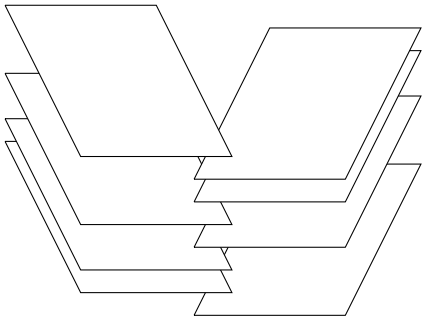
Temps de mélange du *riffle shuffle*

L'objectif du devoir est d'étudier la marche aléatoire sur $\mathfrak{S}(N)$ qui correspond au battage des cartes tel qu'il est effectué dans les casinos : à chaque instant $n \in \mathbb{N}$, on coupe le paquet de cartes en deux parties, et on remélange les deux blocs en les entrelaçant comme représenté sur la figure ci-dessous.



Ce mélange est appelé en anglais le *riffle shuffle* (nous l'appellerons simplement *battage*), et il a été étudié en détail dans les années 90 par Diaconis et ses coauteurs. Le sujet se décompose comme suit :

— Dans la première partie, on précise le modèle de marche aléatoire, et on introduit les notions de *descentes* et de *retours* d'une permutation, qui jouent un rôle essentiel dans l'analyse du modèle.

— Dans la seconde partie, on introduit l'*algèbre de Bayer–Diaconis* $\mathfrak{BD}(N)$: c'est une sous-algèbre commutative de $\mathbb{C}\mathfrak{S}(N)$ qui contient le générateur μ du battage, et donc toutes les lois marginales μ_n de la marche. On calcule la loi marginale μ_n pour tout entier $n \in \mathbb{N}$, et on exhibe une base d'idempotents dans $\mathfrak{BD}(N)$, ce qui permet de déterminer la structure de cette algèbre.

— Dans la troisième partie, on montre que le battage vérifie un phénomène de coupure, avec un temps de mélange $n_{\text{mix}} = \frac{3 \log N}{2 \log 2}$.

1 Battage de cartes, descentes et retours

Si $v = v_1 v_2 \cdots v_r$ et $w = w_1 w_2 \cdots w_s$ sont deux mots dont toutes les lettres sont distinctes, on note $v \sqcup\!\sqcup w$ l'ensemble des mots u de longueur $r + s$ vérifiant les deux propriétés suivantes :

— L'ensemble des lettres de u est $\{v_1, \ldots, v_r, w_1, \ldots, w_s\}$.

— Le sous-mot extrait de u en conservant uniquement les lettres $v_1, \ldots, v_r$ (respectivement, les lettres $w_1, \ldots, w_s$) est le mot v (respectivement, le mot w).

Par exemple,

$$312 \sqcup\!\sqcup 54 = \{31254, 31524, 35124, 53124, 31542, 35142, 53142, 35412, 53412, 54312\}.$$

Par convention, dans le cas où l'un des mots est de longueur 0, on pose $v \sqcup\!\sqcup \emptyset = \{v\}$ et $\emptyset \sqcup\!\sqcup w = \{w\}$. Le battage de cartes est la chaîne de Markov $(\sigma_n)_{n \in \mathbb{N}}$ sur $\mathfrak{S}(N)$ issue de $\sigma_0 = \mathrm{id}_{[1,N]}$, et dont les transitions $\sigma_n \to \sigma_{n+1}$ sont réalisées comme suit :

— On tire au hasard un entier $k_n \in [\![0, N]\!]$ suivant une loi binomiale $\mathcal{B}(N, \frac{1}{2})$, et on forme les deux mots $v_n = \sigma_n(1)\sigma_n(2)\cdots\sigma_n(k_n)$ et $w_n = \sigma_n(k_n+1)\cdots\sigma_n(N)$.

— On tire ensuite au hasard un élément de $v_n \sqcup\!\sqcup w_n$ suivant la loi uniforme sur cet ensemble ; la permutation obtenue est σ_{n+1}.

1.1 Combien d'éléments y-a-t'il dans $v \sqcup\!\sqcup w$ si v a longueur r et w a longueur s ? Montrer que le battage de cartes $(\sigma_n)_{n\in\mathbb{N}}$ est une marche aléatoire sur $\mathfrak{S}(N)$, de générateur

$$\mu = \frac{1}{2^N}\sum_{k=0}^{N}(12\cdots k) \sqcup\!\sqcup ((k+1)(k+2)\cdots N).$$

Dans cette formule, on identifie $v \sqcup\!\sqcup w = \{u^{(1)}, \ldots, u^{(t)}\}$ et la somme formelle $\sum_{i=1}^{t} u^{(i)}$ dans $\mathbb{C}\mathfrak{S}(N)$.

On appelle *retour* d'une permutation $\sigma \in \mathfrak{S}(N)$ un entier $i \in [\![1, N-1]\!]$ tel que, dans le mot de la permutation σ, la lettre i apparaît après la lettre $i+1$. Par exemple, l'ensemble des retours de $\sigma = 861734952$ est $R(\sigma) = \{2, 5, 7\}$. Une façon commode pour trouver les retours est de chercher de gauche à droite les lettres $1, 2, 3, \ldots$ dans le mot σ ; à chaque fois que l'on doit revenir au début du mot après avoir trouvé une lettre i, on a un retour $i \in R(\sigma)$. Pour $r \in [\![0, N-1]\!]$, on note

$$U_r = \sum_{\substack{\sigma\in\mathfrak{S}(N)\\ \operatorname{card}(R(\sigma))=r}} \sigma.$$

1.2 Montrer que le générateur μ du battage s'écrit :

$$\mu = \frac{N+1}{2^N}\,U_0 + \frac{1}{2^N}\,U_1.$$

On appelle *descente* d'une permutation $\sigma \in \mathfrak{S}(N)$ un entier $i \in [\![1, N-1]\!]$ tel que $\sigma(i) > \sigma(i+1)$. Par exemple, l'ensemble des descentes de $\sigma = 861734952$ est $D(\sigma) = \{1, 2, 4, 7, 8\}$.

1.3 Montrer que pour toute permutation σ, $D(\sigma) = R(\sigma^{-1})$.

2 L'algèbre de Bayer–Diaconis

On fixe deux entiers $N \geq 1$ et $a \geq 2$. Si $\sigma \in \mathfrak{S}(N)$, le *$a$-battage* de σ est la permutation aléatoire $\tau = \overline{\sqcup\!\sqcup}^{(a)}(\sigma) \in \mathfrak{S}(N)$ obtenue comme suit :

— On tire au hasard N nombres réels indépendants et de loi uniforme dans $[0, 1)$, et on note $0 \leq x_{\sigma(1)} < x_{\sigma(2)} < \cdots < x_{\sigma(N)} < 1$ leur réordonnement croissant.

— On note $y_i = ax_i \bmod 1$: chaque nombre réel ax_i appartient à $[0, a)$ et s'écrit donc $ax_i = \lfloor ax_i \rfloor + \{ax_i\}$ avec $\lfloor ax_i \rfloor \in [\![0, a-1]\!]$ et $\{ax_i\} \in [0, 1)$, et on pose $y_i = \{ax_i\}$.

— Le réordonnement croissant $y_{\tau(1)} < y_{\tau(2)} < \cdots < y_{\tau(N)}$ des y_i donne une permutation $\tau \in \mathfrak{S}(N)$.

Par exemple, si $N = 4$, $a = 2$ et $\sigma = 4312$, un choix possible de réels est $\{0.2, 0.4, 0.55, 0.75\}$, et l'on note $x_4 = 0.2$, $x_3 = 0.4$, $x_1 = 0.55$ et $x_2 = 0.75$. Les réels y_i sont $y_4 = 0.4$, $y_3 = 0.8$, $y_1 = 0.1$ et $y_2 = 0.5$. Leur réordonnement croissant est $y_1 < y_4 < y_2 < y_3$, donc on pose dans ce cas $\tau = 1423$.

2.1 On introduit le simplexe

$$\Delta^N[0,1) = \{(a_1, a_2, \dots, a_N) \,|\, 0 < a_1 < \cdots < a_N < 1\}$$

des suites croissantes de N nombres réels à valeurs entre 0 et 1. Ce simplexe a pour volume $\frac{1}{N!}$, et la mesure uniforme dessus est donc $N!$ fois la mesure de Lebesgue ; c'est aussi l'image par l'application de réordonnement croissant de la mesure uniforme sur $[0,1)^N$. Montrer que la suite $(y_{\tau(1)}, \dots, y_{\tau(N)})$ obtenue lors de la construction de $\tau = \overline{\sqcup\!\sqcup}^{(a)}(\sigma)$ est indépendante de τ et de loi uniforme sur $\Delta^N[0,1)$ (indication : étant donnée une partition $[0,1) = I_1 \sqcup I_2 \sqcup \cdots \sqcup I_r$ en intervalles et une décomposition $N = N_1 + N_2 + \cdots + N_r$ de N en entiers positifs ou nuls, on pourra calculer la probabilité pour que N_j points $y_{\tau(i)}$ tombent dans I_j pour tout $j \in [\![1, r]\!]$).

2.2 Montrer si $(\sigma_n)_{n\in\mathbb{N}}$ est le battage de cartes défini dans la section précédente, alors les transitions de cette marche aléatoire sont réalisées par le 2-battage : conditionnellement à $\{\sigma_n = \sigma\}$, la loi de σ_{n+1} est celle de la permutation aléatoire $\overline{\sqcup\!\sqcup}^{(2)}(\sigma)$. On pourra commencer par montrer l'identité en loi $\overline{\sqcup\!\sqcup}^{(a)}(\sigma) = \sigma \circ \overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]})$ pour toute permutation $\sigma \in \mathfrak{S}(N)$ et tout $a \geq 2$.

2.3 La question précédente implique que la loi de $\overline{\sqcup\!\sqcup}^{(2)}(\mathrm{id}_{[1,N]})$ s'écrit

$$V_2 = \mu = \frac{1}{2^N} \sum_{k=0}^{N} (12\cdots k) \sqcup\!\sqcup ((k+1)(k+2)\cdots N)$$

dans $\mathbb{C}\mathfrak{S}(N)$. Donner une formule du même type pour la loi V_a de $\overline{\sqcup\!\sqcup}^{(a\geq 2)}(\mathrm{id}_{[1,N]})$, vue comme élément de $\mathbb{C}\mathfrak{S}(N)$ (on ne demande pas de preuve minutieuse de la généralisation).

2.4 Montrer que pour toute permutation σ et tous entiers $a, b \geq 2$, on a l'identité en loi :

$$\overline{\sqcup\!\sqcup}^{(a)}(\overline{\sqcup\!\sqcup}^{(b)}(\sigma)) =_{\text{(loi)}} \overline{\sqcup\!\sqcup}^{(ab)}(\sigma),$$

les deux a-battage et b-battage du terme de gauche étant réalisés indépendamment.

2.5 Montrer que le nombre de retours de $\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]})$ est compris entre 0 et $a-1$. Montrer ensuite en utilisant la question 2.3 que si σ est une permutation avec $0 \leq r = \mathrm{card}\,(R(\sigma)) \leq a-1$, alors

$$\mathbb{P}[\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]}) = \sigma] = \frac{\binom{N+a-r-1}{N}}{a^N}.$$

On pourra introduire les cardinaux

$$N_j = \mathrm{card}\left(\left\{x_i \;\middle|\; \frac{j-1}{a} \leq x_i < \frac{j}{a}\right\}\right),$$

où $x_1 < x_2 < \cdots < x_N$ suit la loi uniforme sur $\Delta^N[0,1)$ et est utilisée pour construire $\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]})$.

2.6 Réinterpréter la question précédente en donnant une décomposition de l'élément $V_{a\geq 2} \in \mathbb{C}\mathfrak{S}(N)$ comme combinaison linéaire des éléments U_r, $r \in [\![0, N-1]\!]$.

2.7 On note $\mu_n = \sum_{\sigma\in\mathfrak{S}(N)} \mathbb{P}[\sigma_n = \sigma]\,\sigma$ la loi de la n-ième permutation σ_n du battage de cartes. Montrer que μ_n est la loi du 2^n-battage de la permutation identité, et qu'elle s'écrit dans $\mathbb{C}\mathfrak{S}(N)$:

$$\mu_n = \sum_{r=0}^{N-1} \frac{\binom{2^n+N-r-1}{N}}{2^{nN}}\, U_r.$$

2.8 Montrer que dans $\mathbb{C}\mathfrak{S}(n)$, $U_iU_j = U_jU_i$ pour tous i, j, et que ce produit est une combinaison linéaire d'éléments $U_{r\in[\![0,N-1]\!]}$. On pourra utiliser la question 2.4. En déduire que le sous-espace vectoriel $\mathfrak{BD}(N)$ engendré linéairement par les $U_{r\in[\![0,N-1]\!]}$ est une sous-algèbre unitaire commutative de $\mathbb{C}\mathfrak{S}(N)$.

2.9 On rappelle la définition des fonctions symétriques élémentaires :

$$e_l(x_1, \dots, x_r) = \sum_{1\le i_1<i_2<\cdots<i_l\le r} x_{i_1}x_{i_2}\cdots x_{i_l},$$

avec pour convention $e_0(x_1, \dots, x_r) = 1$. Montrer que pour tout $a \ge 2$,

$$V_a = \frac{1}{N!}\sum_{l=0}^{N-1} a^{-l}\left(\sum_{r=0}^{N-1} e_l(N-1-r, N-2-r, \dots, 1-r, -r)\, U_r\right).$$

Pour $l \in [\![0, N-1]\!]$, on note $E_l = \sum_{r=0}^{N-1} e_l(N-1-r, N-2-r, \dots, 1-r, -r)\, U_r$. Montrer que tous les éléments E_l appartiennent à $\mathbb{C}[V_2] = \mathrm{Vect}(1, V_2, (V_2)^2, (V_2)^3, \dots)$ (indication : faire apparaître une matrice inversible de Vandermonde). En déduire que le battage de cartes V_2 engendre toute l'algèbre $\mathfrak{BD}(N)$: $\mathbb{C}[V_2] = \mathfrak{BD}(N)$.

2.10 Montrer que $(E_l)_{l\in[\![0,N-1]\!]}$ est une base de $\mathfrak{BD}(N)$, et que pour tous $l, m \in [\![0, N-1]\!]$, $E_l\, E_m = 1_{(l=m)}\, N!\, E_l$. On pourra s'intéresser à la matrice dans la base $(E_l)_{l\in[\![0,N-1]\!]}$ de l'application linéaire $x \in \mathfrak{BD}(N) \mapsto P(V_2)\cdot x$, P étant un polynôme arbitraire. En déduire que l'application

$$\mathfrak{BD}(N) \to \mathbb{C}^N$$
$$x = \frac{1}{N!}\sum_{l=0}^{N-1} x_l\, E_l \mapsto (x_0, x_1, \dots, x_{N-1})$$

est un isomorphisme d'algèbres, l'espace $\mathbb{C}^N$ étant équipé du produit naturel $(x_0, x_1, \dots, x_{N-1})\times (y_0, y_1, \dots, y_{N-1}) = (x_0y_0, x_1y_1, \dots, x_{N-1}y_{N-1})$.

3 Le phénomène de coupure

Dans toute cette section, on pose $n = \frac{\log(N^{3/2}c)}{\log 2}$, où $c \in \mathbb{R}_+^*$ est un réel positif tel que l'expression précédente donne un entier. L'objectif est de calculer en fonction de c la distance en variation totale entre la loi de σ_n et la loi uniforme sur $\mathfrak{S}(N)$.

3.1 Pour $m \in [\![0, N-1]\!]$, on note $A_{N,m}$ le nombre de permutations $\sigma \in \mathfrak{S}(N)$ avec m *montées*, une montée étant un indice $i \in [\![1, N-1]\!]$ tel que $\sigma(i) < \sigma(i+1)$. Montrer que $A_{N,m}$ est aussi égal au nombre de permutations de taille N avec m descentes, et au nombre de permutations de taille N avec m retours. On pourra utiliser la permutation $\sigma_0 : i \mapsto N+1-i$ et l'application $\sigma \mapsto \sigma\sigma_0$. Établir la symétrie : $A_{N,m} = A_{N,N-1-m}$.

3.2 On considère l'hypercube $[0,1)^N$, et pour $m \in [\![0, N-1]\!]$, on introduit les deux régions suivantes :

$$M_{N,m} = \{(x_1, \dots, x_N) \in [0,1)^N \mid \text{il existe } m \text{ indices } i \in [\![1, N-1]\!] \text{ tels que } x_i < x_{i+1}\};$$
$$H_{N,m} = \{(x_1, \dots, x_N) \in [0,1)^N \mid m \le x_1 + x_2 + \cdots + x_N < m+1\}.$$

Montrer que le volume de $M_{N,m}$ est égal à $\frac{A_{N,m}}{N!}$. On considère l'application

$$\Psi : [0,1)^N \to [0,1)^N$$
$$(x_1, \dots, x_N) \mapsto (y_1, \dots, y_N), \quad \text{avec } y_i = \begin{cases} x_{i-1} - x_i & \text{si } x_{i-1} > x_i, \\ 1 + x_{i-1} - x_i & \text{si } x_{i-1} < x_i, \end{cases}$$

en posant par convention $x_0 = 0$. On ne définit pas Ψ sur l'ensemble de mesure nulle où il y a des égalités $x_{i-1} = x_i$. Montrer que Ψ est inversée (à des ensembles de mesure nulle près) par la formule $x_i = 1 + \lfloor y_1 + \cdots + y_i \rfloor - y_1 + \cdots + y_i$. Montrer aussi que Ψ préserve la mesure de Lebesgue (on pourra découper l'hypercube en parties où Ψ est une application affine). Que vaut $\Psi(M_{N,m})$? En déduire l'interprétation probabiliste suivante des *nombres eulériens* $A_{N,m}$:

$$A_{N,m} = N!\, \mathbb{P}[m \le X_1 + X_2 + \cdots + X_N < m + 1],$$

où les X_i sont des variables indépendantes uniformes sur $[0,1)$.

3.3 On rappelle la définition de la distance en variation totale :

$$d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = \sup_{A \subset \mathfrak{S}(N)} \left| \mathbb{P}[\sigma_n \in A] - \frac{|A|}{N!} \right|.$$

Montrer que

$$d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = \frac{1}{2} \sum_{m=0}^{N-1} \frac{A_{N,m}}{N!} \left| \frac{(2^n + N - 1 - m)!}{(2^n - 1 - m)!\, 2^{nN}} - 1 \right|.$$

On pourra utiliser le fait que la loi uniforme et la loi μ_n de σ_n sont constantes sur les ensembles de permutations avec un nombre de retours fixé.

3.4 On fait le changement de variables $m = \frac{N}{2} + \sqrt{\frac{N}{12}}\, x$. Utiliser le théorème central limite pour estimer par une intégrale la somme

$$\sum_{m=0}^{N-1} \frac{A_{N,m}}{N!}\, f(x),$$

où f est une fonction lipschitzienne bornée. Montrer par ailleurs que

$$\frac{(2^n + N - 1 - m)!}{(2^n - 1 - m)!\, 2^{nN}} = \exp\left(-\frac{x}{c\sqrt{12}} - \frac{1}{24c^2} + O_x\left(\frac{1}{\sqrt{N}}\right) \right),$$

où le $O(\cdot)$ peut dépendre de x. On admet que l'on peut négliger le terme $O_x(\frac{1}{\sqrt{N}})$ dans tous les calculs, échanger limites et intégrales, et utiliser le théorème central limite même si la fonction ci-dessus n'est pas lipschitzienne bornée. Montrer alors que, si $n = \frac{\log(N^{3/2}c)}{\log 2}$, on a

$$\lim_{N \to +\infty} d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = \frac{1}{2} \int_{\mathbb{R}} \left| \mathrm{e}^{-\frac{x}{c\sqrt{12}} - \frac{1}{24c^2}} - 1 \right| \frac{\mathrm{e}^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\, dx.$$

3.5 Montrer finalement que l'intégrale ci-dessus se réécrit :

$$\lim_{N \to \infty} d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = 1 - 2F\left(-\frac{1}{4\sqrt{3}c} \right),$$

où F est la fonction de répartition de la gaussienne standard. En déduire le phénomène de coupure annoncé au début de l'énoncé.

Corrigé

1.1 Pour entrelacer les lettres de v et de w, il faut choisir parmi les $r+s$ lettres de $u \in v \sqcup\!\sqcup w$ quelles lettres seront celles de v : ces lettres apparaîtront alors dans l'ordre $v_1 v_2 \cdots v_r$ lorsqu'on lit le mot u de gauche à droite, et les autres lettres non sélectionnées seront celles de w, qui apparaîtront dans l'ordre $w_1 w_2 \cdots w_s$. Donc,

$$\operatorname{card}(v \sqcup\!\sqcup w) = (\text{nombre de parties à } r \text{ éléments dans un ensemble de taille } r+s) = \binom{r+s}{r}.$$

Déterminons maintenant la matrice de transition de la chaîne de Markov $(\sigma_n)_{n\in\mathbb{N}}$. Par définition du battage, la loi conditionnelle de σ_{n+1} sachant $\sigma_n = \sigma$, qu'on peut voir comme un élément de $\mathbb{C}\mathfrak{S}(n)$, s'écrit

$$\begin{aligned} P_\sigma &= \sum_{k=0}^{N} \frac{1}{2^N}\binom{N}{k} (\text{loi uniforme sur } (\sigma(1)\sigma(2)\cdots\sigma(k)) \sqcup\!\sqcup (\sigma(k+1)\cdots\sigma(N))) \\ &= \frac{1}{2^N}\sum_{k=0}^{N} (\sigma(1)\sigma(2)\cdots\sigma(k)) \sqcup\!\sqcup (\sigma(k+1)\cdots\sigma(N))). \end{aligned}$$

Il reste à voir que, étant donnée une permutation $\sigma \in \mathfrak{S}(N)$, on a :

$$(\sigma(1)\sigma(2)\cdots\sigma(k)) \sqcup\!\sqcup (\sigma(k+1)\cdots\sigma(N)) = \big\{\sigma\tau \,|\, \tau \in (12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N)\big\}.$$

Alors, $P_\sigma = \frac{\sigma}{2^N}\sum_{k=0}^{N}((12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N))$, d'où la relation de récurrence suivante entre les lois marginales $(\mu_n)_{n\in\mathbb{N}}$ de la chaîne de Markov $(\sigma_n)_{n\in\mathbb{N}}$:

$$\begin{aligned} \mu_{n+1} &= \sum_{\sigma'\in\mathfrak{S}(N)} \mathbb{P}[\sigma_{n+1} = \sigma']\,\sigma' = \sum_{\sigma\in\mathfrak{S}(N)} \mathbb{P}[\sigma_n = \sigma]\, P_\sigma \\ &= \left(\sum_{\sigma\in\mathfrak{S}(N)} \mathbb{P}[\sigma_n = \sigma]\,\sigma\right)\left(\frac{1}{2^N}\sum_{k=0}^{N}((12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N))\right) \\ &= \mu_n\,\mu, \end{aligned}$$

avec μ comme indiqué dans l'énoncé. C'est la relation de récurrence satisfaite par les lois marginales d'une marche aléatoire sur $\mathfrak{S}(N)$ de générateur μ.

1.2 Soit $k \in [\![1, N-1]\!]$. Remarquons que dans $(12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N)$, le seul retour possible d'une permutation σ est k, puisque les lettres $1, 2, \ldots, k$ apparaissent dans l'ordre de gauche à droite, et de même pour les lettres $(k+1), \ldots, N$. On a même :

$$(12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N) = \{\sigma \in \mathfrak{S}(N) \,|\, R(\sigma) \subset \{k\}\}.$$

Le cas d'un ensemble de retour vide est possible, car la permutation identité est dans cet ensemble. On a donc :

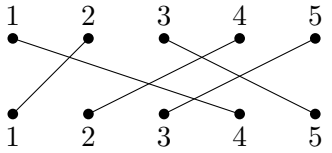
$$(12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N) = \mathrm{id}_{[\![1,N]\!]} + \sum_{\substack{\sigma\in\mathfrak{S}(N)\\ R(\sigma)=\{k\}}} \sigma.$$

Lorsque $k = 0$ ou $k = N$, on est dans le cas particulier d'un battage de deux mots avec l'un des mots vides, donc on obtient $\mathrm{id}_{[1,N]}$. Ainsi,

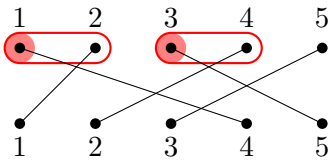
$$\begin{aligned} 2^N \mu &= 2\,\mathrm{id}_{[1,N]} + \sum_{k=1}^{N-1} \left(\mathrm{id}_{[1,N]} + \sum_{\substack{\sigma \in \mathfrak{S}(N) \\ R(\sigma) = \{k\}}} \sigma \right) \\ &= (N+1)\,\mathrm{id}_{[1,N]} + \sum_{\substack{\sigma \in \mathfrak{S}(N) \\ \mathrm{card}\,(R(\sigma)) = 1}} \sigma \\ &= (N+1)\,U_0 + U_1. \end{aligned}$$

1.3 Le plus simple est peut-être de raisonner sur les diagrammes de tresse des permutations. On représente comme dans le cours une permutation σ de taille N par un diagramme reliant deux rangées de points, le point i de la première rangée étant relié au point $\sigma(i)$ de la seconde rangée. Par exemple,

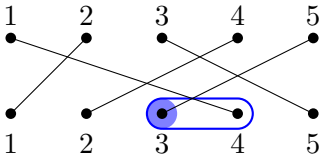
$\sigma = 41523 =$



Sur ce diagramme, les *descentes* sont les entiers i tels que les deux lignes issues des points i et $i+1$ de la première rangée se croisent. Par exemple, $D(41523) = \{1, 3\}$.



Par ailleurs, les *retours* de σ sont les entiers i tels que les deux lignes issues des points i et $i+1$ de la seconde rangée se croisent. Par exemple, $R(41523) = \{3\}$.



Le résultat se déduit immédiatement de cette description géométrique, car le diagramme de σ^{-1} est obtenu à partir du diagramme de σ en échangeant les deux rangées de points.

2.1 Notons que pour la mesure uniforme sur $\Delta^N[0,1)$, si $[0,1) = I_1 \sqcup I_2 \sqcup \cdots \sqcup I_r$ et $N = N_1 + N_2 + \cdots + N_r$, alors la probabilité pour observer N_1 points dans I_1, N_2 points dans I_2, *etc.*, et N_r points dans I_r est donnée par une formule multinomiale. En effet, la mesure uniforme sur $\Delta^N[0,1)$ est l'image par l'application de réordonnement croissant de la mesure de Lebesgue sur

$[0,1)^N$, donc

$$\mathbb{P}_{\Delta^N[0,1)}[\forall j \in [\![1,r]\!],\ |\{a_i \,|\, a_i \in I_j\}| = N_j] = \sum_{\substack{[\![1,N]\!]=K_1 \sqcup \cdots \sqcup K_r \\ \forall j \in [\![1,r]\!],\ |K_j|=N_j}} \prod_{j=1}^{r} \prod_{i \in K_j} \left(\int_{I_j} dx_i \right)$$
$$= \frac{N!}{N_1!\, N_2! \cdots N_r!} \, (\ell(I_1))^{N_1} (\ell(I_2))^{N_2} \cdots (\ell(I_r))^{N_r},$$

où $\ell([s,t)) = t-s$ est la mesure de Lebesgue d'un intervalle. Ceci caractérise la mesure uniforme sur $\Delta^N[0,1)$: en effet, à partir de ces formules, on peut calculer toutes les probabilités de produits d'intervalles

$$\mathbb{P}_{\Delta^N[0,1)}[a_1 \in I_1 \text{ et } a_2 \in I_2 \text{ et } \cdots \text{ et } a_r \in I_r],$$

en se ramenant par intersection à des intervalles disjoints dans lesquels on compte des points. Calculons maintenant la probabilité pour que, lors du a-battage, on observe N_1 points $y_{\tau(i)}$ dans I_1, N_2 points $y_{\tau(i)}$ dans I_2, *etc.* Chaque intervalle I_j est l'image par $x \mapsto ax \bmod 1$ de a intervalles $\widetilde{I}_{j,1}, \ldots, \widetilde{I}_{j,a}$ avec $\ell(I_{j,k}) = \frac{1}{a}\,\ell(I_j)$ pour tous indices j et k. On a donc

$$\begin{aligned}
&\mathbb{P}[\forall j \in [\![1,r]\!],\ |\{y_{\tau(i)} \,|\, y_{\tau(i)} \in I_j\}| = N_j] \\
&= \sum_{\substack{N_1 = N_{1,1} + \cdots + N_{1,a} \\ \vdots \quad\quad \vdots \\ N_1 = N_{r,1} + \cdots + N_{r,a}}} \mathbb{P}[\forall (j,k) \in [\![1,r]\!] \times [\![1,a]\!],\ |\{x_{\sigma(i)} \,|\, x_{\sigma(i)} \in I_{j,k}\}| = N_{j,k}].
\end{aligned}$$

Or, les points x_i sont choisis uniformément dans le simplexe $\Delta^N[0,1)$, donc on obtient

$$\begin{aligned}
&\sum_{\substack{N_1 = N_{1,1} + \cdots + N_{1,a} \\ \vdots \quad\quad \vdots \\ N_1 = N_{r,1} + \cdots + N_{r,a}}} \frac{N!}{N_{1,1}! \cdots N_{1,a}! \cdots N_{r,1}! \cdots N_{r,a}!} \, (\ell(I_{1,1}))^{N_{1,1}} \cdots (\ell(I_{r,a}))^{N_{r,a}} \\
&= \frac{N!}{N_1! \cdots N_r!} \prod_{j=1}^{r} \left(\sum_{N_j = N_{j,1} + \cdots + N_{j,a}} \frac{N_j!}{N_{j,1}! \cdots N_{j,a}!} (\ell(I_{j,1}))^{N_{j,1}} \cdots (\ell(I_{j,a}))^{N_{j,a}} \right) \\
&= \frac{N!}{N_1!\, N_2! \cdots N_r!} \, (\ell(I_1))^{N_1} (\ell(I_2))^{N_2} \cdots (\ell(I_r))^{N_r}
\end{aligned}$$

en utilisant r fois la formule du multinôme de Newton à la dernière ligne. La loi est donc bien uniforme sur $\Delta^N[0,1)$, et indépendante de τ qui ne joue aucun rôle dans le calcul.

2.2 Pour commencer, remarquons que l'on a en fait $\overline{\sqcup\!\sqcup}^{(a)}(\sigma) =_{\text{(loi)}} \sigma \circ (\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[\![1,N]\!]}))$ pour tout $a \geq 2$. En effet, notons $\bar{x} = x_{\sigma(\cdot)} : [\![1,N]\!] \to [0,1)$; c'est une variable aléatoire uniformément choisie dans $\Delta^N[0,1)$. La variable $\bar{y} = a\bar{x} \bmod 1$ est un vecteur aléatoire dans $[0,1)^N$, dont le réordonnement croissant $0 < \bar{y}_{\tau(1)} < \cdots < \bar{y}_{\tau(N)} < 1$ donne une permutation τ de loi $\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[\![1,N]\!]})$, puisque les coordonnées de $\bar{x}$ étaient ordonnées. Mais

$$\bar{y}_{\tau(i)} = a\,\bar{x}_{\tau(i)} \bmod 1 = a\,x_{\sigma(\tau(i))} \bmod 1,$$

donc $\sigma \circ \tau$ est la permutation donnant le réordonnement croissant des $ax_j \bmod 1$; ainsi, $\sigma\tau$ suit une loi $\overline{\sqcup\!\sqcup}^{(a)}(\sigma)$.

Pour traiter la question, il suffit dès lors de montrer que la loi de $\overline{\sqcup\!\sqcup}^{(2)}(\mathrm{id}_{[\![1,N]\!]})$ est la loi μ du générateur du battage de la première section. L'entier k déterminant la taille des blocs lors du battage va être relié au nombre B de réels x_i qui tombe dans $[0,\frac{1}{2})$. Cet entier aléatoire B suit bien une loi binomiale :

$$\mathbb{P}\left[\mathrm{card}\left(\left\{i\in[\![1,N]\!]\;\middle|\; x_i<\frac{1}{2}\right\}\right)=k\right]=\sum_{\substack{I\subset[\![1,N]\!]\\ \mathrm{card}\,(I)=k}}\left(\int_0^{\frac{1}{2}}\prod_{i\in I}dx_i\right)\left(\int_{\frac{1}{2}}^1\prod_{i\notin I}dx_i\right)=\binom{N}{k}\frac{1}{2^N}.$$

On voit alors facilement en conditionnant par rapport à B que vis-à-vis de la partition $[0,1)=[0,\frac{1}{2})\sqcup[\frac{1}{2},1)$, le réordonnement croissant $x_1<\cdots<x_N$ d'un N-uplet de points indépendants uniformes sur $[0,1)$ se comporte comme suit :

- On tire une variable aléatoire $B\sim\mathcal{B}(N,\frac{1}{2})$.
- Conditionnellement à $B=k$, les k premiers réels $x_1<\cdots<x_k$ et les $N-k$ derniers réels $x_{k+1}<\cdots<x_N$ tombent respectivement dans $[0,\frac{1}{2})$ et dans $[\frac{1}{2},1)$, et sont distribués indépendamment suivant les lois uniformes sur $\Delta^k[0,\frac{1}{2})$ et sur $\Delta^{N-k}[\frac{1}{2},1)$.

L'application $x\mapsto 2x \bmod 1$ est une bijection de $[0,\frac{1}{2})$ ou de $[\frac{1}{2},1)$ vers $[0,1)$, et elle conserve les mesures uniformes sur ces intervalles. Par conséquent, conditionnellement à $B=k$, les k premiers réels $y_1<\cdots<y_k$ et les $N-k$ derniers réels $y_{k+1}<\cdots<y_N$ sont distribués indépendamment suivant les lois uniformes sur $\Delta^k[0,1)$ et sur $\Delta^{N-k}[0,1)$. Notons alors que le réordonnement croissant de tous les $y_{i\in[\![1,N]\!]}$ met forcément en jeu une permutation $\sigma\in(12\cdots k)\sqcup\!\sqcup((k+1)\cdots N)$, puisque les entiers $1,2,\ldots,k$ apparaîtront dans cet ordre dans le mot de σ, et de même pour les entiers $(k+1),\ldots,N$. Pour conclure que la loi de $\overline{\sqcup\!\sqcup}^{(2)}(\mathrm{id}_{[\![1,N]\!]})$ est μ, il faut montrer que toutes ces permutations ont la même probabilité. On raisonne par récurrence sur N, l'hypothèse de récurrence $\mathcal{H}(N)$ étant : "pour tout $k\in[\![0,N]\!]$, le réordonnement croissant de l'union de deux suites croissantes $y_1<\cdots<y_k$ et $y_{k+1}<\cdots<y_N$ distribuées indépendamment suivant les lois uniformes sur $\Delta^k[0,1)$ et sur $\Delta^{N-k}[0,1)$ met en jeu une permutation uniformément choisie dans $(12\cdots k)\sqcup\!\sqcup((k+1)\cdots N)$".

Le résultat est trivial au rang $N=1$, et aussi si $k=0$ et $k=N$. Supposons $\mathcal{H}(N)$ vraie, et considérons avec $1\leq k\leq N$ deux suites croissantes $y_1<\cdots<y_k$ et $y_{k+1}<\cdots<y_{N+1}$ indépendantes et de lois uniformes sur $\Delta^k[0,1)$ et sur $\Delta^{N-k}[0,1)$. Pour se ramener au cas de N variables, notons que la plus grande variable parmi tous les y_j est y_k avec probabilité $\frac{k}{N+1}$, et est y_{N+1} avec probabilité $\frac{N+1-k}{N+1}$. Notons E_1 et E_2 ces deux événements. Conditionnellement à E_1 et à la valeur de y_k, les deux suites croissantes $y_1<\cdots<y_{k-1}$ et $y_{k+1}<\cdots<y_{N+1}$ se réordonnent suivant une permutation uniformément choisie dans $(12\cdots(k-1))\sqcup\!\sqcup((k+1)\cdots(N+1))$ (ce sont des suites dans $[0,y_k)$, mais clairement le résultat de l'hypothèse de récurrence est invariant par scaling de l'intervalle $[0,1)$). Ceci implique que, pour toute permutation σ dont le mot est $\tau\cdot k$ avec $\tau\in(12\cdots(k-1))\sqcup\!\sqcup((k+1)\cdots(N+1))$, on a

$$\mathbb{P}_{N+1,k}[\sigma]=\frac{k}{N+1}\mathbb{P}_{N,k-1}[\tau]=\frac{k}{N+1}\frac{(N+1-k)!(k-1)!}{N!}=\frac{1}{\binom{N+1}{k}}.$$

De même, conditionnellement à E_2 et à la valeur de y_{N+1}, les deux suites croissantes $y_1<\cdots<y_k$ et $y_{k+1}<\cdots<y_N$ se réordonnent suivant une permutation uniformément choisie dans $(12\cdots k)\sqcup\!\sqcup((k+1)\cdots N)$. Ceci implique que, pour toute permutation σ dont le mot est $\tau\cdot(N+1)$ avec $\tau\in(12\cdots k-1)\sqcup\!\sqcup((k+1)\cdots N)$, on a

$$\mathbb{P}_{N+1,k}[\sigma]=\frac{N+1-k}{N+1}\mathbb{P}_{N,k}[\tau]=\frac{N+1-k}{N+1}\frac{(N-k)!k!}{N!}=\frac{1}{\binom{N+1}{k}}.$$

On a donc la même probabilité dans les deux cas, et toutes les permutations $\sigma \in (12\cdots k) \sqcup\!\sqcup ((k+1)\cdots(N+1))$ sont ainsi traitées, car

$$(12\cdots k) \sqcup\!\sqcup ((k+1)\cdots(N+1))$$
$$= \Big(((12\cdots(k-1)) \sqcup\!\sqcup ((k+1)\cdots(N+1)))\cdot k\Big) \bigsqcup \Big(((12\cdots k) \sqcup\!\sqcup ((k+1)\cdots N))\cdot(N+1)\Big).$$

2.3 On a plus généralement

$$V_a = \frac{1}{a^N} \sum_{N=N_1+\cdots+N_a} (12\cdots N_1) \sqcup\!\sqcup ((N_1+1)\cdots(N_1+N_2)) \sqcup\!\sqcup \cdots \sqcup\!\sqcup ((N_1+\cdots+N_{a-1}+1)\cdots N),$$

la somme portant sur toutes les façons de décomposer N comme somme de a entiers positifs ou nuls. En effet, pour construire la permutation aléatoire, on choisit d'abord les tailles

$$N_j = \operatorname{card}\left(\left\{x_i \,|\, \frac{j-1}{a} \le x_i \le \frac{j}{a}\right\}\right);$$

le vecteur $(N_1, N_2, \ldots, N_a)$ suit une loi multinomiale de paramètres N et $(\frac{1}{a}, \cdots, \frac{1}{a})$. Conditionnellement à ce vecteur d'entiers, les vecteurs

$$(y_{N_1+\cdots+N_{j-1}+1} < y_{N_1+\cdots+N_{j-1}+2} < \cdots < y_{N_1+\cdots+N_j})$$

sont indépendants et de lois uniformes sur les simplexes $\Delta^{N_j}[0,1)$, pour $j \in [\![1, a]\!]$. Alors, conditionnellement à $(N_1, N_2, \ldots, N_a)$, la permutation $\sigma = \overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[\![1,N]\!]})$ est de loi uniforme sur l'ensemble

$$(12\cdots N_1) \sqcup\!\sqcup ((N_1+1)\cdots(N_1+N_2)) \sqcup\!\sqcup \cdots \sqcup\!\sqcup ((N_1+\cdots+N_{a-1}+1)\cdots N)$$

de tous les entrelacements possibles des mots de taille $N_1, N_2, \ldots, N_a$ ci-dessus : c'est pour les mêmes raisons que dans le cas $a = 2$. Le nombre de tels entrelacements est

$$\frac{N!}{N_1!\cdots N_r!},$$

donc vient compenser le facteur multinomial de la loi multinomiale sur $(N_1, N_2, \ldots, N_a)$; il reste simplement le facteur $\frac{1}{a^N}$ dans le calcul de la probabilité.

2.4 D'après la question 2.2, il suffit de montrer l'identité en loi lorsque $\sigma = \mathrm{id}_{[\![1,N]\!]}$. Supposons donnés $x_1 < x_2 < \cdots < x_N$ choisis suivant la loi uniforme de $\Delta^N[0,1)$, et notons $\sigma = \overline{\sqcup\!\sqcup}^{(b)}(\mathrm{id}_{[\![1,N]\!]})$ la permutation telle que $y_{\sigma(1)} < y_{\sigma(2)} < \cdots < y_{\sigma(N)}$, avec $y_i = bx_i \bmod 1$. On a vu dans 2.1 que la distribution dans $\Delta^N[0,1)$ des points $y_{\sigma(i)}$ était indépendante de $\sigma = \overline{\sqcup\!\sqcup}^{(b)}(\mathrm{id}_{[\![1,N]\!]})$ et était uniforme sur le simplexe. Ceci implique que pour calculer $\overline{\sqcup\!\sqcup}^{(a)}(\overline{\sqcup\!\sqcup}^{(b)}(\mathrm{id}_{[\![1,N]\!]}))$, on peut utiliser les points $y_i = bx_i \bmod 1$. Alors, puisque

$$z_i = (abx_i) \bmod 1 = a(bx_i \bmod 1) \bmod 1,$$

la permutation ρ telle que $z_{\rho(1)} < z_{\rho(2)} < \cdots < z_{\rho(N)}$ suit à la fois la loi de $\overline{\sqcup\!\sqcup}^{(a)}(\overline{\sqcup\!\sqcup}^{(b)}(\mathrm{id}_{[\![1,N]\!]}))$ et celle de $\overline{\sqcup\!\sqcup}^{(ab)}(\mathrm{id}_{[\![1,N]\!]})$, d'où l'identité des deux lois.

2.5 Pour $j \in [\![1, a]\!]$, notons $N_j = \operatorname{card}\{x_i \mid \frac{(j-1)}{a} \le x_i < \frac{j}{a}\}$, où $x_1 < \cdots < x_N$ est choisie suivant la loi uniforme de $\Delta^N[0,1)$. Les retours de la permutation $\sigma = \overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,r]})$ construite à partir de cette suite croissante sont inclus dans l'ensemble

$$\{N_1, N_1 + N_2, \cdots, N_1 + N_2 + \cdots + N_{a-1}\};$$

en effet, lorsqu'on lit les lettres de gauche à droite dans le mot $\sigma(1)\sigma(2)\cdots\sigma(N)$ de σ, les lettres $N_1 + \cdots + N_{j-1} + 1, N_1 + \cdots + N_{j-1} + 2, \ldots, N_1 + \cdots + N_j$ apparaissent dans cet ordre, car

$$\begin{aligned} &\frac{(j-1)}{a} \le x_{N_1+\cdots+N_{j-1}+1} < x_{N_1+\cdots+N_{j-1}+2} < \cdots < x_{N_1+\cdots+N_j} < \frac{j}{a} \\ \Rightarrow \quad &0 \le y_{N_1+\cdots+N_{j-1}+1} < y_{N_1+\cdots+N_{j-1}+2} < \cdots < y_{N_1+\cdots+N_j} < 1. \end{aligned}$$

En effet, la restriction de $x \mapsto ax \bmod 1$ à un intervalle $[\frac{j-1}{a}, \frac{j}{a})$ est croissante. Donc, $\operatorname{card} R(\sigma) \le a - 1$. Pour la seconde partie de la question, notons que si les entiers $N_1, \ldots, N_a$ sont connus, alors il existe un unique entrelacement des mots $12\cdots N_1$, $(N_1+1)\cdots(N_1+N_2)$, *etc.* qui donne une permutation fixée σ. Il s'ensuit que, si $R(\sigma) = \{k_1, \ldots, k_r\}$, alors la probabilité $\mathbb{P}[\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]}) = \sigma]$ est $\frac{1}{a^N}$ fois le nombre de décompositions $N = N_1 + N_2 + \cdots + N_a$ telles que

$$\{k_1, \ldots, k_r\} \subset \{N_1, N_1 + N_2, \ldots, N_1 + N_2 + \cdots + N_{a-1}\}.$$

L'ensemble des retours de σ étant fixé, il reste à rajouter $a-1-r$ points pour obtenir l'ensemble $\{N_1, N_1 + N_2, \ldots, N_1 + N_2 + \cdots + N_{a-1}\}$. Attention, les retours k_i sont tous distincts, mais on peut avoir $N_i = 0$, et donc des répétitions dans le second ensemble. On peut représenter les choix possibles comme suit. Plaçons N symboles $\bullet_{1 \le i \le N}$ parmi $N + a - r - 1$ emplacements : par exemple, avec $a - r = 5$, une possibilité est :

$$* \bullet_1 \bullet_2 * \bullet_3 \bullet_4 \bullet_5 \bullet_6 * * \bullet_7 \bullet_8 \bullet_9.$$

On rajoute à cette représentation des barres | placées juste avant les entiers $k_i + 1$, $1 \le i \le r$. Par exemple, pour $\sigma = 861734952$ d'ensemble de retours $R(\sigma) = \{2, 5, 7\}$, on obtient

$$* \bullet_1 \bullet_2 * \mid \bullet_3 \bullet_4 \bullet_5 \mid \bullet_6 * * \bullet_7 \mid \bullet_8 \bullet_9.$$

Cette nouvelle représentation correspond à un choix d'entiers $N_1, N_2, \ldots, N_a$ tel que $N_1 + N_2 + \cdots + N_a = N$ et tel que $R(\sigma)$ soit inclus dans$\{N_1, N_1+N_2, \ldots, N_1+N_2+\cdots+N_{a-1}\}$: chaque N_j est défini comme le nombre de symboles $\bullet_i$ placés entre deux symboles consécutifs dans $\{*, |\}$. Sur l'exemple précédent, on obtient une décomposition de $N = 9$ comme somme de $a = 8$ entiers positifs ou nuls :

$$9 = 0 + 2 + 0 + 3 + 1 + 0 + 1 + 2.$$

Réciproquement, étant une telle décomposition, en plaçant un symbole pour chaque entier $N_1 + \cdots + N_{j \le a-1}$ et en retirant les r retours de σ, on obtient une représentation avec N symboles $\bullet_i$ et $a - 1 - r$ symboles $*$. Donc, le nombre de choix possibles est $\binom{N+a-r-1}{N}$, et on conclut pour la valeur de $\mathbb{P}[\overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]}) = \sigma]$.

2.6 La question précédente dit que, pour $a \ge 2$,

$$V_a = \text{loi de } \overline{\sqcup\!\sqcup}^{(a)}(\mathrm{id}_{[1,N]}) = \sum_{r=0}^{a-1} \frac{\binom{N+a-1-r}{N}}{a^N} U_r.$$

On peut aussi faire la somme jusqu'à $r = N - 1$, car si $r > a - 1$, alors le coefficient binomial s'annule.

2.7 Par 2.2, la transition de la chaîne de Markov $(\sigma_n)_{n\in\mathbb{N}}$ peut être réalisée avec un 2-battage $\overline{\sqcup\!\sqcup}^{(2)}$. En appliquant n transitions à la permutation identité, on obtient $\sigma_n = (\overline{\sqcup\!\sqcup}^{(2)})^{\circ n}(\mathrm{id}_{[1,N]})$, chaque 2-battage dans la composition étant réalisé indépendamment. D'après la question 2.4, appliquer n fois des 2-battages indépendants est équivalent en loi à appliquer un $2\times 2\times\cdots\times 2 = 2^n$-battage, d'où l'identités des lois

$$\mu_n = \text{loi de } \overline{\sqcup\!\sqcup}^{(2^n)}(\mathrm{id}_{[1,N]}).$$

En remplaçant a par 2^n dans la formule de la question précédente, on obtient le résultat demandé.

2.8 On veut montrer que $U_iU_j = U_jU_i = \sum_{r=0}^{N-1} c(i,j,r)\,U_r$, avec des coefficients $c(i,j,r)$ qui sont donc symétriques : $c(i,j,r) = c(j,i,r)$. Si $i = 0$ ou $j = 0$, c'est évident, car $U_0 = \mathrm{id}_{[1,N]}$. Remarquons sinon que la formule de la question 2.6 donne une relation triangulaire entre les U_i et les V_{i+1} :

$$\begin{aligned}
V_2 &= \frac{1}{2^N}((N+1)\,U_0 + U_1);\\
V_3 &= \frac{1}{3^N}\left(\frac{(N+1)(N+2)}{2}\,U_0 + (N+1)\,U_1 + U_2\right);\\
V_4 &= \frac{1}{4^N}\left(\frac{(N+1)(N+2)(N+3)}{6}\,U_0 + \frac{(N+1)(N+2)}{2}\,U_1 + (N+1)\,U_2 + U_3\right)
\end{aligned}$$

etc. Ceci implique que chaque $U_{i\geq 1}$ s'écrit comme combinaison linéaire de U_0 et des lois de a-battages $V_2, V_3, \ldots, V_{i+1}$. Or, d'après la question 2.4, tous ces éléments commutent entre, car $V_aV_b = V_bV_a = V_{ab}$. Donc, $U_iU_j = U_jU_i$ pour tous i et j. De plus, un produit $V_aV_b = V_{ab}$ est encore une combinaison linéaire d'éléments U_r d'après la formule générale de la question 2.6. Donc, U_iU_j est bien dans $\mathfrak{BD}(N) = \mathrm{Vect}(U_{r\geq 0})$ pour tout couple (i,j). On en déduit que $\mathfrak{BD}(N)$ est stable par produit dans $\mathbb{C}\mathfrak{S}(N)$, et que le produit est commutatif dans cette sous-algèbre (qui est unitaire puisqu'elle contient $U_0 = \mathrm{id}_{[1,N]}$).

2.9 On écrit les coefficients binomiaux dans la formule pour V_a comme des polynômes en a :

$$\begin{aligned}
\frac{1}{a^N}\binom{N+a-1-r}{N} &= \frac{1}{a^N\,N!}\underbrace{(a+N-1-r)(a+N-2-r)\cdots(a-r)}_{\text{polynôme de degré } N}\\
&= \frac{1}{a^N\,N!}\sum_{l=0}^{N} a^{N-l}\,e_l(N-1-r, N-2-r, \cdots, -r)\\
&= \frac{1}{N!}\sum_{l=0}^{N-1} a^{-l}\,e_l(N-1-r, N-2-r, \cdots, -r).
\end{aligned}$$

Dans la dernière formule, on a ôté le terme $l = N$, car $e_N(N-1-r, N-2-r, \cdots, -r) = \prod_{j=0}^{N-1}(j-r) = 0$ (prendre le terme $j = r$). Ainsi, en remplaçant dans la formule pour V_a, on obtient :

$$V_a = \frac{1}{N!}\sum_{l=0}^{N-1}\frac{1}{a^l}\,E_l,$$

où $E_l = \sum_{r=0}^{N-1} e_l(N-1-r, N-2-r, \cdots, -r)\,U_r$. La formule passe au cas $a = 1$, à condition

de poser $V_1 = U_0 = \mathrm{id}_{[1,N]}$. En effet,

$$\begin{aligned}\sum_{l=0}^{N-1} E_l &= \sum_{r=0}^{N-1} \left(\sum_{l=0}^{N} e_l(N-1-r, \cdots, -r) \right) U_r \\ &= \sum_{r=0}^{N-1} \left((N-r)(N-r-1)\cdots(1-r) \right) U_r = N!\, U_0,\end{aligned}$$

les autres termes de la somme s'annulant. Maintenant, on a en particulier pour $a \in \{1, 2, 4, 8, \ldots\}$:

$$\begin{aligned} V_1 &= \frac{1}{N!} \sum_{l=0}^{N-1} 1\, E_l; \\ V_2 &= \frac{1}{N!} \sum_{l=0}^{N-1} \frac{1}{2^l}\, E_l; \\ V_4 &= \frac{1}{N!} \sum_{l=0}^{N-1} \frac{1}{4^l}\, E_l; \\ &\vdots \quad \vdots \\ V_{2^{N-1}} &= \frac{1}{N!} \sum_{l=0}^{N-1} \frac{1}{2^{(N-1)l}}\, E_l. \end{aligned}$$

Or, la matrice $(2^{-ij})_{0 \le i,j \le N-1}$ est inversible, puisque son déterminant est le déterminant de Vandermonde $\prod_{0 \le i < i' \le N-1} (2^{-i} - 2^{-i'}) \neq 0$. On peut donc réciproquement écrire tous les E_l en fonction des puissances de V_2. Puisque V_a est combinaison linéaire des E_l, tout élément V_a est combinaison linéaire des puissances de V_2. Finalement, on a vu précédemment qu'il y avait une relation de passage triangulaire entre $(U_0, U_1, \ldots, U_{N-1})$ et $(V_1, V_2, \ldots, V_N)$, donc tous les éléments de base U_r de $\mathfrak{BD}(N)$ sont des polynômes en V_2. Ceci permet de reprouver que l'algèbre de Bayer–Diaconis est commutative (c'est l'image par l'évaluation en V_2 d'une algèbre de polynômes).

2.10 D'après la question précédente, tous les $V_{a \ge 1}$ sont des combinaisons linéaires de $E_0, \ldots, E_{N-1}$, et il en va de même pour les $U_{r \ge 0}$, qui forment une base de $\mathfrak{BD}(N)$. Comme cette algèbre est de dimension N, on a donc une famille génératrice $(E_l)_{l \in [0, N-1]}$ de la bonne taille, donc une base linéaire. Voyons maintenant pourquoi les $\frac{1}{N!}\, E_l$ sont des *idempotents orthogonaux*. Remarquons que, pour toute combinaison linéaire de la forme

$$V_{2^i} = \sum_{l=0}^{N-1} c(i,l)\, E_l,$$

la multiplication par V_2 multiplie chaque coefficient $c(i,l)$ par $\frac{1}{2^l}$, indépendamment de i. Par l'argument d'inversibilité de la matrice $(2^{-ij})_{0 \le i,j \le N-1}$, et puisque multiplier (à gauche ou à droite) par V_2 est une application linéaire de l'algèbre $\mathfrak{BD}(N)$ vers elle-même, on en déduit que :

$$V_2\, E_l = \frac{1}{2^l}\, E_l$$

pour tout $l \in [\![0, N-1]\!]$. Ceci implique bien sûr que pour tout polynôme en V_2,

$$P(V_2)\, E_l = P\left(\frac{1}{2^l}\right)\, E_l.$$

En particulier, pour les polynômes $P(x) = x^i$ avec $i \in [\![0, N-1]\!]$, on obtient :

$$\frac{1}{2^{il}}\, E_l = V_{2^i}\, E_l = \frac{1}{N!} \sum_{m=0}^{N-1} \frac{1}{2^{im}}\, E_m E_l.$$

De nouveau, on voit que pour toute combinaison linéaire de la forme $\sum_{m=0}^{N-1} c(i,m)\, E_m$, la multiplication par E_l annule toutes les composantes E_m sauf la composante E_l, qu'elle conserve avec coefficient $N!\, c(i,l)$. Toujours par inversibilité de la matrice de Vandermonde, ceci est vrai globalement, et ainsi,

$$E_l E_m = 1_{(l=m)}\, N!\, E_l.$$

Alors, si $x = \frac{1}{N!} \sum_{l=0}^{N-1} x_l\, E_l$ et $y = \frac{1}{N!} \sum_{l=0}^{N-1} y_l\, E_l$, on a bien

$$xy = \frac{1}{(N!)^2} \sum_{l=0}^{N-1} (x_l y_l)\, N!\, E_l = \frac{1}{N!} \sum_{l=0}^{N-1} (x_l y_l)\, E_l.$$

Donc, l'application $\Psi : \mathfrak{BD}(N) \to \mathbb{C}^N$ proposée par l'énoncé, qui est un isomorphisme linéaire puisque $(E_l)_{l \in [\![0,N-1]\!]}$ est une base, est bien compatible avec le produit et est un isomorphisme d'algèbres.

3.1 Si σ a une descente en i, alors $\tau = \sigma \circ \sigma_0$ a une montée en $N - i$, puisque

$$\tau(N+1-i) = \sigma(i) > \sigma(i+1) = \tau(N-i).$$

L'application $\sigma \mapsto \sigma \circ \sigma_0$ est donc une involution de $\mathfrak{S}(N)$ qui change le nombre de montées en le nombre de descentes. On en déduit que

$$\begin{aligned} A_{N,m} &= \text{nombre de permutations de taille } N \text{ avec } m \text{ montées} \\ &= \text{nombre de permutations de taille } N \text{ avec } m \text{ descentes.} \end{aligned}$$

Le même argument avec l'involution $\sigma \mapsto \sigma^{-1}$ montre que

$$A_{N,m} = \text{nombre de permutations de taille } N \text{ avec } m \text{ retours}$$

compte tenu de la question 1.3. Finalement, si une permutation a m montées, alors elle a $N - 1 - m$ descentes ; on en déduit la symétrie $A_{N,N-1-m} = A_{N,m}$.

3.2 Dans toute la discussion qui suit, on exclut le cas où certaines coordonnées ou sommes de coordonnées sont entières, car ces situations correspondent à des ensembles de mesure nulle. Par définition, y_i est la partie entière de $x_{i-1} - x_i$, avec pour convention $x_0 = 0$. On en déduit que, pour tout $i \in [\![1, N]\!]$, $y_1 + \cdots + y_i$ diffère de $(x_0 - x_1) + \cdots + (x_{i-1} - x_i) = -x_i$ par un entier. Autrement dit, puisque $x_i \in [0, 1)$,

$$x_i = -(y_1 + \cdots + y_i) - \lfloor -(y_1 + \cdots + y_i) \rfloor = -(y_1 + \cdots + y_i) + 1 + \lfloor y_1 + \cdots + y_i \rfloor.$$

En effet, pour un réel positif x non entier, $\lfloor -x \rfloor = -1 - \lfloor x \rfloor$. On peut donc bien inverser Ψ. Pour montrer qu'elle préserve la mesure de Lebesgue, plaçons-nous sur une partie de l'hypercube où les inégalités $x_{i-1} < x_i$ ou $x_{i-1} > x_i$ sont toutes déterminées (il y a 2^{N-1} parties de ce type, et

ces parties forment une partition de l'hypercube, à des ensembles de mesure nulle près). Sur une telle de ces parties, Ψ est une application affine, de partie linéaire donnée par la matrice

$$\begin{pmatrix} -1 & 0 & \cdots & \cdots & 0 \\ 1 & -1 & \ddots & & \vdots \\ 0 & 1 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & -1 \end{pmatrix}.$$

Le déterminant de cette matrice est $(-1)^N$, donc l'application Ψ préserve bien la mesure. Examinons maintenant l'ensemble $M_{N,m}$ et son image par Ψ. Pour commencer, notons qu'une suite $(x_1, \ldots, x_N)$ appartient à $M_{N,m}$ si et seulement si son réordonnement croissant $(x_{\sigma(1)}, \ldots, x_{\sigma(N)})$ met en jeu une permutation σ avec $N-1-m$ retours. L'application qui à une suite dans l'hypercube associe la permutation σ de son réordonnement croissant envoie la mesure de Lebesgue de $[0,1)^N$ sur la mesure uniforme sur $\mathfrak{S}(N)$. Par conséquent,

$$\mathrm{vol}(M_{N,m}) = \mathbb{P}[\text{une permutation de } \mathfrak{S}(N) \text{ a } N-1-m \text{ retours}] = \frac{A_{N,N-1-m}}{N!} = \frac{A_{N,m}}{N!}.$$

Si une suite $(x_1, \ldots, x_N)$ est dans $M_{N,m}$, alors il y a m indices $i \in [\![2, N-1]\!]$ tels que $y_i = 1 + x_{i-1} - x_i$. On a aussi $y_1 = 1 - x_1$ dans tous les cas. Par conséquent,

$$y_1 + y_2 + \cdots + y_N = (m+1) - x_N \in (m, m+1).$$

L'image de $M_{N,m}$ par Ψ est donc $H_{N,m}$, et comme Ψ est un isomorphisme de Lebesgue, on conclut que

$$\frac{A_{N,m}}{N!} = \mathrm{vol}(H_{N,m}) = \mathbb{P}[m \leq X_1 + X_2 + \cdots + X_N < m+1].$$

3.3 Considérons plus généralement deux lois ν_1 et ν_2 sur $\mathfrak{S}(N)$ avec la propriété indiquée par l'énoncé : sous $\nu_{i\in\{1,2\}}$, conditionnellement à $|R(\sigma)| = m$, une permutation σ est de loi uniforme sur U_m, l'ensemble des permutations avec m retours. On sait par ailleurs (c'est un résultat classique sur la distance en variation totale) que

$$d_{\mathrm{VT}}(\nu_1, \nu_2) = \frac{1}{2} \sum_{\sigma \in \mathfrak{S}(N)} |\nu_1(\sigma) - \nu_2(\sigma)|.$$

Si l'on décompose le groupe symétrique suivant les nombres de retours des permutations, la somme s'écrit :

$$\sum_{\sigma \in \mathfrak{S}(N)} |\nu_1(\sigma) - \nu_2(\sigma)| = \sum_{m=0}^{N-1} \sum_{\sigma \in U_m} |\nu_1(\sigma) - \nu_2(\sigma)| = \sum_{m=0}^{N-1} A_{N,m} \, |\nu_1(m) - \nu_2(m)|,$$

où $\nu_i(m)$ est la probabilité sous ν_i d'obtenir une permutation fixée avec m retours (par hypothèse, ceci ne dépend pas du choix de la permutation dans U_m). Ceci mène à la formule proposée, car :

— sous $\nu_1 = \mu_n$, la probabilité d'obtenir une permutation fixée avec m retours est

$$\nu_1(m) = \frac{1}{2^{nN}} \binom{2^n + N - m - 1}{N} = \frac{1}{N! \, 2^{nN}} \frac{(2^n + N - m - 1)!}{(2^N - m - 1)!}$$

— pour $\nu_2 =$ loi uniforme, on a $\nu_2(m) = \frac{1}{N!}$ quelque soit la valeur de m.

3.4 La somme $S_N = X_1 + \cdots + X_N$ de variables i.i.d. uniformes sur $[0,1]$ a moyenne $\frac{N}{2}$ et variance $\frac{N}{12}$, et elle vérifie donc le théorème central limite :

$$\frac{S_N - \frac{N}{2}}{\sqrt{\frac{N}{12}}} \to_{N\to+\infty} \mathcal{N}(0,1).$$

Autrement dit, pour toute fonction continue bornée f sur $\mathbb{R}$,

$$\mathbb{E}\left[f\left(\frac{S_N - \frac{N}{2}}{\sqrt{\frac{N}{12}}}\right)\right] \to_{N\to\infty} \int_{\mathbb{R}} f(x)\,\frac{\mathrm{e}^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,dx.$$

L'espérance à gauche peut être découpée en fonction de la partie entière de S_N. Si f est K-lipschitzienne, alors sur un intervalle $m \le S_N \le m+1$, $f(\frac{S_N - \frac{N}{2}}{\sqrt{\frac{N}{12}}})$ varie d'au plus $K\sqrt{\frac{12}{N}}$, donc

$$\mathbb{E}\left[f\left(\frac{S_N - \frac{N}{2}}{\sqrt{\frac{N}{12}}}\right)\right] = \sum_{m=0}^{N-1} \mathbb{P}[m \le S_N \le m+1]\; f\left(\frac{m - \frac{N}{2}}{\sqrt{\frac{N}{12}}}\right) + O\left(\frac{1}{\sqrt{N}}\right).$$

On en déduit à l'aide de la question 3.2 que $\sum_{m=0}^{N-1} \frac{A_{N,m}}{N!}\, f(x)$ tend vers l'intégrale gaussienne lorsque N tend l'infini. Examinons maintenant la fonction $f(x) = \frac{(2^n+N-m-1)!}{(2^n-m-1)!\,2^{nN}}$. Son logarithme est

$$\left(\sum_{i=0}^{N-1} \log(2^n + N - m - 1 - i)\right) - \log(2^{nN}) = \sum_{j=0}^{N-1} \log\left(\frac{2^n + j - m}{2^n}\right) = \sum_{j=0}^{N-1} \log\left(1 + \frac{j-m}{cN^{3/2}}\right)$$

puisque $n = \frac{\log(cN^{3/2})}{\log 2}$. Les $j - m$ sont d'ordre $O(N)$, donc on peut utiliser le développement de Taylor $\log(1+x) = x - \frac{x^2}{2} + O(x^3)$. Ainsi,

$$\begin{aligned}
\log(f(x)) &= \frac{1}{cN^{3/2}} \sum_{j=0}^{N-1} (j-m) - \frac{1}{2c^2N^3} \sum_{j=0}^{N-1} (j-m)^2 + O\left(\frac{1}{\sqrt{N}}\right) \\
&= -\frac{m}{c\sqrt{N}} - \frac{m^2}{2c^2N^2} + \left(\frac{1}{cN^{3/2}} + \frac{m}{c^2N^3}\right) \sum_{j=0}^{N-1} j - \frac{1}{2c^2N^3} \sum_{j=0}^{N-1} j^2 + O\left(\frac{1}{\sqrt{N}}\right) \\
&= -\frac{x}{c\sqrt{12}} - \frac{1}{24c^2} + O_x\left(\frac{1}{\sqrt{N}}\right)
\end{aligned}$$

en utilisant les formules classiques pour $\sum_{j=0}^{N-1} j$ et $\sum_{j=0}^{N-1} j^2$. En admettant qu'on puisse passer sans soucis à la limite, on en déduit donc :

$$\lim_{N\to\infty} d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = \frac{1}{2} \int_{\mathbb{R}} \left|\mathrm{e}^{-\frac{x}{c\sqrt{12}} - \frac{1}{24c^2}} - 1\right| \frac{\mathrm{e}^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,dx.$$

3.5 Finalement, pour calculer l'intégrale $I(c)$ ci-dessus, on remarque que l'exponentielle est plus petite que 1 si et seulement si $x > -\frac{1}{4\sqrt{3}c}$. On a donc :

$$I(c) = \frac{1}{2}\int_{-\infty}^{-\frac{1}{4\sqrt{3}c}} \left(\mathrm{e}^{-\frac{x}{c\sqrt{12}}-\frac{1}{24c^2}} - 1\right) \frac{\mathrm{e}^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,dx + \frac{1}{2}\int_{-\frac{1}{4\sqrt{3}c}}^{\infty} \left(1 - \mathrm{e}^{-\frac{x}{c\sqrt{12}}-\frac{1}{24c^2}}\right) \frac{\mathrm{e}^{-\frac{x^2}{2}}}{\sqrt{2\pi}}\,dx.$$

La partie avec le terme 1 dans les deux parenthèses donne $-\frac{1}{2}\,F(-\frac{1}{4\sqrt{3}c}) + \frac{1}{2}(1 - F(-\frac{1}{4\sqrt{3}c})) = \frac{1}{2}(1 - 2F(-\frac{1}{4\sqrt{3}c}))$, où F est la fonction de distribution de la gaussienne. Pour les autres termes, on remarque que :

$$-\frac{x^2}{2} - \frac{x}{c\sqrt{12}} - \frac{1}{24c^2} = -\frac{1}{2}\left(x + \frac{1}{2\sqrt{3}c}\right)^2.$$

En faisant le changement de variables $y = x + \frac{1}{2\sqrt{3}c}$, on obtient donc avec les autres termes $\frac{1}{2}F(\frac{1}{4\sqrt{3}c}) - \frac{1}{2}(1 - F(\frac{1}{4\sqrt{3}c})) = \frac{1}{2}(1 - 2F(-\frac{1}{4\sqrt{3}c}))$, ce qui est la même quantité que précédemment. Ainsi,

$$\lim_{N\to\infty} d_{\mathrm{VT}}(\sigma_n, \text{loi uniforme}) = 1 - 2F\left(-\frac{1}{4\sqrt{3}c}\right).$$

En particulier, cette limite est proche de 0 si c est grand, et est proche de 1 si c est petit. Puisque $n = \frac{3\log N}{2\log 2} + \frac{\log c}{\log 2}$, on en déduit qu'il y a un phénomène de coupure pour le battage de cartes au temps $n_{\mathrm{mix}} = \frac{3\log N}{2\log 2}$.