Examen – Chaînes de Markov

24 octobre 2025

Durée : 3 heures. Les notes de cours (polycopiés ou notes manuscriptes) sont autorisées. Sont interdits : livres, calculatrices, téléphones, ordinateurs ou objets apparentés. Toutes les réponses doivent être justifiées ; la rédaction sera prise en compte. On pourra admettre un résultat d'une question précédente si nécessaire. Les questions plus difficiles sont marquées d'un symbole $(*)$.

Dans tout le sujet, $N \geq 1$ est un entier fixé, et on note $\mathfrak{S}(N)$ l'ensemble des bijections $\sigma : [\![1, N]\!] \to [\![1, N]\!]$. Une telle bijection sera donnée par la liste de ses valeurs entre crochets : $\sigma = [\sigma(1), \sigma(2), \dots, \sigma(N)]$. Par exemple, $[4, 2, 1, 3]$ est un élément de $\mathfrak{S}(4)$. On rappelle que $\mathfrak{S}(N)$ est de cardinal

$$|\mathfrak{S}(N)| = N! = 1 \times 2 \times 3 \times \cdots \times N.$$

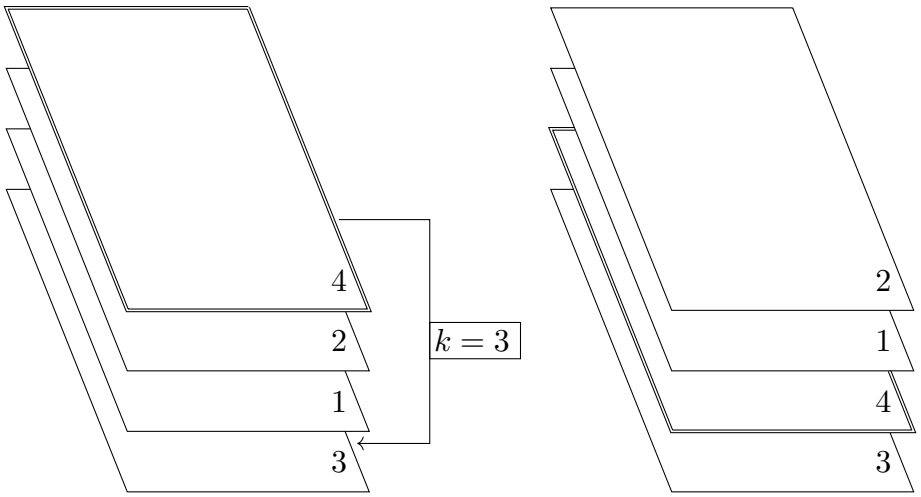
Les éléments de $\mathfrak{S}(N)$ seront également appelées *permutations*. L'ensemble $\mathfrak{S}(N)$ est un groupe pour la composition $\circ$ des bijections ; certaines questions ci-dessous utiliseront l'inverse σ^{-1} d'une bijection σ. Par exemple, l'inverse de la permutation $[4, 2, 1, 3]$ est $[3, 2, 4, 1]$. Si $i_1, i_2, \dots, i_l$ sont des entiers différents de $[\![1, N]\!]$, on notera $c = (i_1, i_2, \dots, i_l)$ le *cycle* défini par :

$$c(i_1) = i_2 \quad ; \quad c(i_2) = i_3 \quad ; \quad \cdots \quad ; \quad c(i_l) = i_1$$

et $c(x) = x$ si $x \notin \{i_1, i_2, \dots, i_l\}$. Par ailleurs, on notera $\mathrm{id} = \mathrm{id}_N$ la bijection identité : $\mathrm{id}(x) = x$ pour tout $x \in [\![1, N]\!]$. La bijection identité id est l'élément neutre du groupe $\mathfrak{S}(N)$.

1. La chaîne top-to-random

Supposons donné un paquet de N cartes numérotées $1, 2, \dots, N$. Si les cartes sont mélangées, l'ordre des cartes lorsqu'on les énumère du haut vers le bas du paquet peut être décrit par une permutation : la première carte en haut du paquet a un numéro $\sigma(1)$, la carte juste en-dessous a un numéro $\sigma(2)$, etc. jusqu'à la dernière carte en bas du paquet qui a pour numéro $\sigma(N)$; et σ est une permutation dans $\mathfrak{S}(N)$. Par exemple, si $N = 4$ et $\sigma = [\sigma(1), \sigma(2), \sigma(3), \sigma(4)] = [4, 2, 1, 3]$, alors le paquet de cartes a tout en haut la carte numéro 4, puis en-dessous la carte numéro 2, puis la carte numéro 1, et enfin tout en bas la carte numéro 3.



(1) Supposons que le paquet soit dans un ordre $\sigma \in \mathfrak{S}(N)$. Étant donné $k \in [\![2, n]\!]$, on retire la carte tout en haut du paquet, et on la replace à la k-ième position (les positions étant comptées de haut en bas). On note σ' le nouvel ordre du paquet de cartes. Par exemple, si $\sigma = [4, 2, 1, 3]$ et $k = 3$, alors $\sigma' = [2, 1, 4, 3]$. Écrire une formule qui relie σ, σ' et le cycle $c_k = (1, 2, \dots, k-1, k)$.

Si $k = 1$, le paquet de cartes est laissé invariant par la transformation décrite ci-dessus ; on notera donc $c_1 = \mathrm{id}$.

(2) La chaîne *top-to-random* est la suite de permutations aléatoires $(\sigma_n)_{n\in\mathbb{N}}$ dans $\mathfrak{S}(N)$ définie comme suit :

- On part avec les cartes ordonnées par ordre croissant dans le paquet : $\sigma_0 = \mathrm{id}_N$.
- À chaque temps $n \geq 1$:
  - on tire au hasard $k_n \in [\![1, N]\!]$ uniformément : $\mathbb{P}[k_n = k] = \frac{1}{N}$ pour tout k.
  - on applique au paquet de cartes d'ordre σ_{n-1} la transformation de la question précédente, en retirant la carte tout en haut du paquet et en la replaçant à la k_n-ième position.

On note σ_n le nouvel ordre des cartes du paquet.

On suppose les variables de la suite $(k_n)_{n\geq 1}$ indépendantes. Établir une relation reliant σ_{n-1}, σ_n et c_{k_n}. En déduire que $(\sigma_n)_{n\in\mathbb{N}}$ est une chaîne de Markov sur $\mathfrak{S}(N)$.

(3) On note P la matrice de transition de la chaîne de Markov $(\sigma_n)_{n\in\mathbb{N}}$. À quelle condition a-t-on $P(\sigma, \tau) \neq 0$? Donner dans ce cas la valeur de $P(\sigma, \tau)$.

(4) Montrer que la matrice P est bistochastique :

$$\forall \sigma \in \mathfrak{S}(N), \quad \sum_{\tau\in\mathfrak{S}(N)} P(\tau, \sigma) = 1.$$

(5) $(*)$ Soit $\sigma : [\![1, N]\!] \to [\![1, N]\!]$ une permutation. Montrer qu'il existe $r \geq 0$ tel que

$$\left(\sigma \circ \underbrace{(c_N \circ c_N \circ \cdots \circ c_N)}_{r \text{ termes}}\right)(N) = N.$$

En déduire que la chaîne de matrice P sur $\mathfrak{S}(N)$ est irréductible (on pourra faire une récurrence sur $N \geq 1$).

(6) Montrer que l'unique mesure invariante π de la matrice P est la loi uniforme sur $\mathfrak{S}(N)$:

$$\forall \sigma \in \mathfrak{S}(N), \ \ \pi(\sigma) = \frac{1}{N!}.$$

(7) Montrer que la chaîne de matrice P est apériodique.

(8) Soit π_n la loi marginale de σ_n : $\pi_n[\sigma] = \mathbb{P}[\sigma_n = \sigma]$. Par construction, $\pi_0 = \delta_{\mathrm{id}}$. Calculer pour toute permutation σ la limite $\lim_{n\to\infty} \pi_n(\sigma)$.

2. La position de la carte N

Dans cette section, on s'intéresse à la variable aléatoire

$$X_n = (\text{position de la carte numérotée } N \text{ dans le paquet au temps } n).$$

On rappelle qu'une variable géométrique G de paramètre p (notation : $G \sim \mathrm{Geom}(p)$) est une variable à valeurs dans $\{1, 2, 3, ...\}$ telle que

$$\mathbb{P}[G = t] = (1 - p)^{t-1}\, p \quad \text{pour tout } t \geq 1.$$

(1) Comment exprimer X_n en fonction de σ_n (indication : la position de la carte numérotée N *n'est pas* $\sigma_n(N)$) ?

(2) Montrer que $(X_n)_{n\in\mathbb{N}}$ est une chaîne de Markov sur $[\![1,N]\!]$.

Initialement, la carte N est en bas du paquet (position $X_0 = N$). Elle y reste jusqu'à ce que la carte en haut du paquet soit insérée tout en bas ($k_n = N$), et à ce moment-là elle se retrouve en position $N-1$.

(3) Notons $T_{N-1} = \inf(\{n \in \mathbb{N} \,|\, X_n = N-1\})$ le temps d'atteinte de la position $N-1$ par la carte numérotée N. Montrer que T_{N-1} suit une loi géométrique de paramètre $p = \frac{1}{N}$.

(4) Plus généralement, pour $m \in [\![1,N]\!]$, on note $T_m = \inf(\{n \in \mathbb{N} \,|\, X_n = m\})$. Par convention, $T_N = 0$. Montrer que

$$0 = T_N < T_{N-1} < T_{N-2} < \cdots < T_1.$$

Si $T_{m+1} \leq n < T_m$, que vaut X_n ?

(5) (∗) Montrer que les variables $(T_m - T_{m+1})_{m\in[\![1,N-1]\!]}$ sont des variables géométriques indépendantes, avec $T_m - T_{m+1} \sim \mathrm{Geom}(\frac{N-m}{N})$. On pourra réécrire un événement

$$T_{N-1} = t_{N-1},\, T_{N-2} - T_{N-1} = t_{N-2}, \ldots, T_1 - T_2 = t_1$$

en fonction des valeurs prises par les variables aléatoires $k_{n\geq 1}$.

(6) En utilisant la série entière $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$ et sa dérivée, montrer que l'espérance d'une variable géométrique $G \sim \mathrm{Geom}(p)$ est $\mathbb{E}[G] = \frac{1}{p}$.

(7) On pose $T = 1 + T_1$. Montrer que

$$\mathbb{E}[T] = N\left(\sum_{m=1}^{N} \frac{1}{m}\right).$$

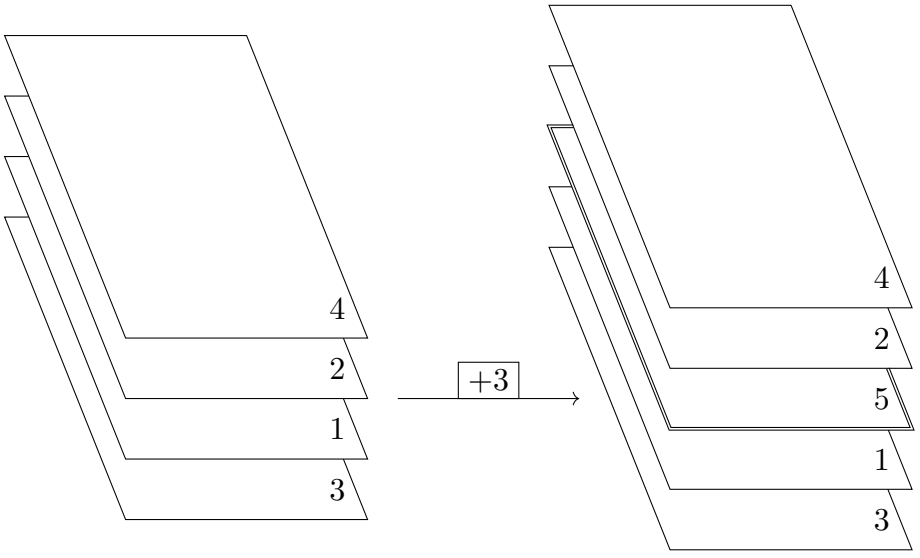
Ceci implique que $\mathbb{E}[T] \simeq N \log N$ lorsque N tend vers l'infini.

3. Le temps de mélange

Soit $\rho_{N-1} \in \mathfrak{S}(N-1)$ une permutation, dont on note les valeurs dans l'ordre : $\rho_{N-1} = [\rho_{N-1}(1), \rho_{N-1}(2), \ldots, \rho_{N-1}(N-1)]$. Pour $j \in [\![1,N]\!]$, on note :

$$\rho_N = \rho_{N-1} + j = [\rho_{N-1}(1), \ldots, \rho_{N-1}(j-1), N, \rho_{N-1}(j), \ldots, \rho_{N-1}(N-1)]$$

la permutation dans $\mathfrak{S}(N)$ obtenue en insérant N en j-ième position dans la liste des valeurs de ρ_{N-1}. Par exemple, si $\rho_4 = [4,2,1,3]$ et $j = 3$, alors $\rho_5 = \rho_4 + 3 = [4,2,5,1,3]$.



(1) On suppose que ρ_{N-1} est une permutation aléatoire de loi uniforme sur $\mathfrak{S}(N-1)$: pour toute permutation $\sigma \in \mathfrak{S}(N-1)$, $\mathbb{P}[\rho_{N-1} = \sigma] = \frac{1}{(N-1)!}$. Soit j_N une variable aléatoire de loi uniforme dans $[\![1, N]\!]$, indépendante de ρ_{N-1}. Si $\rho_N = \rho_{N-1} + j_N$, montrer que la loi de ρ_N est uniforme sur $\mathfrak{S}(N)$.

La section précédente a montré que la carte N remontait progressivement dans le paquet de cartes, jusqu'au temps T_1 où elle se retrouve tout en haut du paquet. On note i_1 le numéro de la carte insérée sous la carte numérotée N au temps T_{N-1} ; i_2 le numéro de la carte insérée au temps T_{N-2} parmi les cartes sous la carte numérotée N ; etc. jusqu'à i_{N-1} le numéro de la carte insérée au temps T_1 parmi les cartes sous la carte numérotée N. Au temps T_{N-m}, la carte N a sous elle les cartes numérotées $i_1, i_2, \dots, i_m$, dans un ordre décrit par une permutation ρ_m de taille m :

$$\sigma_{T_{N-m}} = [\dots, N, i_{\rho_m(1)}, \dots, i_{\rho_m(m)}].$$

Dans cette écriture où l'on ne précise pas les $N-(m+1)$ premières valeurs, les indices $i_1, \dots, i_m$ sont aléatoires, ainsi que la permutation ρ_m.

(2) Pour $m \in [\![1, N-1]\!]$, établir une relation entre ρ_{m-1}, ρ_m et $k_{T_{N-m}}$. En déduire que la permutation ρ_m suit une loi uniforme sur $\mathfrak{S}(m)$.

(3) $(*)$ Si $T_{N-1} = t_{N-1}, \dots, T_1 = t_1$, exprimer en fonction de valeurs $\sigma_n(1)$ avec des temps n bien choisis les indices $i_1, \dots, i_{N-1}$. En déduire que pour $m \in [\![1, N-1]\!]$, $(i_1, \dots, i_m)$ et ρ_m sont indépendants.

(4) On rappelle que $T = 1 + T_1$; à cet instant, la carte numérotée N qui était en haut du paquet au temps T_1 est réinsérée aléatoirement dans le paquet. Montrer que la permutation σ_T suit une loi uniforme sur $\mathfrak{S}(N)$.

On peut utiliser ce résultat et celui à la fin de la seconde section pour montrer que le temps de mélange de ce modèle de permutations aléatoires est $N \log N$: si $n \geq N \log N$, alors la loi de σ_n est presque uniforme sur $\mathfrak{S}(N)$.

Corrigé

I.1 Si $\sigma = [\sigma(1), \sigma(2), \dots, \sigma(k), \sigma(k+1), \dots, \sigma(N)]$ et si l'on replace en k-ième position la première carte, on obtient

$$\begin{aligned}\sigma' &= [\sigma(2), \dots, \sigma(k), \sigma(1), \sigma(k+1), \dots, \sigma(N)] \\ &= [\sigma(c_k(1)), \dots, \sigma(c_k(k-1)), \sigma(c_k(k)), \sigma(c_k(k+1)), \dots, \sigma(c_k(N))] \\ &= \sigma \circ c_k.\end{aligned}$$

I.2 La question précédente donne $\sigma_n = \sigma_{n-1} \circ c_{k_n}$. On a donc une fonction

$$\begin{aligned}F : \mathfrak{S}(N) \times [\![1, N]\!] &\to \mathfrak{S}(N) \\ \sigma, k &\mapsto \sigma \circ c_k\end{aligned}$$

telle que $\sigma_n = F(\sigma_{n-1}, k_n)$, et les variables $(k_n)_{n\geq 1}$ sont indépendantes (et indépendantes de la variable aléatoire constante $\sigma_0 = \mathrm{id}$). Par le théorème de représentation des chaînes de Markov, $(\sigma_n)_{n\in\mathbb{N}}$ est une chaîne de Markov sur $\mathfrak{S}(N)$.

I.3 Le théorème de représentation donne :

$$P(\sigma, \tau) = \mathbb{P}[F(\sigma, K) = \tau] = \mathbb{P}[\sigma \circ c_K = \tau] = \mathbb{P}[c_K = \sigma^{-1} \circ \tau]$$

avec K variable uniforme dans $[\![1, N]\!]$. Cette probabilité vaut 0 si $\sigma^{-1} \circ \tau$ n'est pas un cycle de la forme c_k, et elle vaut $\frac{1}{N}$ si $\sigma^{-1} \circ \tau = c_k$ pour un certain $k \in [\![1, N]\!]$.

I.4 Compte tenu de la question précédente,

$$\sum_{\tau\in\mathfrak{S}(N)} P(\tau, \sigma) = \sum_{k=1}^{N} P(\sigma \circ (c_k)^{-1}, \sigma) = \sum_{k=1}^{N} \frac{1}{N} = 1.$$

La matrice de transition est donc bistochastique.

I.5 Soit r_N l'unique entier de $[\![1, N]\!]$ tel que $\sigma(r_N) = N$. On a $(c_N)^{r_N}(N) = r_N$, et donc $(\sigma \circ (c_N)^{r_N})(N) = \sigma(r_N) = N$. Montrons alors par récurrence sur $N \geq 1$: pour toute permutation $\sigma \in \mathfrak{S}(N)$, il existe des entiers $r_1, \dots, r_N \geq 0$ tels que

$$\sigma \circ (c_N)^{r_N} \circ (c_{N-1})^{r_{N-1}} \circ \cdots \circ (c_2)^{r_2} \circ (c_1)^{r_1} = \mathrm{id}_N.$$

Le cas $N = 1$ est trivial (et on peut prendre $r_1 = 0$). Si le résultat est vrai jusqu'au rang $N-1$ et si $\sigma \in \mathfrak{S}(N)$, remarquons que la permutation $\sigma \circ (c_N)^{r_N}$ précédemment exhibée envoie N sur N et donc $[\![1, N-1]\!]$ sur $[\![1, N-1]\!]$. Sa restriction à $[\![1, N-1]\!]$ est donc une bijection, et par hypothèse de récurrence, il existe des indices $r_1, \dots, r_{N-1}$ tels que

$$(\sigma \circ (c_N)^{r_N})|_{[\![1,N-1]\!]} \circ (c_{N-1})^{r_{N-1}} \circ \cdots (c_2)^{r_2} \circ (c_1)^{r_1} = \mathrm{id}_{N-1}.$$

Tous les termes de la composée laisse N invariant, donc on a en fait :

$$(\sigma \circ (c_N)^{r_N}) \circ (c_{N-1})^{r_{N-1}} \circ \cdots \circ (c_2)^{r_2} \circ (c_1)^{r_1} = \mathrm{id}_N,$$

et le cas N de la récurrence est établi.

La propriété établie ci-dessus montre que toute permutation σ communique avec l'identité. Remarquons de plus que chaque entier r_k peut être choisi dans $[\![0, k-1]\!]$, puisque $(c_k)^k = \mathrm{id}$. Alors, si

$$\sigma \circ (c_N)^{r_N} \circ (c_{N-1})^{r_{N-1}} \circ \cdots \circ (c_2)^{r_2} \circ (c_1)^{r_1} = \mathrm{id},$$

on obtient en inversant les cycles :

$$\begin{aligned}\sigma &= (c_1)^{-r_1} \circ (c_2)^{-r_2} \circ \cdots \circ (c_{N-1})^{-r_{N-1}} \circ (c_N)^{-r_N} \\ &= (c_1)^{1-r_1} \circ (c_2)^{2-r_2} \circ \cdots \circ (c_{N-1})^{N-1-r_{N-1}} \circ (c_N)^{N-r_N}.\end{aligned}$$

Ceci prouve qu'inversement, l'identité communique avec toute permutation σ. Alors, si σ et τ sont deux permutations arbitraires, il existe un chemin $\sigma \to \mathrm{id}$ dans le graphe associé à la matrice P, et un chemin $\mathrm{id} \to \tau$, donc par concaténation un chemin $\sigma \to \tau$. La matrice P est donc irréductible.

I.6 La propriété de bistochasticité implique que la mesure uniforme $\pi(\sigma) = \frac{1}{N!}$ est invariante par P :

$$(\pi P)(\sigma) = \frac{1}{N!} \sum_{\tau \in \mathfrak{S}(N)} P(\tau, \sigma) = \frac{1}{N!} = \pi(\sigma).$$

I.7 Pour toute permutation σ, 1 est dans l'ensemble des temps de retour possibles en σ, car $P(\sigma, \sigma) = \frac{1}{N} \neq 0$. La chaîne est donc apériodique.

I.8 Comme P est irréductible apériodique sur un espace fini, et donc automatiquement récurrente positive, par le théorème de convergence vers la loi stationnaire, π_n converge vers la loi invariante :

$$\forall \sigma \in \mathfrak{S}(N), \quad \lim_{n \to \infty} \pi_n(\sigma) = \frac{1}{N!}.$$

II.1 On a $X_n = (\sigma_n)^{-1}(N)$.

II.2 Par conséquent,

$$X_n = (\sigma_n)^{-1}(N) = (\sigma_{n-1} \circ c_{k_n})^{-1}(N) = (c_{k_n})^{-1}\left((\sigma_{n-1})^{-1}(N)\right) = (c_{k_n})^{-1}(X_{n-1}).$$

Ainsi, il existe une application

$$\begin{aligned} F : [\![1, N]\!] \times [\![1, N]\!] &\to [\![1, N]\!] \\ x, k &\mapsto (c_k)^{-1}(x) \end{aligned}$$

telle que $X_n = F(X_{n-1}, k_n)$, avec des variables $(k_n)_{n \geq 1}$ indépendantes. Par le théorème de représentation des chaînes de Markov, $(X_n)_{n \in \mathbb{N}}$ est une chaîne de Markov sur $[\![1, N]\!]$.

II.3 La carte N monte d'une position dans le paquet la première fois que la carte du haut du paquet est replacée en N-ième position. On a donc :

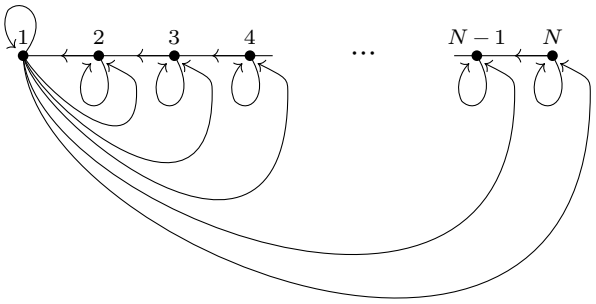
$$T_{N-1} = \inf(\{n \in \mathbb{N} \mid k_n = N\}).$$

Si l'on considère la suite d'expériences de Bernoulli indépendantes dont les succès sont $(k_n = N)$, alors T_{N-1} est l'indice du premier succès. La variable T_{N-1} est donc géométrique, de paramètre $p = \mathbb{P}[k_n = N] = \frac{1}{N}$.

II.4 Notons que si $X_n = m$ avec $m \geq 2$, alors il y a deux possibilités pour $X_{n+1} = (c_{k_{n+1}})^{-1}(X_n) = (k_{n+1}, k_{n+1} - 1, \ldots, 2, 1)(X_n)$:

- si $k_{n+1} \geq m$, alors $X_{n+1} = X_n - 1$: une carte est insérée sous la carte numéro N, qui remonte d'un rang.
- si $k_{n+1} < m$, alors $X_{n+1} = X_n$: une carte est insérée au-dessus de la carte numéro N, qui ne change pas de position.

Si $X_n = 1$, la carte numéro N est à l'étape d'après réinsérée n'importe où dans le paquet, donc X_{n+1} peut être n'importe quelle valeur dans $[\![1, N]\!]$. Autrement dit, le graphe de la chaîne de Markov $(X_n)_{n \in \mathbb{N}}$ est le suivant :



Par conséquent, la suite $(X_n)_{n\geq 0}$ est croissante au moins jusqu'au temps T_1, avec des sauts 0 ou +1. Elle atteint successivement les niveaux $N-1$, $N-2$, etc. aux temps $T_{N-1} < T_{N-2} < \cdots < T_1$. Entre les instants T_{m+1} inclus et T_m exclus, $X_n = m+1$.

II.5 Fixons des entiers $t_1, t_2, \ldots, t_{N-1} \geq 1$. Remarquons que les événements

$$(T_{N-1} = t_{N-1},\ T_{N-2} - T_{N-1} = t_{N-2},\ \ldots, T_1 - T_2 = t_1)$$

et

$$\begin{aligned}
&k_1, \ldots, k_{t_{N-1}-1} > N,\ \ k_{t_{N-1}} \leq N,\\
&k_{t_{N-1}+1}, \ldots, k_{t_{N-1}+t_{N-2}-1} > N-1,\ \ k_{t_{N-1}+t_{N-2}} \leq N-1,\\
&\quad\vdots \qquad\qquad \vdots\\
&k_{t_{N-1}+\cdots+t_2+1}, \ldots, k_{t_{N-1}+\cdots+t_1-1} > 2,\ \ k_{t_{N-1}+\cdots+t_1} \leq 2
\end{aligned}$$

sont les mêmes. Par indépendance des variables k_n, le second événement a pour probabilité

$$\left(\frac{N-1}{N}\right)^{t_{N-1}-1} \frac{1}{N} \left(\frac{N-2}{N}\right)^{t_{N-2}-1} \frac{2}{N} \cdots \left(\frac{1}{N}\right)^{t_1-1} \frac{N-1}{N}.$$

Si G_m désigne une variable géométrique de paramètre $\frac{N-m}{N}$ et si les G_m sont indépendantes, alors la formule ci-dessus est la loi jointe

$$\mathbb{P}[G_{N-1} = t_{N-1},\ G_{N-2} = t_{N-2}, \ldots, G_1 = t_1].$$

II.6 En dérivant l'expression $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$, on obtient :

$$\frac{1}{(1-z)^2} = \sum_{n=1}^{\infty} n\, z^{n-1}.$$

Donc, $\sum_{n=1}^{\infty} n\,(1-p)^{n-1} = \frac{1}{p^2}$, et $\mathbb{E}[G] = \sum_{n=1}^{\infty} n\,(1-p)^{n-1}p = \frac{p}{p^2} = \frac{1}{p}$.

II.7 On déduit des questions précédentes la formule pour $\mathbb{E}[T]$:

$$\begin{aligned}
\mathbb{E}[T] &= 1 + \sum_{m=1}^{N-1} \mathbb{E}[T_m - T_{m+1}] = 1 + \sum_{m=1}^{N-1} \mathbb{E}[G_m]\\
&= 1 + \sum_{m=1}^{N-1} \frac{N}{N-m} = 1 + \sum_{m=1}^{N-1} \frac{N}{m} = \sum_{m=1}^{N} \frac{N}{m}.
\end{aligned}$$

III.1 Soit τ une permutation de taille N. Notons qu'il existe une unique paire (σ, j) avec $\sigma \in \mathfrak{S}(N-1)$ et $j \in [\![1, N]\!]$ telle que $\tau = \sigma + j$: en effet, j est la position de N dans la liste des valeurs de τ (autrement dit, $j = \tau^{-1}(N)$), et σ est obtenue à partir de τ en retirant la valeur N de $[\tau(1), \tau(2), \ldots, \tau(N)]$.

Alors, si $\tau \in \mathfrak{S}(N)$ et (σ, j) est la paire associée, on a :

$$\mathbb{P}[\rho_N = \tau] = \mathbb{P}[\rho_{N-1} = \sigma \text{ et } j_N = j] = \mathbb{P}[\rho_{N-1} = \sigma]\,\mathbb{P}[j_N = j] = \frac{1}{(N-1)!}\,\frac{1}{N} = \frac{1}{N!}$$

en utilisant l'unicité de la décomposition pour la première égalité, et l'indépendance de ρ_{N-1} et de j_N pour la seconde égalité. Ainsi, la loi de ρ_N est uniforme sur $\mathfrak{S}(N)$.

III.2 Pour $m \in [\![1, N-1]\!]$, i_m est le numéro de la carte insérée sous la carte N au temps T_{N-m}. Cet indice i_m est choisi dans $[\![1, N-1]\!] \setminus \{i_1, \dots, i_{m-1}\}$, et on a ensuite :

$$\rho_m = \rho_{m-1} + (k_{T_{N-m}} - (N-m)).$$

En effet, au temps T_{N-m}, la carte i_m qui était en haut du paquet est insérée en position $k_{T_{N-m}}$, donc

$$\sigma_{T_{N-m}} = \left[\underbrace{\dots}_{N-1-m \text{ valeurs}}, N, i_{\rho_{m-1}(1)}, \dots, i_{\rho_{m-1}(m-1)}\right] + (i_m \text{ insérée en position } k_{T_{N-m}})$$

$$= \left[\underbrace{\dots}_{N-1-m \text{ valeurs}}, N\right] \cdot \left([i_{\rho_{m-1}(1)}, \dots, i_{\rho_{m-1}(m-1)}] + (i_m \text{ insérée en position } k_{T_{N-m}} - (N-m))\right)$$

où sur la deuxième ligne $\cdot$ indique la concaténation de deux suites de valeurs.

On est presque dans la situation de la question précédente, mais avec une variable aléatoire $k_{T_{N-m}} - (N-m)$ qui est construite à partir d'une suite de variables indépendantes *en prenant un indice aléatoire*. Pour montrer par récurrence sur m que ρ_m suit une loi uniforme sur $\mathfrak{S}(m)$, il va falloir établir l'indépendance de ρ_{m-1} et de $k_{T_{N-m}} - (N-m)$. La façon la plus claire de faire cela est de décomposer en fonction des valeurs $s = T_{N-m+1} \geq 0$ et $t = T_{N-m} - T_{N-m+1}$. Si $s = T_{N-m+1}$ est fixé, alors ρ_{m-1} ne dépend que de $\sigma_0, \dots, \sigma_s$, et donc de $k_1, \dots, k_s$; il existe donc un ensemble $K(s, \sigma) \subset [\![1, N]\!]^s$ tel que $\rho_{m-1} = \sigma$ si et seulement si $(k_1, \dots, k_s) \in K(s, \sigma)$. Par ailleurs,

$$\begin{aligned}&\left(T_{N-m} - T_{N-m+1} = t,\ k_{T_{N-m}} - (N-m) = j\right)\\ &\Leftrightarrow \left(k_{s+1}, \dots, k_{s+t-1} \leq N-m,\ k_{s+t} = N-m+j\right).\end{aligned}$$

On peut donc écrire, pour $\sigma \in \mathfrak{S}(N-1)$ et $j \in [\![1, m]\!]$:

$$\begin{aligned}&\mathbb{P}[\rho_{m-1} = \sigma,\ k_{T_{N-m}} - (N-m) = j]\\ &= \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma),\ T_{N-m} - T_{N-m+1} = t,\ k_{T_{N-m}} - (N-m) = j]\\ &= \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma),\ k_{s+1}, \dots, k_{s+t-1} \leq N-m,\ k_{s+t} = N-m+j]\\ &= \frac{1}{N} \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma),\ k_{s+1}, \dots, k_{s+t-1} \leq N-m]\\ &= \frac{1}{m} \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma),\ k_{s+1}, \dots, k_{s+t-1} \leq N-m,\ k_{s+t} > N-m]\\ &= \frac{1}{m} \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma),\ T_{N-m} - T_{N-m+1} = t]\\ &= \frac{1}{m} \sum_{\substack{s\geq 0\\ t\geq 1}} \mathbb{P}[(k_1, \dots, k_s) \in K(s,\sigma)] = \frac{1}{m}\,\mathbb{P}[\rho_{m-1} = \sigma],\end{aligned}$$

d'où l'indépendance de ρ_{m-1} et de $k_{T_{N-m}} - (N-m)$, et l'uniformité de la deuxième variable dans $[\![1,m]\!]$. La question précédente permet de conclure que ρ_m est uniforme dans $\mathfrak{S}(m)$ pour tout $m \in [\![1, N-1]\!]$.

III.3 On a $i_m = \sigma_{T_{N-m}-1}(1)$: c'est la valeur de la carte en haut du paquet juste avant le temps T_{N-m}. Fixons une suite de valeurs distinctes $(a_1, \dots, a_m) \in [\![1, N-1]\!]^m$, ainsi qu'une permutation $\tau \in \mathfrak{S}(m)$, qui est déterminée par des insertions successives :

$$\tau = [\ ] + j_1 + j_2 + \cdots + j_m$$

avec chaque $j_l \in [\![1, l]\!]$. On a :

$$\begin{aligned}
&\mathbb{P}[(i_1, \dots, i_m) = (a_1, \dots, a_m),\ \rho_m = \tau] \\
&= \sum_{t_{N-1} < t_{N-2} < \cdots < t_{N-m}} \mathbb{P}[(i_1, \dots, i_m) = (a_1, \dots, a_m),\ \rho_m = \tau,\ T_{N-1} = t_{N-1}, \dots, T_{N-m} = t_{N-m}] \\
&= \sum_{t_{N-1} < t_{N-2} < \cdots < t_{N-m}} \mathbb{P}[A \cap B \cap C]
\end{aligned}$$

avec dans la dernière somme :

$$\begin{aligned}
A &= \{\sigma_{t_{N-1}-1}(1) = i_1, \dots, \sigma_{t_{N-m}-1}(1) = i_m\}; \\
B &= \{k_1, \dots, k_{t_{N-1}-1} \leq N-1, \dots, k_{t_{N-m-1}+1}, \dots, k_{t_{N-m}-1} \leq N-m\}; \\
C &= \{k_{t_{N-1}} = (N-1) + j_1, \dots, k_{t_{N-m}} = (N-m) + j_m\}.
\end{aligned}$$

On aimerait découpler l'événement C de $A \cap B$. Dans l'événement A, la première valeur ne dépend que de $k_1, \dots, k_{t_{N-1}-1}$:

$$\sigma_{t_{N-1}-1} = c_{k_1} \circ c_{k_2} \circ \cdots \circ c_{k_{t_{N-1}-1}}.$$

Cela ne semble pas aussi simple pour les permutations ultérieures ; par exemple,

$$\sigma_{t_{N-2}-1} = c_{k_1} \circ c_{k_2} \circ \cdots \circ c_{k_{t_{N-1}-1}} \circ c_{k_{t_{N-1}}} \circ c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}}$$

semble mettre en jeu la variable $k_{t_{N-1}}$. Néanmoins, les temps $t_1, \dots, t_{N-1}$ étant fixés, on a $k_{t_{N-1}+1}, \dots, k_{t_{N-2}-1} \leq N-2$ et donc $c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}}(1) \leq N-2$. Comme $k_{t_{N-1}} \geq N$, ceci implique que

$$c_N \circ c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}}(1) = c_{k_{t_{N-1}}} \circ c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}}(1).$$

Autrement dit, on peut remplacer $k_{t_{N-1}}$ par N pour calculer la seconde valeur :

$$\sigma_{t_{N-2}-1}(1) = c_{k_1} \circ c_{k_2} \circ \cdots \circ c_{k_{t_{N-1}-1}} \circ c_N \circ c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}}(1).$$

Le même argument montre que pour tout $m \in [\![1, N-1]\!]$, $\sigma_{t_{N-m}-1}(1)$ peut être calculé en remplaçant $k_{t_{N-1}}, \dots, k_{t_{N-m+1}}$ par $N, N-1, \dots, N-m+2$:

$$\begin{aligned}
&\sigma_{t_{N-m}-1}(1) \\
&= c_{k_1} \circ \cdots \circ c_{k_{t_{N-1}-1}} \circ c_N \circ c_{k_{t_{N-1}+1}} \circ \cdots \circ c_{k_{t_{N-2}-1}} \circ c_{N-1} \circ \cdots \\
&\quad \circ c_{N-m+2} \circ c_{k_{t_{N-m+1}+1}} \circ \cdots \circ c_{k_{t_{N-m}-1}}(1).
\end{aligned}$$

Par indépendance des k_n, C est donc indépendant de $A \cap B$, et

$$\mathbb{P}[C] = \left(\frac{1}{N}\right)^m = \frac{1}{m!}\,\mathbb{P}[k_{t_{N-1}} > (N-1), \dots, k_{t_{N-m}} > (N-m)].$$

Si $C' = \{k_{t_{N-1}} > (N-1), \dots, k_{t_{N-m}} > (N-m)\}$, alors

$$A \cap B \cap C' = \{(i_1, \dots, i_m) = (a_1, \dots, a_m),\ T_{N-1} = t_{N-1}, \dots, T_{N-m} = t_{N-m}\},$$

donc

$$\begin{aligned}
&\mathbb{P}[(i_1,\dots,i_m)=(a_1,\dots,a_m),\ \rho_m=\tau]\\
&=\frac{1}{m!}\sum_{t_{N-1}<t_{N-2}<\cdots<t_{N-m}}\mathbb{P}[(i_1,\dots,i_m)=(a_1,\dots,a_m),\ T_{N-1}=t_{N-1},\dots,T_{N-m}=t_{N-m}]\\
&=\frac{1}{m!}\,\mathbb{P}[(i_1,\dots,i_m)=(a_1,\dots,a_m)].
\end{aligned}$$

III.4 Remarquons que $\{i_1,\dots,i_{N-1}\}=[\![1,N-1]\!]$. On ne connaît pas la distribution de la suite $(i_1,\dots,i_{N-1})$: c'est une permutation aléatoire $i\in\mathfrak{S}(N-1)$. Néanmoins, puisque i et ρ_{N-1} sont indépendants, pour toute permutation $\tau\in\mathfrak{S}(N-1)$,

$$\mathbb{P}[i\circ\rho_{N-1}=\tau]=\sum_{\nu\in\mathfrak{S}(N-1)}\mathbb{P}[i=\nu,\ \rho_{N-1}=\nu^{-1}\circ\tau]=\sum_{\nu\in\mathfrak{S}(N-1)}\frac{\mathbb{P}[i=\nu]}{(N-1)!}=\frac{1}{(N-1)!}.$$

Comme $[\sigma(2),\dots,\sigma(N)]=[i\circ\rho_{N-1}(1),\dots,i\circ\rho_{N-1}(N-1)]$, on a donc montré qu'au temps T_1, les $N-1$ dernières valeurs de la permutation σ_{T_1} sont réparties suivant une loi uniforme sur $\mathfrak{S}(N-1)$. Comme σ_T est obtenue en insérant N au hasard à l'une des N positions possibles dans cette permutation, de nouveau par la première question de cette section, ceci implique que σ_T suit une loi uniforme sur $\mathfrak{S}(N)$.