket 0, n \rrbracket} \binom{n}{p} \left(\frac{4}{N}\right)^p \left(1 - \frac{4}{N}\right)^{n-p} \tilde{Q}_p^{(2)}(x, x) \\ &\leq c' \sum_{p \in \llbracket 0, n \rrbracket} \binom{n}{p} \left(\frac{4}{N}\right)^p \left(1 - \frac{4}{N}\right)^{n-p} \frac{1}{p+1} \\ &= \frac{c'N}{4(n+1)} \sum_{p \in \llbracket 0, n \rrbracket} \binom{n+1}{p+1} \left(\frac{4}{N}\right)^{p+1} \left(1 - \frac{4}{N}\right)^{n-p} \\ &\leq c' \frac{N}{n+1} \end{aligned}$$

By comparison, this bound enables to evaluate $P^{(2)}$ on the diagonal:

Lemma 21. *There exists a constant $c'' > 0$ such that for $N \geq 4$,*

$$\forall x \in \mathbb{Z}/(N\mathbb{Z}), \forall n \in \mathbb{N}, \quad P_n^{(2)}((0, x), (0, x)) \leq 1 \wedge \left(c'' \left(\frac{N}{1+n} + \frac{n}{N^3}\right)\right)$$

Proof. By symmetry of the problem, we can assume that $x \in \llbracket 0, \lfloor N/2 \rfloor \rrbracket$ (where $\mathbb{Z}/(N\mathbb{Z})$ was naturally identified with $\llbracket 0, N-1 \rrbracket$) and consider $(X_n, Y_n)_{n \in \mathbb{N}}$ be a Markov chain starting from $(0, x)$ and admitting $P^{(2)}$ as transition kernel. Let $y := (x + N)/2$, if $x + N$ is even we define τ_X (respectively τ_Y) as the first time $(X_n)_{n \in \mathbb{N}}$ (resp. $(Y_n)_{n \in \mathbb{N}}$) reaches y and if $x + N$ is odd, let τ_X (respectively τ_Y) be the first time $(X_n)_{n \in \mathbb{N}}$ (resp. $(Y_n)_{n \in \mathbb{N}}$) reaches either $(x+N+1)/2$ or $(x+N-1)/2$. Next we “cut” the discrete circle $\mathbb{Z}/(N\mathbb{Z})$ at y . This means that now, if $x + N$ is even (respectively odd), we identify $\mathbb{Z}/(N\mathbb{Z})$ with $\llbracket y - N + 1, -1 \rrbracket \sqcup \llbracket 0, y \rrbracket$ (resp. with $\llbracket y - N + 1/2, -1 \rrbracket \sqcup \llbracket 0, y - \frac{1}{2} \rrbracket$). Then up to the time $\tau := \tau_X \wedge \tau_Y$, $(X_n, Y_n)_{n \in \mathbb{N}}$ behaves like a Markov chain $(\tilde{X}_n, \tilde{Y}_n)_{n \in \mathbb{N}}$ on $\mathcal{V}^{(2)}$ starting from $(0, x)$ and admitting $Q^{(2)}$ as transition matrix (more rigorously this means there exists a coupling between these two chains so that for any $n \leq \tau$, $(\tilde{X}_n, \tilde{Y}_n) = (X_n, Y_n)$). It follows that for any $n \in \mathbb{N}$, we have

$$\begin{aligned} P_n^{(2)}((0, x), (0, x)) &\leq Q_n^{(2)}((0, x), (0, x)) + \mathbb{P}[\tau \leq n] \\ &\leq Q_n^{(2)}((0, x), (0, x)) + \mathbb{P}[\tau_X \leq n] + \mathbb{P}[\tau_Y \leq n] \\ &= Q_n^{(2)}((0, x), (0, x)) + 2\mathbb{P}[\tau_X \leq n] \\ &\leq Q_n^{(2)}((0, x), (0, x)) + 2\mathbb{P}[\tilde{\tau} \leq n] \end{aligned}$$

with

$$\tilde{\tau} := \inf\{n \in \mathbb{N} : d(0, X_n) \geq y \wedge (N - y) - 1/2\}$$

Arguments similar to those used in the proof of Lemma 18 enable to see that there exists a universal constant $c''' > 0$ such that $\tilde{\tau}$ is stochastically bounded below by an exponential random variable of parameter $c'''N^{-1}(y \wedge (N - y) - 1/2)^{-2}$. But for $N \geq 4$, we have $y \wedge (N - y) \geq N/4$, so we deduce that for any time $n \in \mathbb{N}$,

$$\begin{aligned} \mathbb{P}[\tilde{\tau} \leq n] &\leq 1 - \exp(-8^2 c''' n/N^3) \\ &\leq 8^2 c''' \frac{n}{N^3} \end{aligned}$$

The announced result then follows from the bound given above the lemma on $Q_n^{(2)}((0, x), (0, x))$. ■

The proof of (15) is now clear: by the previous estimate, we have

$$N \sum_{x \in \llbracket 1, L_N \rrbracket} \left(P_{n_N}^{(2)}((0, x), (0, x)) \right)^K \leq N L_N \left(c'' \left(\frac{N}{1 + n_N} + \frac{n_N}{N^3} \right) \right)^K$$

and taking into account the form of n_N , this expression will vanish for large N if

$$\lim_{N \rightarrow \infty} N^{-1} L_N \frac{1}{\alpha_N^K} = 0$$

and

$$\lim_{N \rightarrow \infty} N^{-2K+3} L_N \alpha_N^K = 0$$

Remembering that $L_N := \alpha_N^{\frac{1}{4}} N^{\frac{1}{2} + \frac{1}{K}}$ and that the sequence $(\alpha_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ is bounded, the latter convergence is a consequence of the fact that $-2K + 7/2 + 1/K$ is negative for $K \geq 3$. Concerning the former convergence, it amounts to the condition (13) of Proposition 17, and this ends its proof. Taking into account Corollary 15, we can now complete the proof of the transition phenomenon of Theorem 2, which is based on the following observation: for any time $n \in \mathbb{N}$, we have

$$\begin{aligned} \mathbb{P}[B_n^c] &= \mathbb{P}[S_n = 0] \\ &\leq \frac{\text{Var}(S_n)}{\mathbb{E}^2[S_n]} \end{aligned}$$

Let $\alpha > 0$ be fixed, Proposition 17 implies that

$$\liminf_{N \rightarrow \infty} \mathbb{P}\left[B_{\alpha N^{1+\frac{2}{K}}}\right] \geq 1 - \frac{1}{I^K(\alpha)} \tag{18}$$

so as announced,

$$\lim_{\alpha \rightarrow 0+} \liminf_{N \rightarrow \infty} \mathbb{P}\left[B_{\alpha N^{1+\frac{2}{K}}}\right] = 1$$

Remark 22. We strongly believe that the condition (13) of Proposition 17 is only technical and that a further investigation should enable to remove it. It would follow that the transition phenomenon for the non-existence of a fixed point is unique in the sense given in the introduction.

To complete the proof of Theorem 2, it remains to show that the transition for the non-existence of a fixed point is flared, namely to find a non-empty interval $(\alpha_*, \alpha^*) \subset \mathbb{R}_+$ such that for any $\alpha \in (\alpha_*, \alpha^*)$,

$$0 < \underline{L}(\alpha) \leq \bar{L}(\alpha) < 1 \tag{19}$$

where

$$\begin{aligned} \underline{L}(\alpha) &:= \liminf_{N \rightarrow \infty} \mathbb{P}\left[B_{\alpha N^{1+\frac{2}{K}}}\right] \\ \overline{L}(\alpha) &:= \limsup_{N \rightarrow \infty} \mathbb{P}\left[B_{\alpha N^{1+\frac{2}{K}}}\right] \end{aligned}$$

Corollary 15 already shows that $\overline{L}(\alpha) < 1$ for $\alpha \in (\alpha', +\infty)$. Unfortunately, (18) only informs us that $\underline{L}(\alpha) > 0$ for $\alpha \in (0, \alpha')$. To go beyond α' , we use Bonferroni inequalities (also known under the name of exclusion-inclusion principle) which in our context say that at any time $n \in \mathbb{N}$: for any odd $p \geq 1$,

$$\mathbb{P}(\cup_{x \in E_N} B_n(x)) \leq \sum_{l=1}^p (-1)^{l-1} \sum_{x_1 < x_2 < \dots < x_l \in E_N} \mathbb{P}[\cap_{j \in [1,l]} B_n(x_j)]$$

and for any even $p \geq 2$,

$$\mathbb{P}(\cup_{x \in E_N} B_n(x)) \geq \sum_{l=1}^p (-1)^{l-1} \sum_{x_1 < x_2 < \dots < x_l \in E_N} \mathbb{P}[\cap_{j \in [1,l]} B_n(x_j)]$$

Consider the case $p = 2$, we get

$$\mathbb{P}[B_n] \geq \sum_{x \in E_N} \mathbb{P}[B_n(x)] - \sum_{x < y \in E_N} \mathbb{P}[B_n(x) \cap B_n(y)]$$

According to (12), the last sum is equal to $(\text{Var}(S_n) - \mathbb{E}[S_n] + \mathbb{E}^2[S_n])/2$ and it follows that

$$\mathbb{P}[B_n] \geq \frac{3}{2} \mathbb{E}[S_n] - \frac{1}{2} \mathbb{E}^2[S_n] - \frac{1}{2} \text{Var}(S_n)$$

Let $\alpha > 0$ be fixed, for $K \geq 3$, Lemma 14 and Proposition 17 imply that

$$\begin{aligned} \liminf_{N \rightarrow \infty} \mathbb{P}\left[B_{\alpha N^{1+\frac{2}{K}}}\right] &\geq \frac{3}{2} I^K(\alpha) - \frac{1}{2} I^{2K}(\alpha) - \frac{1}{2} I^K(\alpha) \\ &= I^K(\alpha) \left(1 - \frac{1}{2} I^K(\alpha)\right) \end{aligned}$$

We deduce that $\underline{L}(\alpha) > 0$ for $\alpha \in (\alpha'', +\infty)$ with

$$\begin{aligned} \alpha'' &:= \inf\{\alpha > 0 : I^K(\alpha) \leq 2\} \\ &= \frac{1}{2^{2+\frac{2}{K}} \pi} \\ &< \alpha' \end{aligned}$$

Together with (18), this implies that $\underline{L}(\alpha) > 0$ for any $\alpha \in (0, +\infty)$. Thus (19) holds with $\alpha_* = \alpha'$ and $\alpha^* = +\infty$.

We end this section with the observation that the interval on which we know that $\overline{L}(\alpha) < 1$ can be improved as K becomes larger and larger:

Remark 23. The study of the flared transition relative to the non-existence of a fixed point in the neighbor generating transposition model can be pushed further, as it is suggested by the Bonferroni inequalities.

For $p \geq 3$ and $x_1 < x_2 < \dots < x_p \in E_N$, the p -tuple process $(Z_n(x_1), \dots, Z_n(x_p))_{n \in \mathbb{N}}$ is a Markov chain, let $P^{(p)}$ be its transition matrix. As it was done in this section for the case $p = 2$, we can consider $\tilde{P}^{(p)}$ the transition matrix on $\mathbb{Z}/(N\mathbb{Z})$ where the main interaction of exchange between two components has been removed from $\tilde{P}^{(p)}$. Considerations similar to those of Lemma 16 enable to see that for N large

$$\tilde{P}^{(p)}_{\lfloor \alpha N^{1+\frac{2}{K}} \rfloor}((x_1, \dots, x_p), (x_1, \dots, x_p)) \sim I^p(\alpha) \frac{1}{N^{\frac{p}{K}}}$$

Furthermore, arguments similar to those which have led to Proposition 17 show that for any given $\alpha > 0$, the quantity

$$\sum_{x_1 < x_2 < \dots < x_p} \mathbb{P}[\cap_{j \in \llbracket 1, p \rrbracket} B_{\alpha N^{1+\frac{2}{K}}}(x_j)] = \sum_{x_1 < x_2 < \dots < x_p} (P^{(p)}_{\lfloor \alpha N^{1+\frac{2}{K}} \rfloor}((x_1, \dots, x_p), (x_1, \dots, x_p)))^K$$

has the same behavior for large N as

$$\sum_{x_1 < x_2 < \dots < x_p} (\tilde{P}^{(p)}_{\lfloor \alpha N^{1+\frac{2}{K}} \rfloor}((x_1, \dots, x_p), (x_1, \dots, x_p)))^K$$

at least if $K > (p + 2)/2$. Thus if p is odd, we get that

$$\bar{L}(\alpha) \leq \sum_{l=1}^p (-1)^{l-1} \frac{I^{lK}(\alpha)}{l!}$$

while if p is even, we have

$$\underline{L}(\alpha) \geq \sum_{l=1}^p (-1)^{l-1} \frac{I^{lK}(\alpha)}{l!}$$

Note that as $\alpha \rightarrow 0_+$, the latter r.h.s. goes to $-\infty$, so none of these lower bounds enables to recover the fact that $\lim_{\alpha \rightarrow 0_+} \underline{L}(\alpha) = 1$. Of course, one would like to forget the condition $K > (p + 2)/2$ and let p go to infinity to obtain

$$\lim_{N \rightarrow \infty} \mathbb{P}[B_{\alpha N^{1+\frac{2}{K}}}] = 1 - \exp(-I^K(\alpha)) \tag{20}$$

Heuristically this is what we will do in next section by allowing the multiplicity K to depend on the size N .

5. SHARP TRANSITION FOR THE NEIGHBOR GENERATING TRANSPOSITIONS

Here we give the proof of an extension of Theorem 3. It is based on the estimates of the previous section, whose arguments indeed simplify in the case we are interested in of multiplicity increasing with size. The heuristic convergence (20) gives a feeling why it

should be true: for large K , the r.h.s. seen as a function of $\alpha \in \mathbb{R}_+$ becomes closer and closer to a function whose value is 1 on $[0, \alpha')$ and 0 on $[\alpha', +\infty)$, where $\alpha' = 1/(4\pi)$ was introduced in Corollary 15. But this picture is also a little misleading, since the true critical value $\tilde{\alpha}$ appearing in Theorem 3 is not equal to α' , as it will be checked in Section 6. This comes from the different renormalizations we use: in some sense the limits that we are considering are not commuting.

Recall that the function J was defined in the introduction by

$$J : \mathbb{R}_+ \ni \alpha \mapsto \int_0^1 \exp(-2\alpha(1 - \cos(2\pi s))) ds$$

and for any $\beta > 0$, consider $\alpha(\beta) \in \mathbb{R}_+^*$ the unique value such that $J(\alpha(\beta)) = \exp(-1/\beta)$. Theorem 3 can be extended into

Theorem 24. *In the model of neighbor generating transpositions, there is a (K, T) -sharp transition for the non-existence of a fixed point with*

$$\begin{aligned} K(N) &:= \beta \ln(N) \\ T(N) &:= \alpha(\beta)N \end{aligned}$$

Let $\alpha, \beta > 0$ be given, from now on, we denote for $N \geq 2 \vee \exp(2/\beta)$

$$\begin{aligned} K_N &:= \lfloor \beta \ln(N) \rfloor \\ n_N(\alpha) &:= \lfloor \alpha N \rfloor \end{aligned}$$

Our primary object of interest is the random variable counting the number of fixed points:

$$S(N, \alpha) := \sum_{x \in E_N} \mathbb{1}_{B_{n_N(\alpha)}^{(K_N)}(x)}$$

Noting that, on one hand,

$$\mathbb{P}[B_{n_N(\alpha)}^{(K_N)}] \leq \mathbb{E}[S(N, \alpha)]$$

and on the other hand,

$$\begin{aligned} \mathbb{P}[(B_{n_N(\alpha)}^{(K_N)})^c] &= \mathbb{P}[S(N, \alpha) = 0] \\ &\leq \mathbb{P}[|S(N, \alpha) - \mathbb{E}[S(N, \alpha)]| \geq \mathbb{E}[S(N, \alpha)]] \\ &\leq \frac{\text{Var}(S(N, \alpha))}{\mathbb{E}[S(N, \alpha)]^2} \end{aligned}$$

the above theorem is a consequence of the following estimates:

Proposition 25. *The crude asymptotical behavior of the expectation of the above sum is*

$$\lim_{N \rightarrow \infty} \mathbb{E}[S(N, \alpha)] = \begin{cases} +\infty, & \text{if } \alpha < \alpha(\beta) \\ 0, & \text{if } \alpha > \alpha(\beta) \end{cases} \tag{21}$$

Furthermore, in the case $\alpha < \alpha(\beta)$, we have

$$\lim_{N \rightarrow \infty} \frac{\text{Var}(S(N, \alpha))}{\mathbb{E}^2[S(N, \alpha)]} = 0 \tag{22}$$

The proof of (21) begins with the explicit formula for the expectation given in Lemma 13:

$$\mathbb{E}[S(N, \alpha)] = N \left(\frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \left(1 + \frac{2}{N} \left(\cos \left(\frac{2\pi l}{N} \right) - 1 \right) \right)^{n_N(\alpha)} \right)^{K_N}$$

Note that we can find a universal constant $c > 0$ such that for any $l \in \llbracket 0, N-1 \rrbracket$,

$$\begin{aligned} \exp \left(-\frac{c}{N^2} \right) \exp \left(\frac{2}{N} \left[\cos \left(\frac{2\pi l}{N} \right) - 1 \right] \right) &\leq 1 + \frac{2}{N} \left(\cos \left(\frac{2\pi l}{N} \right) - 1 \right) \\ &\leq \exp \left(\frac{2}{N} \left[\cos \left(\frac{2\pi l}{N} \right) - 1 \right] \right) \end{aligned}$$

so since $n_N(\alpha)K_N/N^2$ goes to zero for large N , we get that

$$\begin{aligned} \mathbb{E}[S(N, \alpha)] &\sim N \left(\frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \exp \left(\frac{2}{N} \left[\cos \left(\frac{2\pi l}{N} \right) - 1 \right] n_N(\alpha) \right) \right)^{K_N} \\ &= N \left(\frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \exp \left(2\alpha \left[\cos \left(\frac{2\pi l}{N} \right) - 1 \right] \right) \right)^{K_N} \end{aligned}$$

Next recognizing a Riemann type sum, we have

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{l \in \llbracket 0, N-1 \rrbracket} \exp \left(2\alpha \left[\cos \left(\frac{2\pi l}{N} \right) - 1 \right] \right) = J(\alpha)$$

so it appears that

$$\lim_{N \rightarrow \infty} \frac{\ln(\mathbb{E}[S(N, \alpha)])}{\ln(N)} = 1 + \beta \ln(J(\alpha)) \tag{23}$$

and the announced convergence (21) follows at once.

Concerning the convergence (22), since for $\alpha < \alpha(\beta)$, we have $\lim_{N \rightarrow \infty} \mathbb{E}[S(N, \alpha)] = +\infty$, it is sufficient (recall (12)) to show that

$$\lim_{N \rightarrow \infty} \mathbb{E}^{-2}[S(N, \alpha)] \sum_{x \neq y \in E_N} \mathbb{P}^{K_N}[Z_{n_N(\alpha)}(x) = x, Z_{n_N(\alpha)}(y) = y] = 1$$

Using the notations introduced above Lemma 16 and identifying E_N with $\mathbb{Z}/(N\mathbb{Z})$, this amounts to

$$\lim_{N \rightarrow \infty} \mathbb{E}^{-2}[S(N, \alpha)] N \sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (P_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} = 1$$

and Lemma 16 implies immediately that

$$\begin{aligned} & \lim_{N \rightarrow \infty} \mathbb{E}^{-2}[S(N, \alpha)]N \sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \\ &= \lim_{N \rightarrow \infty} \mathbb{E}^{-2}[S(N, \alpha)] \frac{N(N-1)}{2} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, 0), (0, 0)))^{K_N} \\ &= 1 \end{aligned} \tag{24}$$

so we are led to show that

$$\lim_{N \rightarrow \infty} \frac{\sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (P_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N}}{\sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N}} = 1 \tag{25}$$

Let $(L_N)_{N \in \mathbb{N} \setminus \{0,1\}}$ be a sequence of positive integers diverging to infinity but such that $\lim_{N \rightarrow \infty} L_N/N = 0$. We decompose the above numerator into

$$\begin{aligned} R_1(N, \alpha) &:= \sum_{x \in \mathbb{Z}/(N\mathbb{Z}) : d(0,x) > L_N} (P_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \\ R_2(N, \alpha) &:= \sum_{x \in \mathbb{Z}/(N\mathbb{Z}) : 1 \leq d(0,x) \leq L_N} (P_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \end{aligned}$$

On one hand, according to Lemma 19, we have, with the constant $c > 0$ defined there and for any $x \in \mathbb{Z}/(N\mathbb{Z})$ such that $d(0, x) > L_N$,

$$\begin{aligned} |P_{n_N(\alpha)}^{(2)}((0, x), (0, x)) - \tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x))| &= |P_{n_N(\alpha)}^{(2)}((0, x), (0, x)) - \tilde{P}_{n_N(\alpha)}^{(2)}((0, 0), (0, 0))| \\ &\leq \frac{2cn_N(\alpha)}{NL_N^2} \\ &\leq \frac{2c\alpha}{L_N^2} \end{aligned}$$

and on the other hand, (23) and (24) show that

$$\liminf_{N \rightarrow \infty} \tilde{P}_{n_N(\alpha)}^{(2)}((0, 0), (0, 0)) \geq J^2(\alpha)$$

We deduce that for large N ,

$$\begin{aligned} R_1(N) &\sim \sum_{x \in \mathbb{Z}/(N\mathbb{Z}) : d(0,x) > L_N} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \\ &= (N - 2L_N - 1)_+ \tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x))^{K_N} \\ &\sim \sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \end{aligned}$$

Finally, contrary to what we have done in Section 4, we don't need here isoperimetric estimates to treat the term $R_2(N, \alpha)$, we just write that

$$\begin{aligned} R_2(N, \alpha) &\leq 2L_N + 1 \\ &\ll J^2(\alpha)(N - 1) \\ &\sim \sum_{x \neq 0 \in \mathbb{Z}/(N\mathbb{Z})} (\tilde{P}_{n_N(\alpha)}^{(2)}((0, x), (0, x)))^{K_N} \end{aligned}$$

to end the proof of (25).

Remark 26. We believe that the results obtained in this section and in the previous one also hold for the transition corresponding to transitivity. But to follow the approach presented in Section 3, we would need to know the spectra of the exclusion processes associated to the simple random walk on $\mathbb{Z}/(N\mathbb{Z})$. Unfortunately they do not seem to be known and this looks like an interesting subject to be investigated.

6. SIMULATIONS

Here we use the computer to evaluate numerically the constant $\tilde{\alpha}$ and to plot Monte Carlo approximations of the mappings defined in (1) in several situations to illustrate our results and to support some conjectures.

Usual numerical resolution techniques gives the following approximate value for the constant $\tilde{\alpha}$ defined above Theorem 3:

$$\tilde{\alpha} \approx 0.2916614$$

So as announced at the beginning of Section 5, $\tilde{\alpha}$ is clearly different from $\alpha' = 1/(4\pi) \approx 0.0795775$. Note that $\tilde{\alpha}$ is quite close to 0.25, so if we come back to the complexity arguments presented after Theorem 2, we see that the complexities in the cases of uniform transpositions and neighbor transpositions (of Theorem 3), respectively $N \ln(N)/2$ and $2\tilde{\alpha}N \ln(N)$, are very close (without taking into account the cost of the underlying uniform samplings). At least for the nonexistence of a fixed point property, the last picture below suggests that if Theorem 3 holds for the transitivity property, then the corresponding constant α should be not very far from $2\tilde{\alpha}$.

Now we come to the pictures of the mappings defined in (1).

We made several experiments with the computer algebra system Maple, using the package "group" which provides facilities to represent permutations, compute product of permutations, generate subgroups and compute orbits. Maple also has a command `rand(1..N)()` which allows to produce sequences of integers between 1 and N almost following a uniform distribution.

For each case we experimented, we let the program run 100 (independent) times, then we took the average values as an empirical estimation of the targeted probability. The graphics in Figure 1 picture interpolating curves.

6.1. Cut-Off for Transitivity in the Uniform Transposition Case

Picture (a) is an illustration of Theorem 1. We fix $K = 4$ and we consider three values of N . The empirical probability that the generated subgroup is transitive is plotted against the

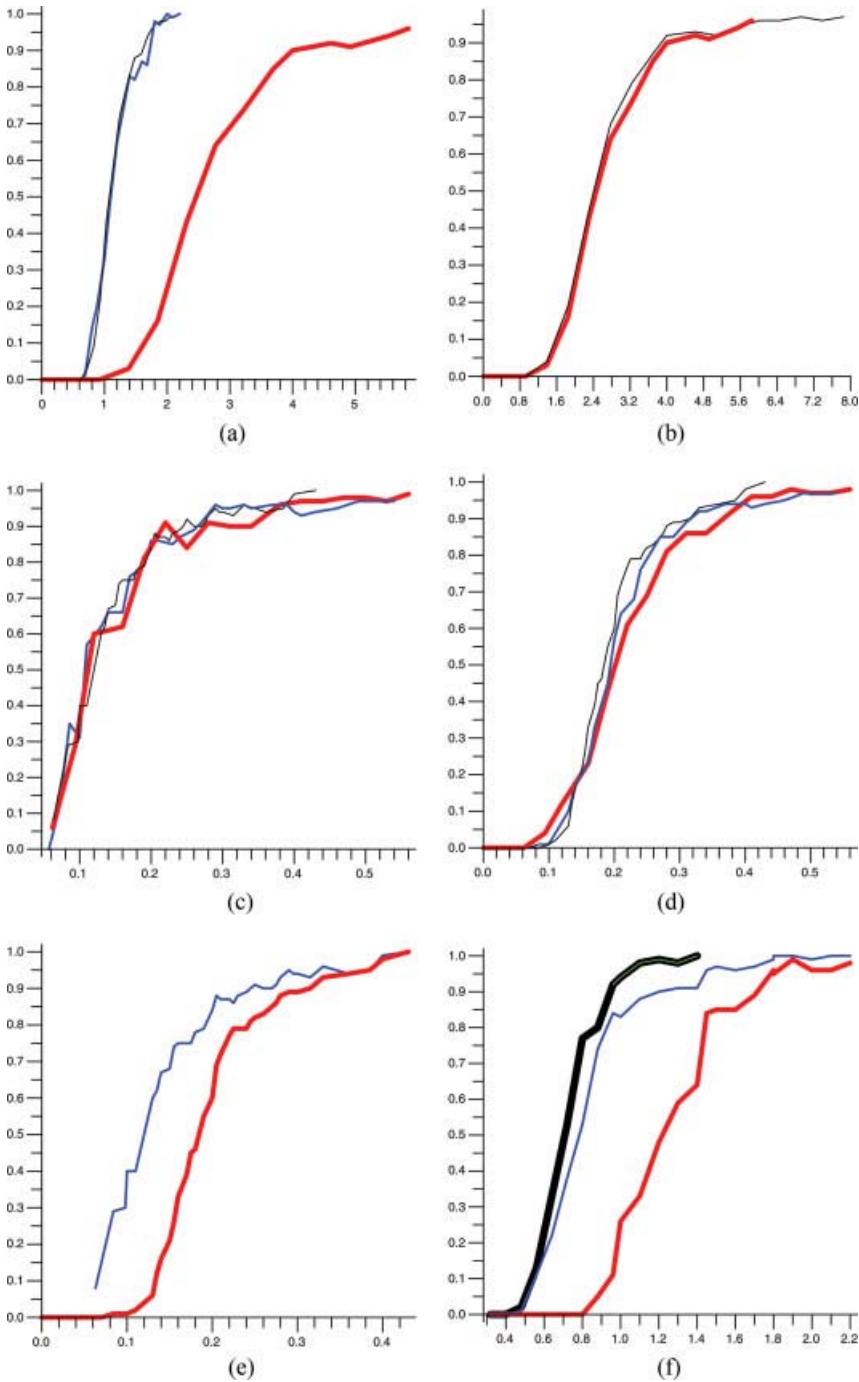


Fig. 1. Transitions for uniform and neighbor transposition cases. (a): uniform, transitivity $N = 30, 50, 100, K = 4$; (b): uniform, nofixedpoint-transitivity $N = 30, K = 4$; (c): neighbor, nofixedpoint-transitivity $N = 30, 50, 80, K = 4$; (d): neighbor, transitivity $N = 30, 50, 80, K = 4$; (e): neighbor, nofixedpoint-transitivity $N = 80, K = 4$; (f): uniform-neighbor $N = 50, K = 8$. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

time (or the number of product of uniform transpositions) normalized by $N \ln(N)/(2K)$.

The three values for the size of the problem are:

$N = 30$, in red and thickness 4, at the right of the picture

$N = 50$, in blue and thickness 2, at the middle of the picture

$N = 100$ in black and thickness 1, very close to the previous plot.

As expected, a cut-off phenomenon appears around the normalized time 1.

6.2. Comparison of Nonexistence of a Fixed Point and Transitivity in the Uniform Transposition Case

Picture (b) shows that the events of nonexistence of a fixed point and transitivity are very close in the uniform transposition case, in accordance with Theorem 1 and its proof. The values $N = 30$ and $K = 4$ are fixed and as above the time is divided by $N \ln(N)/(2K)$ in the x -axis. The plot of the empirical probabilities for transitivity (respectively for nonexistence of a fixed point) is in red with thickness 4 (resp. in black thickness 1).

Of course, the graph for nonexistence of a fixed point is above the one for transitivity, but they are very close. Indeed, if in Picture (a) we had rather plotted the curves for nonexistence of a fixed point, we would have ended up with a very similar picture.

6.3. Flared Transition for Nonexistence of a Fixed Point in the Neighbor Transposition Case

Picture (c) is an illustration of Theorem 2. We fix $K = 4$ and we consider three values of N . The empirical probability that there is no fixed point for the generated subgroup is plotted against the time normalized by $N^{1+\frac{2}{K}}$ (recall this is just an order, so the value 1 has no real meaning in the x -axis). The three values for the size of the problem are:

$N = 30$, in red and thickness 4

$N = 50$, in blue and thickness 2

$N = 80$ in black and thickness 1.

The three graphs are quite close, suggesting that there is indeed a fast convergence as N goes to infinity of the graph of the transitivity probabilities as a function of the renormalized time.

6.4. Flared Transition for Transitivity in the Neighbor Transposition Case

Picture (d) suggest that Theorem 2 also holds for the transitivity property. The values are the same as in Picture (c), except that we have plotted the empirical probabilities for the transitivity property of the generated subgroup.

Again the three graphs are quite close, this also supports the conjecture there is a flared transition in this situation. Note the limit graph would be quite different for nonexistence of a fixed point and transitivity.

6.5. Comparison of Nonexistence of a Fixed Point and Transitivity in the Neighbor Transposition Case

Picture (e) shows that there is a nonnegligeable difference between the events of nonexistence of a fixed point and transitivity in the neighbor transposition case, contrary to the

uniform transposition situation. The values $N = 80$ and $K = 4$ are fixed and the time is still divided by $N^{1+\frac{2}{K}}$ in the x -axis. The plot of the empirical probabilities for nonexistence of a fixed point (respectively transitivity) is in red with thickness 4 (resp. in blue thickness 2).

As expected, the graph for nonexistence of a fixed point is above the one for transitivity. Their difference suggests there will be new difficulties if one wants to extend Theorem 2 to the transitive case or to investigate the limiting graphs.

6.6. Comparison Uniform vs Neighbor Transposition Models

Picture (f) is an illustration for Theorem 3 and suggests that in order to extend it to the transitivity property, $\tilde{\alpha}$ would have to be modified. We consider $N = 50$ and $K = 8$ which is close to $2 \ln(N)$. In the x -axis, the time is renormalized by $0.26N$ which is also approximately equal to $N \ln(N)/(2K)$. The empirical probabilities are plotted. In the uniform transposition case, the probabilities for nonexistence of a fixed point and for transitivity are the same, up to the thickness of the line, black (and green inside) with thickness 6. On the contrary, in the neighbor case, the graphs of nonexistence of a fixed point and of transitivity are clearly distinct, their respective colors are red and blue, with thickness 4 and 2.

Note that the plots of nonexistence of a fixed point probability are quite similar, this mirrors the fact that both satisfy a cut-off phenomenon as predicted by Theorem 1 and 3. But the graph for transitivity becomes also similar to them if its time scale is divided by two.

ACKNOWLEDGMENTS

We are indebted to Persi Diaconis for his advice and encouragement to persevere with the investigation of this subject. We are grateful to Thierry Delmotte, who pointed out to us the lecture notes of Coulhon [4] and to the referees who helped us to improve this paper. Finally we are grateful to the Laboratoire d'Analyse, Topologie, Probabilités (UMR 6632) in Marseille, where parts of this work were done.

REFERENCES

- [1] D. Aldous and P. Diaconis, Strong uniform times and finite random walks, *Adv Appl Math* 8 (1987), 69–97.
- [2] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.
- [3] G. Chèze and A. Galligo, Four lectures on polynomial absolute factorization, *Solving polynomial equations, Algorithm Comput Math* 14 (2005), 339–392.
- [4] T. Coulhon, Random walks and geometry on infinite graphs, *Lecture notes on analysis in metric spaces (Trento, 1999)*, *Appunti Corsi Tenuti Docenti Sc., Scuola Normale Superiore*, Pisa, 2000, pp. 5–36.
- [5] P. Diaconis, *Group representations in probability and statistics*, *Institute of Mathematical Statistics Lecture Notes—Monograph Series*, 11, Institute of Mathematical Statistics, Hayward, CA, 1988.
- [6] P. Diaconis, The cutoff phenomenon in finite Markov chains, *Proc Natl Acad Sci USA* 93 (1996), 1659–1664.

- [7] P. Donnelly, P. Lloyd, and A. Sudbury, Approach to stationarity of the Bernoulli-Laplace diffusion model, *Adv Appl Probab* 26 (1994), 715–727.
- [8] P. Diaconis and L. Miclo, On times to quasi-stationarity for birth and death processes, *J Theor Probab* 22 (2009), 558–586.
- [9] P. Diaconis and M. Shahshahani, Time to reach stationarity in the Bernoulli-Laplace diffusion model, *SIAM J Math Anal* 18 (1987), 208–218.
- [10] J. Jonasson, The mathematics of card shuffling, Preprint Available at, <http://www.math.chalmers.se/~jonasson/convrates.pdf>, 2009.
- [11] S. Karlin and J. McGregor, Coincidence properties of birth and death processes, *Pacific J Math* 9 (1959), 1109–1140.
- [12] T. Łuczak and L. Pyber, On random generation of the symmetric group [MR1264722 (95b:20004)], *Combinatorics, geometry and probability* (Cambridge, 1993), Cambridge University Press, Cambridge, 1997, pp. 463–470.
- [13] R. Motwani and P. Raghavan, *Randomized algorithms*, Cambridge University Press, Cambridge, 1995.
- [14] A. J. Sommese and C. W. Wampler II, *The numerical solution of systems of polynomials: Arising in engineering and science*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.