On the cut-off phenomenon for the transitivity of randomly generated subgroups

André Galligo and Laurent Miclo

April 21, 2010

Plan of the talk

Random walks under consideration

Consider $Z := (Z_n)_{n\in\mathbb{N}}$ a random walk on the symmetric group S_N, starting from the identity and whose increments $Z_n^{-1}Z_{n+1}$ follow a law μ.
Let $Z^{(1)}, ..., Z^{(K)}$ be K independent chains distributed as Z.
At any time $n \in \mathbb{N}$, $G_n^{(K)}$ is the subgroup of S_N generated by $Z_n^{(1)}, ..., Z_n^{(K)}$. Two events concerning the action of $G_n^{(K)}$ on $[\![1, N]\!]$ are of interest for us:

$$
\begin{aligned}
A_n^{(K)} &:= \{G_n^{(K)} \text{ is transitive}\} \\
B_n^{(K)} &:= \{G_n^{(K)} \text{ admits at least a fixed point}\}
\end{aligned}
$$

First observations

Our goal: to study the mappings

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

for two particular choices of μ and especially to exhibit or not cut-off phenomena.

Contrary to the study of convergence to equilibrium, we don't know if these mappings are monotonous and this is related to the initial condition.

If Z is irreducible and aperiodic, a.s.,

$$\liminf_{n\to\infty} 1_{A_n^{(K)}} = 0 \quad \text{and} \quad \limsup_{n\to\infty} 1_{A_n^{(K)}} = 1$$

so it cannot be asserted in a deterministic way that $G_n^{(K)}$ eventually becomes transitive (idem for fixed points).

Transition phenomena 1

Cut-off phenomenon relatively to some events $C_{K,n}$ (typically $A_n^{(K)}$ or $(B_n^{(K)})^c$, if there exists a time $T(N,K) \in \mathbb{R}_+$ such that

$$\begin{array}{rcl} \forall\, \alpha \in [0,1), & \lim_{N\to\infty} \mathbb{P}\left[C_{K,\alpha T(N,K)}\right] & = & 0 \\ \forall\, \alpha \in (1,+\infty), & \lim_{N\to\infty} \mathbb{P}\left[C_{K,\alpha T(N,K)}\right] & = & 1 \end{array}$$

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

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

Transition phenomena 2

At the opposite of cut-off: a transition at times of order $T(N, K) \in \mathbb{R}_+^*$ is flared if there exist $0 < \alpha_* < \alpha^*$ such that for any $\alpha \in (\alpha_*, \alpha^*)$,

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

There is still a possibility for a sharp transition in this situation, if we can find a sequence $(K, T) := (K(N), T(N))$ such that

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

Uniform transposition model

It corresponds to

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

and for this model we have:

Theorem 1

There is a cut-off for transitivity as well as for the non-existence of fixed point at time

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

This suggests that a fixed point is the last resort against transitivity and this will be confirmed by simulations.

Before equilibrium

Theorem 1 also holds with μ replaced by

$$\widetilde{\mu} \quad := \quad \frac{1}{N^2} \sum_{i,j \in [\![1,N]\!]} \delta_{(i,j)}$$

The cut-off phenomenon for convergence to equilibrium (in the total variation sense) occurs at time $\frac{1}{2} N \ln(N)$ for the corresponding product chain $(Z^{(1)}, ..., Z^{(K)})$, so the properties of transitivity and of non-existence of fixed point appear strictly before the equilibrium is reached.

Successive transposition model

It corresponds to

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

The situation is now different:

Theorem 2

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

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

We conjecture the same result holds for transtivity as it is suggested by simulations.

Monte-Carlo procedures?

Both models can be seen as Monte-Carlo ways to sample subgroups of the symmetric group without fixed point (and hopefully of transitive semigroups). The complexity of these algorithms is heuristically $C := KT(N, K)$.
For the uniform transposition model, $C = N\ln(N)/2$, while $C = KN^{1+\frac{2}{K}}$ for successive transposition model. Optimizing in K, the better choice is $K = 2\ln(N)$, so C is of the same order in both cases. One may think that the first algorithm has the advantage that it admits a cut-off phenomenon, but this is also true for the second algorithm:

Sharp transition

For $\beta > 0$, let $\alpha(\beta) \in \mathbb{R}_+^*$ be the unique value such that $J(\alpha(\beta)) = \exp(-1/\beta)$, with

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

which is going from 1 to 0. Then we have

Theorem 3

In the model of successive generating transpositions, for any $\beta > 0$, there is a (K, T)-sharp transition for the non-existence of fixed point with

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

Again we conjecture this also holds for transitivity, as suggested by simulations.

Motivation

Our motivation: the design of algorithms for bivariate polynomials factorization. Very briefly, the zeros of a "generic" bivariate polynomial of degree N defines a smooth Riemann surface $X \subset \mathbb{C}^2$ and let $\pi : X \to \mathbb{C}$ denote the first projection. X has $N(N-1)$ points with a vertical tangent and let Δ be their projections by π. Suppose $0 \notin \Delta$ and denote by E, the fiber above 0. Next 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. They lead to a permutation p_γ on E, only depending on the homotopical class of γ in $\mathbb{C} \setminus \Delta$. γ can be decomposed into "small" loops each circling around only one discriminant point, whose corresponding permutation is a transposition. Then the question is to predict when a subgroup generated by K permutations themselves generated by the product of "small" loops has the same connecting effect on E as the whole monodromy group.

An easy upper bound 1

We begin with the proof of

$$\forall\, \alpha > 1, \qquad \lim_{N\to\infty} \mathbb{P}[B_{\alpha T(N,K)}] \;=\; 0$$

For any $x \in [\![1, N]\!]$, consider the event that x is a fixed point:

$$B_n(x) \;:=\; \{\forall\, i \in [\![1, K]\!], \quad Z_n^{(i)}(x) = x\}$$

so that $B_n = \cup_{x\in E_N} B_n(x)$ and

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

An easy upper bound 2

Note that $(Z_n(1))_{n\in\mathbb{N}}$ is a Markov chain, starting from 1 and whose transition matrix is $P = \frac{2}{N-1}M + \left(1 - \frac{2}{N-1}\right)\mathrm{Id}$ where where M is the transition matrix whose all entries are $1/N$. So we get

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

and we get

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

A concentration result 1

We want to show now that

$$\forall\, \alpha \in [0,1), \qquad \lim_{N\to\infty} \mathbb{P}[B_{\alpha T(N,K)}] \;=\; 1$$

Consider the number of fixed points at time $n \in \mathbb{N}$,

$$S_n \;=\; \sum_{x\in E_N} 1_{B_n(x)}$$

In the previous slide we computed $\mathbb{E}[S_n]$ and the above convergence is based on the fact that for $\alpha \in [0,1)$,

$$\lim_{N\to\infty} \frac{\mathrm{Var}(S_{\alpha T(N,K)})}{\mathbb{E}[S_{\alpha T(N,K)}]^2} \;=\; 0$$

Indeed, just write that, with $n_N = \alpha T(N,K)$,

$$\begin{aligned}
\mathbb{P}[B^c_{n_N}] &= \mathbb{P}[S_{n_N} = 0] \\
&\le \mathbb{P}[|S_{n_N} - \mathbb{E}[S_{n_N}]| \ge \mathbb{E}[S_{n_N}]] \\
&\le \frac{\mathrm{Var}(S_{n_N})}{\mathbb{E}[S_{n_N}]^2}
\end{aligned}$$

A concentration result 2

Note that $(X_m, Y_m)_{m\in\mathbb{N}} = (Z_m(1), Z_m(2))_{m\in\mathbb{N}}$ is a Markov chain starting from $(1, 2)$ and whose matrix transition is

$$P^{(2)}((x,y),(x',y')) = \begin{cases} \frac{2}{N(N-1)} & \text{, if } x' \neq x \text{ and } y' = y \\ \frac{2}{N(N-1)} & \text{, if } x' = x \text{ and } y' \neq y \\ \frac{2}{N(N-1)} & \text{, if } x' = y \text{ and } y' = x \\ 1 - \frac{4N-6}{N(N-1)} & \text{, if } x' = x \text{ and } y' = y \\ 0 & \text{, otherwise} \end{cases}$$

Its interest is that by symmetry, we have

$$\mathrm{Var}(S_n) = N(N-1)\mathbb{P}[X_n = 1, Y_n = 2]^K + \mathbb{E}[S_n] - \mathbb{E}^2[S_n]$$

Remove the exchange interaction by considering

A concentration result 3

$$\widetilde{P}^{(2)}((x,y),(x',y')) = \begin{cases} \frac{2}{N(N-1)} & \text{, if } x' \neq x \text{ and } y' = y \\ \frac{2}{N(N-1)} & \text{, if } x' = x \text{ and } y' \neq y \\ 1 - \frac{4}{N} & \text{, if } x' = x \text{ and } y' = y \\ 0 & \text{, otherwise} \end{cases}$$

The only interaction between the two particles is now the share of the time resource, in particular $\widetilde{P}_n^{(2)}$ can be computed explicitely and we have for large N,

$$\mathbb{P}[\widetilde{X}_{n_N} = 1, \widetilde{Y}_{n_N} = 2] \sim N^{-2\frac{\alpha}{K}}$$

The same is true for $\mathbb{P}[X_{n_N} = 1, Y_{n_N} = 2]$, because a simple coupling argument shows that

$$\left| \mathbb{P}[X_{n_N} = 1, Y_{n_N} = 2] - \mathbb{P}[\widetilde{X}_{n_N} = 1, \widetilde{Y}_{n_N} = 2] \right| = \mathcal{O}\left(\frac{\ln(N)}{N}\right)$$

A basic bound

The cut-off phenomena for fixed point already implies that

$$\forall\, \alpha \in [0,1), \qquad \lim_{N\to\infty} \mathbb{P}\left[A_{\alpha T(N,K)}\right] \;=\; 0$$

To get the opposite behavior for $\alpha > 1$, we write

$$\begin{aligned}
\mathbb{P}[A_n^{\mathrm{c}}] &\leq \sum_{R\in\mathcal{R}} \mathbb{P}[\forall\, k \in [\![1,K]\!],\, Z_n^{(k)}(R) = R] \\
&= \sum_{R\in\mathcal{R}} \mathbb{P}[Z_n(R) = R]^K \\
&= \sum_{r=1}^{\lfloor N/2 \rfloor} \binom{N}{r} \mathbb{P}[Z_n(\{1,\dots,r\}) = \{1,\dots,r\}]^K
\end{aligned}$$

where $\mathcal{R}$ is the set of nonempty subsets of $[\![1,N]\!]$.

Exclusion process

Note that $(Z_n(\{1, ..., r\}))_{n\in\mathbb{N}}$ is a Markov chain on the set of subsets of $[\![1, N]\!]$ whose cardinal is r, starting from $\{1, ..., r\}$ and whose transition matrix is

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

We can write it in terms of the adjacency matrix $M^{(r)}$ of the distance transitive Johnson graph $J(N, r)$ as

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

We deduce that the eigenvalues of $P^{(r)}$ are the $\theta_l = 1 - \frac{2l(N-l+1)}{N(N-1)}$ for $l \in [\![0, r]\!]$ with multiplicities $\binom{N}{l} - \binom{N}{l-1}$.
Due to the strong symmetries of this model, we have

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

Next we divide the last sum in three terms, corresponding to small, medium and large values of l (in a way depending on N), to get, after some tedious computations, that

$$\forall\, \alpha > 1, \qquad \lim_{N\to\infty} \mathbb{P}\left[A_{\alpha T(N,K)}\right] \;=\; 1$$

Remark: this kind of cut-off phenomenon is relatively stable by time-change, that is why it also holds for $\widetilde{\mu}$ defined after Theorem 1 or in continuous time.

Expectation of number of fixed points 1

With the same notations as before,

$$\mathbb{E}[S_n] = \sum_{x \in E_N} \mathbb{P}[B_n(x)] = \sum_{x \in E_N} \mathbb{P}[Z_n(x) = x]^K = N\mathbb{P}[X_n = 0]^K$$

where $(X_n)_{n\in\mathbb{N}}$ is a Markov chain on $\mathbb{Z}/(N\mathbb{Z})$, starting from 0 and whose transition matrix is

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

Its eigenvalues are known and we deduce

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

Expectation of number of fixed points 2

It follows that for any $\alpha \in (0, +\infty)$,

$$\lim_{N\to\infty} \mathbb{E}[S_{\alpha N^{1+\frac{2}{K}}}] \quad = \quad I^K(\alpha)$$

with $I(\alpha) := \frac{1}{2\sqrt{\pi\alpha}}$, and thus

$$\lim_{\alpha\to+\infty} \limsup_{N\to\infty} \mathbb{P}[B_{\alpha N^{1+\frac{2}{K}}}] \leq \lim_{\alpha\to+\infty} I^K(\alpha) = 0$$

and for any $\alpha > \alpha_* := \frac{1}{4\pi}$

$$\limsup_{N\to\infty} \mathbb{P}[B_{\alpha N^{1+\frac{2}{K}}}] \quad < \quad 1$$

This is the easy part of Theorem 2.

Variance of number of fixed points

To proceed, we need informations on the variance:

Proposition 4

Assume that $K \geq 3$, then we have for $\alpha > 0$,

$$\lim_{N\to\infty} \frac{\mathrm{Var}(S_{\alpha N^{1+\frac{2}{K}}})}{\mathbb{E}^2[S_{\alpha N^{1+\frac{2}{K}}}]} = I^{-K}(\alpha)$$

As a consequence, we get

$$\lim_{\alpha\to 0_+} \liminf_{N\to\infty} \mathbb{P}[B_{\alpha N^{1+\frac{2}{K}}}] \geq \lim_{\alpha\to 0_+} 1 - \frac{1}{I^K(\alpha)} = 1$$

Two interacting particles

The proof of Proposition 4 is more involved than before because of the lack of symmetry: the quantity $\mathbb{P}[Z_n(x) = x, Z_n(y) = y]$ now depends on $d(x, y)$. But the chain $(Z_n(x), Z_n(y))_{n\in\mathbb{N}}$ is again Markovian, with transition matrix

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

Let $\widetilde{P}^{(2)}$ be the corresponding transition matrix where the exchange interaction has been removed.

Coupling

If $P^{(2)}$ could be replaced by $\widetilde{P}^{(2)}$, Proposition 4 would follow easily. This suggests to couple the corresponding chains and we get that uniformly over $x, y \in \mathbb{Z}/(N\mathbb{Z})$ such that $d(x, y) \geq L$,

$$\left| P_n^{(2)}((x, y), (x, y)) - \widetilde{P}_n^{(2)}((x, y), (x, y)) \right| \leq \frac{2cn}{NL^2}$$

This leads to good estimates only if $x, y \in \mathbb{Z}/(N\mathbb{Z})$ are sufficiently apart. To deal with the remaining terms, we need a bound on $P_m^{(2)}((x, y), (x, y))$, not necessary sharp at the level of constants.

Indeed there exists a constant $c > 0$ such that

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

To show this, we consider the set $\mathbb{Z}^2 \setminus \{(x,x) \,:\, x \in \mathbb{Z}\}$ (with similar cross-diagonal links as those induced by $P^{(2)}$ on $(\mathbb{Z}/(N\mathbb{Z}))^2 \setminus \{(x,x) \,:\, x \in \mathbb{Z}/(N\mathbb{Z})\}$) and we couple the corresponding random walks, this leads to the term n/N^3. Next we apply a 2-dimensional isoperimetric inequality to get heat kernel type bounds on the chain living in $\mathbb{Z}^2 \setminus \{(x,x) \,:\, x \in \mathbb{Z}\}$, to deduce the term $N/(1+n)$.
The above bound is sufficient to end the proof of Proposition 4.

Bonferroni inequalities

To end the proof of Theorem 2, we use the general inequality

$$\begin{aligned}\mathbb{P}[B_n] &\geq \sum_{x\in E_N}\mathbb{P}[B_n(x)]-\sum_{x<y\in E_N}\mathbb{P}[B_n(x)\cap B_n(y)]\\ &= \frac{3}{2}\mathbb{E}[S_n]-\frac{1}{2}\mathbb{E}^2[S_n]-\frac{1}{2}\mathrm{Var}(S_n)\end{aligned}$$

The above computations then imply that for $\alpha > 0$,

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

and we get that $\liminf_{N\to\infty}\mathbb{P}[B_{\alpha N^{1+\frac{2}{K}}}] > 0$ for

$$\alpha > \inf\{\alpha' > 0 \,:\, I^K(\alpha') \leq 2\} < \alpha_*$$

Bonferroni inequalities enable to improve these estimate for larger K.

Expectation and variance 1

As for Theorem 1, it is sufficient to show the

Proposition 5

The crude asymptotical behavior of the expectation of the number $S(N, \alpha)$ of fixed points of the $\lfloor \beta \ln(N) \rfloor$ chains at time $\lfloor \alpha N \rfloor$ is

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

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

$$\lim_{N \to \infty} \frac{\mathrm{Var}(S(N, \alpha))}{\mathbb{E}^2[S(N, \alpha)]} = 0 \tag{1}$$

Expectation and variance 2

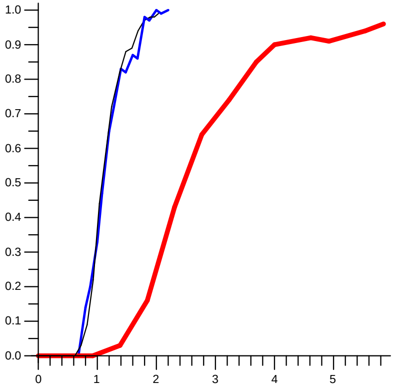
This comes from computations similar to ones presented above, in particular the explicit formula for the expectation leads to

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

and this explains how the function J and the value $\alpha(\beta)$ enter into the game. The proof for the variance is even easier than in the previous case, no isoperimetric inequality is needed.

Uniform: cut-off for transitivity

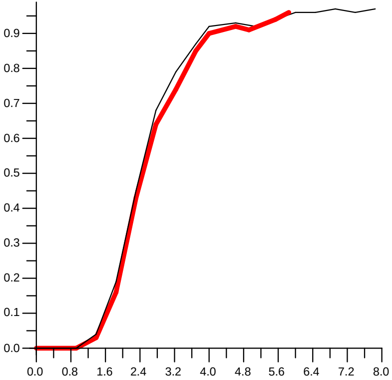
Illustration of Theorem 1:



$K = 4$, $N = 30, 50, 100$ and time is renormalized by $N \ln(N)/(2K)$.

Uniform: fixed point vs transitivity

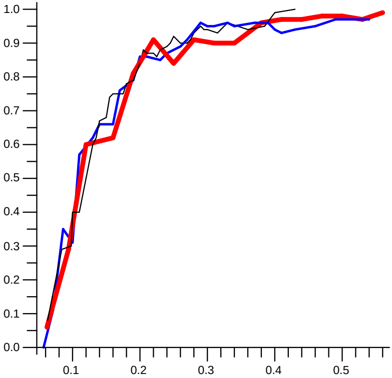
Illustration of Theorem 1 and its proof:



$K = 4$, $N = 30$ and time is renormalized by $N \ln(N)/(2K)$.

Successive: flared transition for fixed point

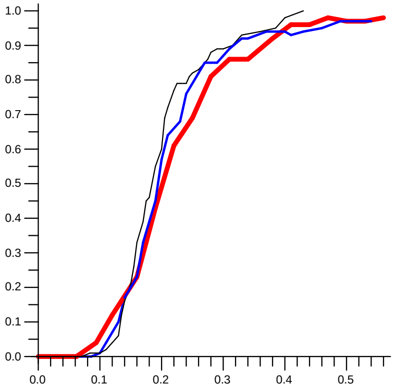
Illustration of Theorem 2:



$K = 4$, $N = 30, 50, 100$ and time is renormalized by $N^{1+\frac{2}{K}}$.

Successive: flared transition for transitivity

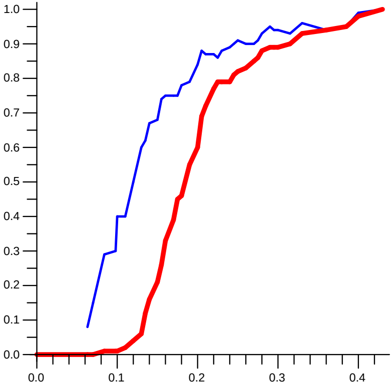
Illustration of conjecture relative to Theorem 2:



$K = 4$, $N = 30, 50, 100$ and time is renormalized by $N^{1+\frac{2}{K}}$.

Successive: fixed point vs transitivity

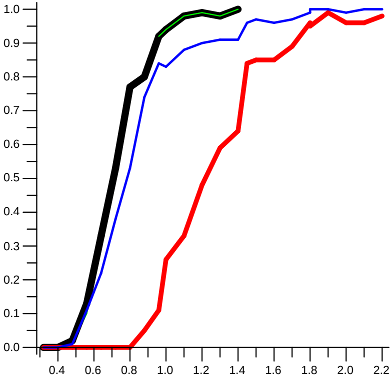
Illustration of the conjecture relative to Theorem 2:



$K = 4$, $N = 30$ and time is renormalized by $N^{1+\frac{2}{K}}$.

Uniform vs successive

Illustration of Theorem 3 and its conjecture:



$N = 50$, $K = 8 \approx 2\ln(N)$ and time is renormalized by $0.26N \approx N\ln(N)/(2K) \approx \alpha(2)N$.