Mélange d'un jeu de cartes : le riffle shuffle

Florian Galliot

Mélange d'un jeu de cartes : le *riffle shuffle*

Florian Galliot

21 juin 2018

Mémoire de M2 encadré par Justin Salez

Université Pierre et Marie Curie

Un grand merci aux membres de mon jury de soutenance, pour avoir accepté de lire ce mémoire et de m'écouter pendant quarante-cinq minutes qui je l'espère leur paraîtront courtes. Je resterai très reconnaissant à Justin Salez pour ce choix de sujet qui m'a passionné et pour l'entière liberté dont j'ai bénéficié.

Table des matières

Le *riffle shuffle*, ou *dovetail shuffle*, est une technique de mélange d'un jeu de cartes, utilisée par les joueurs du monde entier et même par les croupiers dans certains casinos. Nous nous intéressons ici au modèle GSR (Gilbert-Shannon-Reeds), qui consiste en une ou plusieurs itérations du procédé suivant :

- Le croupier sépare le jeu de n cartes en deux paquets, à un emplacement qui suit une loi binomiale de paramètres $(n, \frac{1}{2})$. Remarquons que notre modèle autorise donc les paquets vides. On obtient un paquet gauche contenant g_1 cartes, et un paquet droit contenant d_1 cartes.
- Les deux paquets sont ensuite entrelacés comme suit. Imaginons que le croupier est assis à une table. Il fait tomber les cartes des deux paquets, une par une, les unes sur les autres, de manière à reformer un unique paquet construit de bas en haut. Ceci se fait donc en n étapes, où à chaque étape le croupier choisit une et une seule carte à faire tomber : ou bien la carte tout en-dessous du paquet gauche, ou bien la carte tout en-dessous du paquet droit. Dans notre modèle, ce choix se fait comme suit : en notant g_i (resp. d_i) le nombre de cartes restantes dans le paquet gauche (resp. droit) avant l'étape i, la carte tout en-dessous du paquet gauche (resp. droit) tombe avec probabilité $\frac{g_i}{g_i+d_i}$ (resp. $\frac{d_i}{g_i+d_i}$). Remarquons que l'ordre relatif des cartes du paquet gauche (resp. droit) est conservé au cours du procédé.

Ce mémoire, qui s'appuie sur l'article référence [BD] de Dave Bayer et Persi Diaconis, a pour but d'évaluer la qualité de cette technique de mélange. Combien d'itérations sont nécessaires pour que des cartes initialement triées terminent dans un ordre uniforme ou presque ? Si le jeu est mal mélangé, est-il possible d'en tirer un avantage concret en prédisant efficacement l'ordre des cartes ?

Dans un premier temps, nous présentons différentes manières de modéliser la loi décrite ci-dessus : en plus d'offrir des points de vue complémentaires sur le problème, cela va nous permettre de constater que la loi de l'arrangement des cartes après t itérations du mélange n'est pas plus complexe qu'après une seule itération, et nous obtiendrons une formule explicite pour cette loi.

Notre deuxième section consiste à étudier le temps de mélange d'un jeu de n cartes pour ce modèle, c'est-à-dire le nombre $t_{mix}^{(n)}(\varepsilon)$ d'itérations du riffle shuffle qui sont nécessaires et suffisantes pour que l'ordre des cartes approche (au sens de la variation totale) un ordre uniforme à ε près. Pour $n = 52$ et la précision critique $\varepsilon = \frac{1}{4}$, on calcule $t_{mix}^{(52)}(\frac{1}{4}) = 8$. Pour n très grand, nous obtenons un développement asymptotique de $t_{mix}^{(n)}(\varepsilon)$ à l'ordre 2, observant en particulier que $t_{mix}^{(n)}(\varepsilon) \sim \frac{3}{2}\log_2(n)$: cet équivalent est indépendant de la précision ε souhaitée, on dit qu'on a *cutoff*.

Enfin, notre troisième partie s'inspire de la considération suivante : intuitivement, un jeu mal mélangé est un jeu dont un observateur avisé peut prédire l'ordre des cartes plus facilement que s'il était parfaitement uniforme. Dans [BD], les auteurs décrivent une stratégie conjecturée comme optimale pour deviner les cartes successives d'un jeu mélangé par riffle shuffle avec *feedback*. Nous réfutons cette conjecture par un contre-exemple, mais montrons qu'une partie du raisonnement est valable et nécessaire à l'optimalité.

1 Du 2-shuffle au a-shuffle

Les n cartes du deck seront toujours assimilées à des entiers de 1 à n, et leur arrangement à une permutation $\sigma \in \mathfrak{S}_n$ et écrite en ligne. Par exemple, pour une configuration de $n = 5$ cartes dont l'ordre **de haut en bas** dans le paquet est 2-5-3-1-4, on a $\sigma = 2\ 5\ 3\ 1\ 4$. La permutation $\sigma = \mathrm{Id}$ correspond donc à un jeu trié.

Nous généralisons la méthode de mélange décrite en introduction, en séparant le jeu en a paquets au lieu de 2, définissant ce que nous appellerons un a-shuffle. Ce dernier, à la différence de ce que nous appellerons donc désormais un 2-shuffle, aura vocation à n'être effectué **qu'une seule fois** : le but est de voir t itérations d'un 2-shuffle comme une unique itération d'un 2^t-shuffle, dont nous expliciterons la loi.

1.1 Généralités

1.1.1 Suites croissantes d'une permutation

Définition. Soit $\sigma \in \mathfrak{S}_n$. On dit que σ admet une *descente* (resp. une *montée*) entre i et $i+1$ lorsque $\sigma(i) > \sigma(i+1)$ (resp. $\sigma(i) < \sigma(i+1)$). On appelle *suite croissante* de σ une suite maximale d'entiers consécutifs $i, i+1, \ldots, i+k$ vérifiant $\sigma^{-1}(i) < \sigma^{-1}(i+1) < \cdots < \sigma^{-1}(i+k)$.

Exemple. $\sigma = 7\ 3\ 1\ 4\ 5\ 2\ 6$ possède trois descentes et trois suites croissantes (1 2 ; 3 4 5 6 ; 7).

Notation. On note $d(\sigma)$ (resp. $r(\sigma)$) le nombre de descentes (resp. de suites croissantes) de $\sigma \in \mathfrak{S}_n$.

Proposition 1.1.1. *Pour tout* $\sigma \in \mathfrak{S}_n$: $r(\sigma) = 1 + d(\sigma^{-1})$.

Démonstration.
Dans l'écriture en ligne de σ, une carte $i \neq n$ marque la fin d'une suite croissante si et seulement si $i+1$ est à gauche de i i.e. $\sigma^{-1}(i+1) < \sigma^{-1}(i)$. □

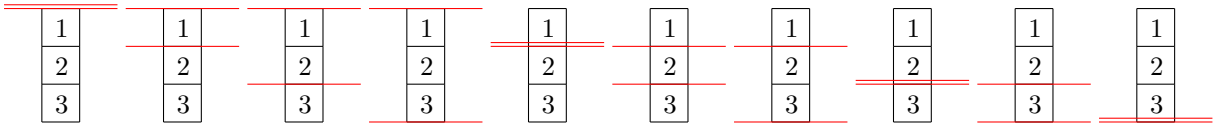
Le nombre de suites croissantes est une statistique qui va nous intéresser : un jeu de $n = 52$ cartes initialement trié contient au maximum 2 (resp. 4, resp. 8) suites croissantes après 1 (resp. 2, resp. 3) itérations du riffle shuffle, ce qui de toute évidence est trop peu et témoigne d'un mauvais mélange.

1.1.2 Le a-shuffle : définitions et notations

Notation. On note $\mathscr{P}_a(n)$ l'ensemble des valeurs possibles $p = (p_1, \ldots, p_a)$ d'une loi multinomiale de paramètres $(n, \frac{1}{a}, \ldots, \frac{1}{a})$, que l'on voit comme l'ensemble des découpes possibles d'un deck de n cartes en a paquets (où les paquets vides sont autorisés).

Définition. Etant donné $p \in \mathscr{P}_a(n)$, une séparation entre deux paquets est appelée une *coupe* de p. Il y a $a-1$ coupes au total. L'*emplacement* d'une coupe est le numéro entre 0 et n de la carte qui se situe juste au-dessus de cette coupe (une coupe située tout en haut est à l'emplacement 0).

Exemple. Pour $n = 3$ et $a = 3$, l'ensemble $\mathscr{P}_3(3)$ compte 10 éléments schématisés comme suit :



Ci-dessus, l'élément représenté tout à droite est $p = (3, 0, 0)$, et les deux coupes sont à l'emplacement 3.

Définition. On dit qu'un entrelacement $\sigma \in \mathfrak{S}_n$ est *p-compatible* lorsque les entiers appartenant à un même paquet apparaissent dans l'ordre croissant.

Notation. On note $\mathscr{C}_a(n)$ l'ensemble des couples (p, σ) où $p \in \mathscr{P}_a(n)$ et σ est p-compatible.

Proposition 1.1.2. *Pour tout $p = (p_1, \ldots, p_a) \in \mathscr{P}_a(n)$, il existe exactement $\binom{n}{p_1, \ldots, p_a}$ entrelacements p-compatibles. On en déduit par sommation que $\#\mathscr{C}_a(n) = a^n$.*

Démonstration.
Ceci est clair : on choisit les p_1 emplacements finaux des cartes du premier paquet, les p_2 emplacements finaux des cartes du deuxième paquet, etc., et une fois ces choix faits l'entrelacement est forcé par la p-compatibilité. □

Définition. On dit qu'une variable aléatoire S à valeurs dans $\mathfrak{S}_n$ a la loi d'un *a-shuffle* lorsqu'il existe une variable aléatoire P à valeurs dans $\mathscr{P}_a(n)$ telle que :

- P suit la loi multinomiale de paramètres $(n, \frac{1}{a}, \ldots, \frac{1}{a})$;
- Pour tout $p \in \mathscr{P}_a(n)$, la loi de S sachant $\{P = p\}$ est uniforme parmi les entrelacements p-compatibles.

Nous allons désormais détailler plusieurs manières de mélanger un jeu de cartes suivant cette loi.

1.2 Différents modèles pour le a-shuffle

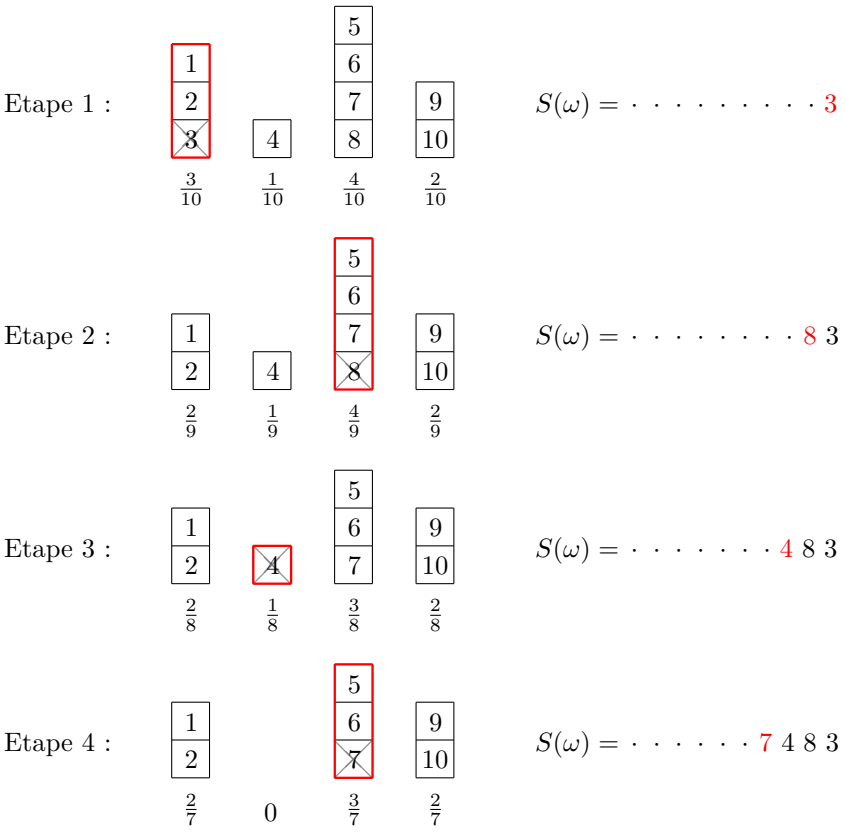
1.2.1 Description multinomiale

Cette description est la généralisation directe du mélange décrit en introduction. Le jeu de cartes, initialement trié, est découpé en a paquets comme indiqué par une multinomiale P de paramètres $(n, \frac{1}{a}, \ldots, \frac{1}{a})$. On construit l'arrangement final S du deck, carte par carte en commençant par le bas, comme suit : à chacune des n étapes, on assigne à chaque paquet une probabilité proportionnelle à sa

taille actuelle, on tire un paquet suivant cette loi (indépendamment de tous les tirages précédents) et la carte qui est en bas de ce paquet tombe dans le deck final.

Pour $a = 2$, on retrouve donc exactement le modèle présenté dans l'introduction.

Exemple. Voici un exemple avec $n = 10$, $a = 4$ et une découpe initiale en paquets $P(\omega) = (3, 1, 4, 2)$, pour les quatre premières étapes, où le paquet choisi à chaque étape est encadré en rouge :



Proposition 1.2.1. *S a la loi d'un a-shuffle.*

Démonstration.
Soit $p = (p_1, \dots, p_a) \in \mathscr{P}_a(n)$, on veut montrer que la loi de S sachant $\{P = p\}$ est uniforme parmi les $\binom{n}{p_1, \dots, p_a}$ entrelacements p-compatibles. Soit donc σ un entrelacement p-compatible : se donner σ revient à se donner la suite $(i_1, \dots, i_n) \in \{1, \dots, a\}^n$ des paquets successivement choisis au cours du procédé, où pour tout $i \in \{1, \dots, a\}$: $\#\{j \mid i_j = i\} = p_i$. Avant l'étape j, il reste $n - (j-1)$ cartes au total, dont $p_{i_j} - \#\{k < j \,|\, i_k = i_j\}$ restantes dans le paquet n°i_j. L'indépendance permet alors d'écrire que

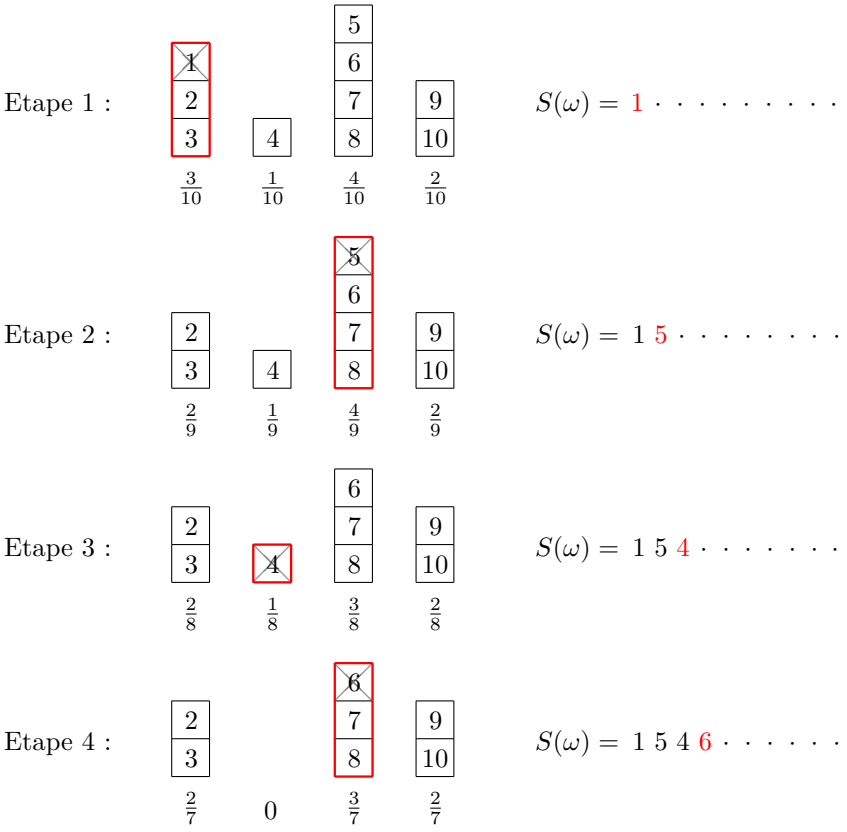
$$\mathbb{P}(S = \sigma \,|\, P = p) = \prod_{j=1}^{n} \frac{p_{i_j} - \#\{k < j \,|\, i_k = i_j\}}{n - (j-1)} = \frac{\prod_{j=1}^{n} \left(p_{i_j} - \#\{k < j \,|\, i_k = i_j\}\right)}{n!} \,,$$

où le numérateur est égal à $\displaystyle\prod_{i=1}^{a} \prod_{\substack{1 \le j \le n \\ i_j = i}} (p_i - \#\{k < j \,|\, i_k = i\}) = \prod_{i=1}^{a} p_i!$: on obtient finalement que

$\mathbb{P}(S = \sigma \,|\, P = p) = \dfrac{p_1! \cdots p_a!}{n!} = \dfrac{1}{\binom{n}{p_1, \dots, p_a}}$, ce qui conclut. □

Remarque. Notons qu'on obtiendrait de même un a-shuffle en construisant plutôt l'arrangement final du deck de haut en bas, en prenant la carte en haut du paquet choisi à chaque étape plutôt que celle du bas. La preuve est rigoureusement la même. Cette vision du mélange nous sera utile dans la dernière section de ce mémoire.

Exemple. Voici une illustration de cette remarque avec $n = 10$, $a = 4$ et une découpe initiale en paquets $P(\omega) = (3, 1, 4, 2)$, pour les quatre premières étapes :



1.2.2 Description emboitée

Le jeu de cartes, initialement trié, est ici encore découpé en a paquets comme indiqué par une multinomiale P de paramètres $(n, \frac{1}{a}, \ldots, \frac{1}{a})$. Les paquets 1 et 2 sont ensuite entrelacés comme dans le cas $a = 2$ de la description multinomiale ci-dessus, puis la réunion ainsi obtenue des paquets 1 et 2 est entrelacée de même avec le paquet 3, et ainsi de suite où les entrelacements successifs sont indépendants les uns des autres. L'arrangement final des n cartes du jeu ainsi obtenu est comme d'habitude noté S.

Proposition 1.2.2. *S a la loi d'un a-shuffle.*

Démonstration.
Pour $a = 2$, la description emboîtée est identique à la description multinomiale déjà traitée. Pour $a \geq 3$, on se ramène au cas $a = 2$ en considérant les entrelacements successifs un par un. Traitons par exemple le cas $a = 3$: soient $p = (p_1, p_2, p_3) \in \mathscr{P}_3(n)$ et σ un des $\binom{n}{p_1, p_2, p_3}$ entrelacements p-compatibles. L'entrelacement τ des paquets 1 et 2 est forcé, car l'ordre de ces cartes est conservé dans l'entrelacement final σ avec le

paquet 3. Sachant $\{P = p\}$, on sait par le cas $a = 2$ que la probabilité que l'entrelacement des paquets 1 et 2 donne τ est $\frac{1}{\binom{p_1+p_2}{p_1}}$, et qu'ensuite la probabilité que l'entrelacement de leur réunion avec le paquet 3 donne σ est $\frac{1}{\binom{p_1+p_2+p_3}{p_1+p_2}}$. En conclusion, par indépendance :

$$\mathbb{P}(S = \sigma \,|\, P = p) = \frac{1}{\binom{p_1+p_2}{p_1}} \frac{1}{\binom{p_1+p_2+p_3}{p_1+p_2}} = \frac{p_1!\,p_2!}{(p_1+p_2)!} \frac{(p_1+p_2)!\,p_3!}{n!} = \frac{1}{\binom{n}{p_1,p_2,p_3}} \,. \qquad \square$$

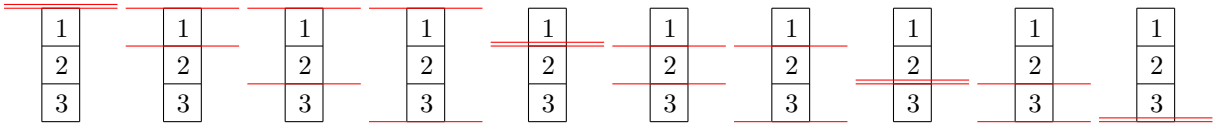
1.2.3 Description uniforme et formule pour la loi

Cette description, qui permet de transformer les calculs de probabilités en calculs de cardinaux, nous sera particulièrement utile. On se donne ici (P, S) suivant la loi uniforme sur $\mathscr{C}_a(n)$.

Proposition 1.2.3. *S a la loi d'un a-shuffle.*

Démonstration.
En notant $c(p)$ le nombre d'entrelacements p-compatibles, on a $\mathbb{P}(P = p) = \dfrac{c(p)}{\#\mathscr{C}_a(n)} = \dfrac{1}{a^n}\binom{n}{p_1, \ldots, p_a}$ d'après 1.1.2, ainsi P suit une loi multinomiale de paramètres $(n, \frac{1}{a}, \ldots, \frac{1}{a})$. De plus il est évident que la loi de S sachant P est uniforme parmi les entrelacements P-compatibles. $\square$

Exemple. Pour $n = 3$ et $a = 3$, l'ensemble $\mathscr{C}_3(3)$ compte $3^3 = 27$ éléments schématisés comme suit :



1 2 3 | 1 2 3
2 1 3
2 3 1 | 1 2 3
1 3 2
3 1 2 | 1 2 3 | 1 2 3
2 1 3
2 3 1 | 1 2 3
1 3 2
2 1 3
2 3 1
3 1 2
3 2 1 | 1 2 3
2 1 3
2 3 1 | 1 2 3
1 3 2
3 1 2 | 1 2 3
1 3 2
3 1 2 | 1 2 3

En comptant les occurrences de chaque permutation, on en déduit la loi d'un 3-shuffle sur 3 cartes :

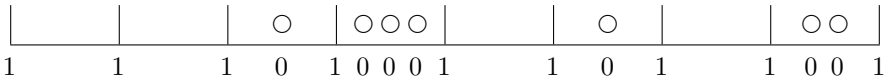
- $\mathbb{P}(S = 1\ 2\ 3) = \dfrac{10}{27}$.
- $\mathbb{P}(S = 1\ 3\ 2) = \mathbb{P}(S = 2\ 1\ 3) = \mathbb{P}(S = 2\ 3\ 1) = \mathbb{P}(S = 3\ 1\ 2) = \dfrac{4}{27}$.
- $\mathbb{P}(S = 3\ 2\ 1) = \dfrac{1}{27}$.

La description uniforme permet en fait le calcul explicite de la loi d'un a-shuffle pour n'importe quelles valeurs de n et a. C'est l'objet du théorème à suivre, qui est l'un des résultats centraux de ce mémoire.

Lemme 1.2.4. *Il y a* $\binom{m-1+k}{k}$ *façons de placer* k *objets indistinguables dans* m *boîtes distinguables.*

Démonstration.
On peut visualiser les k objets comme des boules identiques, et les boîtes comme étant numérotées et alignées bord à bord, avec la boîte 1 tout à gauche et la boîte m tout à droite. Une configuration des boules dans les boîtes peut être assimilée à un mot binaire, où les 0 représentent les boules et les 1 représentent les bords des boîtes. Deux bords collés ne comptent que pour un seul, si bien qu'il y a exactement $m+1$ occurrences de la lettre 1. Il y a obligatoirement des 1 aux deux extrémités du mot : ce sont les bords extérieurs des boîtes 1 et m. Pour le reste, chaque configuration des $m-1+k$ autres lettres est possible, et chacune correspond à une unique disposition des boules à l'intérieur des boîtes. Cela consiste à choisir où placer les k occurrences de 0 parmi les $m-1+k$ emplacements de lettres restants. □

Exemple. Pour $k=7$ et $m=8$, le mot 1110100011011001 correspond à la configuration suivante :



Théorème 1.2.5. *Pour tout* $\sigma \in \mathfrak{S}_n$: $\mathbb{P}(S=\sigma) = \dfrac{1}{a^n}\binom{a-r(\sigma)+n}{n}$ $(=0$ *par convention si* $r(\sigma)>a)$.

Démonstration.
Soit $\sigma \in \mathfrak{S}_n$, on a $\mathbb{P}(S=\sigma) = \dfrac{p(\sigma)}{\#\mathscr{C}_a(n)} = \dfrac{p(\sigma)}{a^n}$ où $p(\sigma) := \#\{p \in \mathscr{P}_a(n) \mid \sigma \text{ est } p\text{-compatible}\}$. Notons $i_1 < \cdots < i_{r(\sigma)-1}$ les cartes autres que n marquant la fin des suites croissantes de σ (il y a bien $r(\sigma)-1$ telles cartes puisque n marque toujours la fin d'une suite croissante). Alors, pour tout $p \in \mathscr{P}_a(n)$, σ est p-compatible si et seulement si p contient au moins une coupe aux emplacements $i_1, \ldots, i_{r(\sigma)-1}$. On a ainsi $r(\sigma)-1$ coupes forcées, et les $a-1-(r(\sigma)-1) = a-r(\sigma)$ coupes restantes peuvent être placées n'importe où parmi les $n+1$ emplacements possibles. Le lemme précédent permet alors de conclure que :

$$p(\sigma) = \binom{(n+1)-1+(a-r(\sigma))}{a-r(\sigma)} = \binom{a-r(\sigma)+n}{n}.$$ □

1.2.4 Description par positions et règle du produit

Notation. On note $\Pi_a(n)$ l'ensemble des a-partitions ordonnées de $\{1,\ldots,n\}$ avec parties vides autorisées, c'est-à-dire l'ensemble des $\mathbf{I} = (I_1, \ldots, I_a)$ où les I_k sont deux-à-deux disjoints et d'union $\{1,\ldots,n\}$.

Notation. Pour $\mathbf{I} \in \Pi_a(n)$, on note $\sigma_{\mathbf{I}}$ la permutation obtenue en plaçant les entiers de 1 à $\#I_1$ dans l'ordre aux positions I_1, les entiers de $\#I_1+1$ à $\#I_1+\#I_2$ dans l'ordre aux positions I_2, etc. Pour $a=2$ et la partition $(I, {}^cI)$, on note σ_I. Notons que $\sigma_{\mathbf{I}}^{-1}$ est simplement la permutation obtenue en plaçant les éléments de I_1 dans l'ordre croissant aux positions 1 à $\#I_1$, les éléments de I_2 dans l'ordre croissant aux positions $\#I_1+1$ à $\#I_1+\#I_2$, etc.

Remarque. Composer à droite par $\sigma_{\mathbf{I}}$ revient donc à placer les $\#I_1$ premières cartes aux positions I_1, les $\#I_2$ suivantes aux positions I_2, etc. Composer à droite par $\sigma_{\mathbf{I}}^{-1}$ revient à placer aux positions 1 à $\#I_1$ les

cartes qui étaient aux positions I_1, aux positions $\#I_1+1$ à $\#I_1+\#I_2$ les cartes qui étaient aux positions I_2, etc.

La description par positions consiste à se donner les positions finales des cartes de chaque paquet, la définition de S étant alors forcée par la compatibilité, en procédant comme suit. On assigne à chaque position i une variable aléatoire U_i uniforme sur $\{1,\dots,a\}$, avec $U_1,\dots,U_n$ indépendantes. On pose $\mathbf{I}\in\Pi_a(n)$ la partition "associée" aux U_i, définie par $I_k:=\{i\,|\,U_i=k\}$, puis on pose $S:=\sigma_{\mathbf{I}}$.

Exemple. Supposons $n=13$, $a=3$ et $(U_i(\omega))_{1\le i\le 13}=(2,3,1,3,2,3,1,3,2,3,2,3,3)$.
Alors $S(\omega)=3\ 7\ 1\ 8\ 4\ 9\ 2\ 10\ 5\ 11\ 6\ 12\ 13$ et $S^{-1}(\omega)=3\ 7\ 1\ 5\ 9\ 11\ 2\ 4\ 6\ 8\ 10\ 12\ 13$.

Proposition 1.2.6. *S a la loi d'un a-shuffle.*

Démonstration.
Posons $P_k:=\#I_k$, alors $P=(P_1,\dots,P_a)$ suit la loi multinomiale de paramètres $(n,\frac{1}{a},\dots,\frac{1}{a})$. Soit $(p,\sigma)\in\mathscr{C}_a(n)$, il reste à montrer que $\mathbb{P}(S=\sigma\,|\,P=p)=\frac{1}{\binom{n}{p_1,\cdots,p_a}}$, c'est-à-dire que $\mathbb{P}(S=\sigma,P=p)=\frac{1}{a^n}$. Ceci est vérifié car $\mathbb{P}(S=\sigma,P=p)=\mathbb{P}\left(\bigcap_{k=1}^{a}\{U_{\sigma^{-1}(p_1+\dots+p_{k-1}+1)}=\dots=U_{\sigma^{-1}(p_1+\dots+p_k)}=k\}\right)=\left(\frac{1}{a}\right)^n$. □

Nous proposons une première application de la description par positions : le calcul explicite de la loi de la première carte d'un jeu mélangé par un a-shuffle.

Proposition 1.2.7. $\mathbb{P}(S(1)=1)=\dfrac{1}{a^n}\displaystyle\sum_{k=1}^{a}k^{n-1}$, *et* $\forall\, j\ge 2:\ \mathbb{P}(S(1)=j)=\dfrac{\binom{n-1}{j-1}}{a^n}\displaystyle\sum_{k=1}^{a-1}k^{n-j}(a-k)^{j-1}$.

Démonstration.

- Remarquons que $S(1)=1$ équivaut à $U_1=\min\limits_{1\le i\le n}U_i$, d'où en discutant suivant la valeur de U_1 :

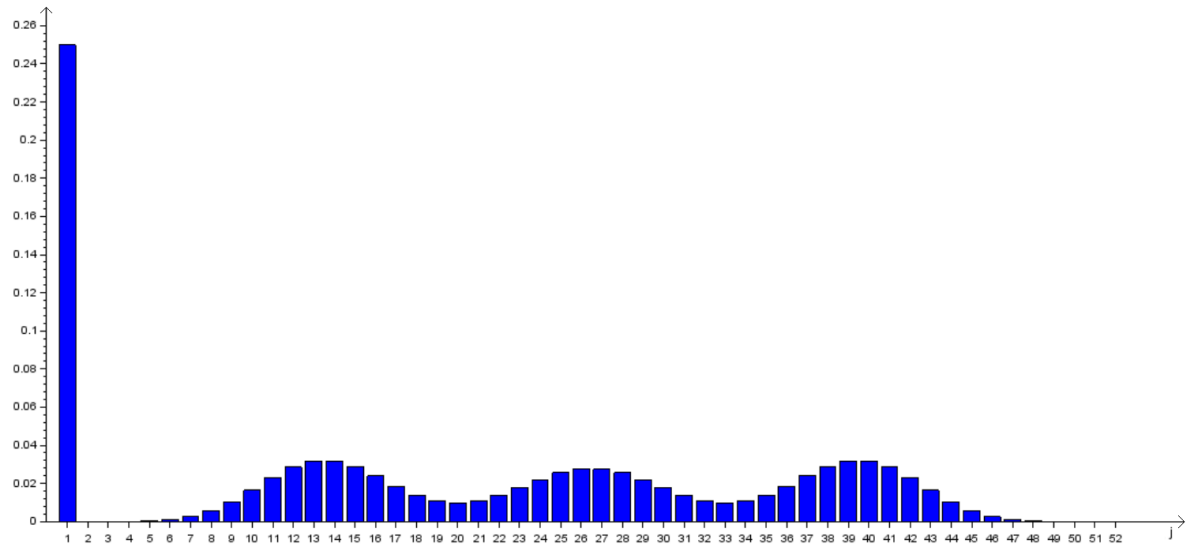
$$\mathbb{P}(S(1)=1)=\sum_{k=1}^{a}\mathbb{P}\left(\{U_1=k\}\cap\bigcap_{i=2}^{n}\{U_i\ge k\}\right)=\sum_{k=1}^{a}\frac{1}{a}\left(\frac{a-(k-1)}{a}\right)^{n-1}=\frac{1}{a^n}\sum_{k=1}^{a}k^{n-1}.$$

- Soit $j\in\{2,\dots,n\}$. Sur l'évènement $\{U_1=1\}$, on a $S(1)=1\neq j$. Sur $\{U_1=k\}$ où $k\ge 2$, on a $S(1)=j$ si et seulement si exactement $j-1$ positions ont leur marque U_i entre 1 et $k-1$:

$$\begin{aligned}\mathbb{P}(S(1)=j)&=\sum_{k=2}^{a}\mathbb{P}(U_1=k,\ \#\{i\ge 2\,|\,U_i\le k-1\}=j-1)\\&=\sum_{k=2}^{a}\mathbb{P}(U_1=k)\sum_{\substack{I\subset\{2,\dots,n\}\\ \#I=j-1}}\mathbb{P}\left(\bigcap_{i\in I}\{U_i\le k-1\}\cap\bigcap_{i\notin I}\{U_i\ge k\}\right)\\&=\sum_{k=2}^{a}\frac{1}{a}\binom{n-1}{j-1}\left(\frac{k-1}{a}\right)^{j-1}\left(\frac{a-(k-1)}{a}\right)^{n-1-(j-1)}\\&=\frac{\binom{n-1}{j-1}}{a^n}\sum_{k=1}^{a-1}k^{n-j}(a-k)^{j-1}.\end{aligned}$$

□

Exemple. Voici le graphe de $j \mapsto \mathbb{P}(S(1) = j)$ pour $n = 52$ et $a = 4$:



L'application principale de la description par positions est le résultat crucial suivant : la loi du 2-shuffle itéré t fois, qui est celle qui nous intéresse, est précisément la loi du 2^t-shuffle. Nous énonçons une règle plus générale, sur la composition d'un a-shuffle et d'un b-shuffle indépendants où a et b sont quelconques.

Proposition 1.2.8. *On assigne à chaque carte j un mot (V_j, U_j), où les U_j (resp. V_j) sont uniformes sur $\{1, \dots, a\}$ (resp. $\{1, \dots, b\}$) et toutes ces variables sont indépendantes. Notons T la permutation dans laquelle l'ordre des cartes est l'ordre lexicographique de leurs mots associés, avec départage par la plus petite valeur de la carte. Alors $T = \sigma_{\mathbf{I}}^{-1} \circ \sigma_{\mathbf{I}'}^{-1}$, où $\mathbf{I} \in \Pi_a(n)$ est la partition associée aux U_j et $\mathbf{I}' \in \Pi_b(n)$ est la partition associée aux $V_{\sigma_{\mathbf{I}}^{-1}(j)}$. De plus, $\sigma_{\mathbf{I}}$ et $\sigma_{\mathbf{I}'}$ sont un a-shuffle et un b-shuffle indépendants.*

Démonstration.
La permutation T peut s'obtenir à partir de Id en deux étapes :

- Etape 1 : on trie suivant la valeur de U_j. Les cartes j telles que $U_j = 1$ sont placées au début, les cartes j telles que $U_j = 2$ viennent juste après, etc. : on obtient donc la permutation $\sigma_{\mathbf{I}}^{-1}$.
- Etape 2 : on trie suivant la valeur de V_j. Les cartes j telles que $V_j = 1$, c'est-à-dire les cartes dont la position actuelle i vérifie $V_{\sigma_{\mathbf{I}}^{-1}(i)} = 1$, sont placées au début. Les cartes j telles que $V_j = 2$, c'est-à-dire les cartes dont la position actuelle i vérifie $V_{\sigma_{\mathbf{I}}^{-1}(i)} = 2$, viennent juste après, etc. Ceci revient à composer à droite par $\sigma_{\mathbf{I}'}^{-1}$: on obtient donc finalement la permutation $\sigma_{\mathbf{I}}^{-1} \circ \sigma_{\mathbf{I}'}^{-1}$.

Comme $\mathbf{I}'$ dépend de $\mathbf{I}$, la dernière assertion mérite d'être vérifiée. Soient $\mathbf{u} \in \{1, \dots, a\}^n$ et $\mathbf{v} \in \{1, \dots, b\}^n$, alors en notant $\pi \in \Pi_a(n)$ la partition associée aux u_i :
$\mathbb{P}((U_i)_i = \mathbf{u}, (V_{\sigma_{\mathbf{I}}^{-1}(i)})_i = \mathbf{v}) = \mathbb{P}((U_i)_i = \mathbf{u}, (V_{\sigma_{\pi}^{-1}(i)})_i = \mathbf{v}) = \mathbb{P}((U_i)_i = \mathbf{u})\mathbb{P}((V_{\sigma_{\pi}^{-1}(i)})_i = \mathbf{v}) = \dfrac{1}{a^n}\dfrac{1}{b^n}$. □

Théorème 1.2.9. *Soient S_a ayant la loi d'un a-shuffle et S_b ayant la loi d'un b-shuffle, indépendants. Alors $S_a \circ S_b$ a la loi d'un ab-shuffle.*

Démonstration.
Reprenons les notations de la proposition précédente. D'une part : $T^{-1} = \sigma_{\mathbf{I}'} \circ \sigma_{\mathbf{I}} \overset{\text{loi}}{=} S_b \circ S_a$. D'autre part, la définition de T permet d'écrire $T = \sigma_{\mathbf{J}}^{-1}$, avec $\mathbf{J} \in \Pi_{ab}(n)$ définie par $J_m := \{i \mid W_i = m\}$ où $W_i := U_i + (V_i - 1)a$. Les W_i étant indépendantes uniformes sur $\{1, \dots, ab\}$, on en déduit que $T^{-1} = \sigma_{\mathbf{J}}$

a la loi d'un ab-shuffle. Ceci montre le théorème pour $S_b \circ S_a$, d'où le même résultat pour $S_a \circ S_b$ en échangeant les rôles de a et b. □

1.3 Interprétation markovienne

Soient $(R_t)_{t\geq 1}$ des 2-shuffle indépendants. Notre objet d'intérêt est la marche aléatoire $(S_t)_{t\in\mathbb{N}}$, où $S_t := R_1 \circ \cdots \circ R_t$ décrit l'arrangement des cartes après t itérations du riffle shuffle. Nous savons désormais grâce à 1.2.9 que S_t a la loi d'un 2^t-shuffle. En utilisant l'expression de cette loi calculée en 1.2.5, nous obtenons les résultats suivants :

Théorème 1.3.1. *$(S_t)_{t\in\mathbb{N}}$ est une marche aléatoire sur $\mathfrak{S}_n$, issue de* Id *et de loi d'incréments μ définie par $\mu(\tau) = \frac{1}{2^n}\binom{n+2-r(\tau)}{n}$. En particulier, $(S_t)_{t\in\mathbb{N}}$ est une chaîne de Markov de loi initiale δ_{Id} et de matrice de transition P définie par $P(\sigma,\sigma') = \mu(\sigma^{-1}\sigma')$, et pour tout $t \in \mathbb{N}$: $P^t(\mathrm{Id},\sigma) = \frac{1}{2^{tn}}\binom{n+2^t-r(\sigma)}{n}$.*

Théorème 1.3.2. *Soit $\sigma_0 \in \mathfrak{S}_n$, on pose $T_t := \sigma_0 \circ R_1^{-1} \circ \cdots \circ R_t^{-1}$. Alors $(T_t)_{t\in\mathbb{N}}$ est une marche aléatoire sur $\mathfrak{S}_n$, issue de σ_0 et de loi d'incréments μ_* définie par $\mu_*(\tau) = \mu(\tau^{-1})$. En particulier, $(T_t)_{t\in\mathbb{N}}$ est une chaîne de Markov de loi initiale δ_{σ_0} et de matrice de transition P^*, où P^* désigne le noyau dual de P défini par $P^*(\sigma,\sigma') := \frac{\pi(\sigma')P(\sigma',\sigma)}{\pi(\sigma)} = P(\sigma',\sigma)$.*

Enfin, la proposition suivante assure que le mélange se fait bel et bien :

Proposition 1.3.3. *La matrice P (ainsi que P^* par suite) est irréductible et apériodique, de loi invariante π uniforme sur $\mathfrak{S}_n$. En particulier : $S_t \xrightarrow[t\to\infty]{loi} \pi$.*

Démonstration.
P est irréductible si et seulement si le support de la loi d'incréments μ engendre $\mathfrak{S}_n$, ainsi il suffit de montrer que les transpositions $(i \quad i+1)$ sont dans le support de μ. Or on sait que celui-ci est constitué des permutations possédant au maximum 2 suites croissantes : comme $(i \quad i+1)$ compte exactement 1 descente i.e. 2 suites croissantes, l'irréductibilité est établie. Le fait que Id soit également dans le support de μ assure l'apériodicité. Enfin, pour tout σ : $\sum_\tau \pi(\tau)P(\tau,\sigma) = \frac{1}{n!}\sum_\tau \mu(\tau^{-1}\sigma) = \frac{1}{n!}\sum_\tau \mu(\tau) = \frac{1}{n!} = \pi(\sigma)$, donc π est bien la loi invariante. □

2 Etude du temps de mélange

D'après 1.3.3, l'ordre des cartes tend donc vers un ordre uniforme lorsque le nombre t d'itérations du riffle shuffle tend vers l'infini. Cependant, ce résultat asymptotique ne nous convient pas : nous souhaitons savoir exactement combien d'itérations effectuer dans la pratique pour que le jeu soit suffisamment bien mélangé. Nous avons donc besoin de quantifier l'écart à t fixé entre la loi de S_t et la loi uniforme limite π, ce qui se fait à l'aide de la distance en variation totale.

2.1 Rappels sur la distance en variation totale et le temps de mélange

Définition. Pour un ensemble fini E, la *distance en variation totale* est la distance $\mathrm{d_{tv}}$ sur l'ensemble des probabilités sur E définie par $\mathrm{d_{tv}}(\nu_1, \nu_2) := \max_{A \subset E} |\nu_1(A) - \nu_2(A)| = \sum_{x \in E} (\nu_1(x) - \nu_2(x))_+$.

Proposition. *Soient $X, (X_t)_{t\in\mathbb{N}}$ des variables aléatoires à valeurs dans E, de lois respectives $\nu, (\nu_t)_{t\in\mathbb{N}}$. Alors $X_t \xrightarrow[t\to\infty]{loi} X$ si et seulement si $\mathrm{d_{tv}}(\nu_t, \nu) \xrightarrow[t\to\infty]{} 0$.*

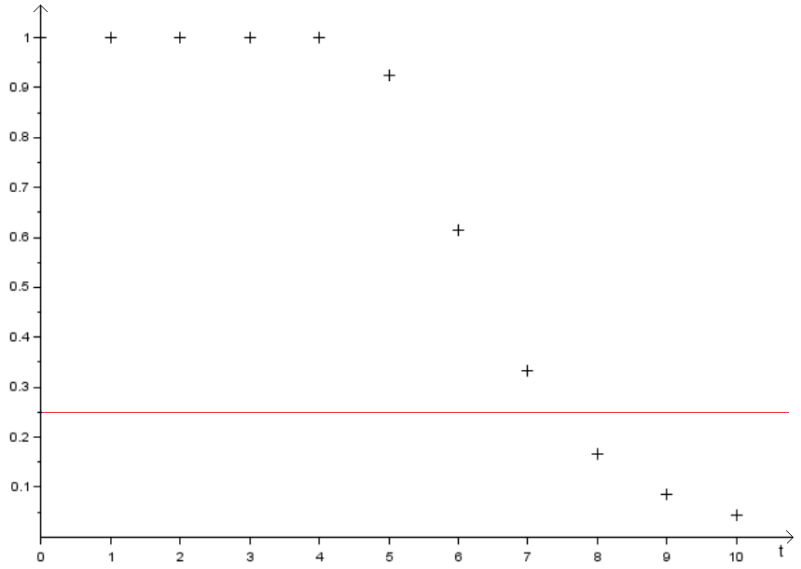
Notation. Pour $E = \mathfrak{S}_n$ et $t \in \mathbb{N}$, on définit $\mathscr{D}_n(t) := \mathrm{d_{tv}}(P^t(\mathrm{Id}, \cdot\,), \pi) = \sum_{\sigma \in \mathfrak{S}_n} (\frac{1}{n!} - P^t(\mathrm{Id}, \sigma))_+$.

La distance en variation totale est une mesure satisfaisante de l'écart à l'uniformité : si $\mathscr{D}_n(t)$ est très petit, alors il n'existe aucun évènement qui ait une probabilité éloignée de ce qu'on aurait sous une loi uniforme, c'est-à-dire qu'un jeu de cartes mélangé par t itérations du riffle shuffle ne présente aucune anomalie qu'un joueur observateur pourrait mettre à profit.

Proposition. *La fonction $t \mapsto \mathscr{D}_n(t)$ décroît vers 0. De plus, pour tous $t, s \in \mathbb{N}$: $\mathscr{D}_n(t+s) \leq 2\mathscr{D}_n(t)\mathscr{D}_n(s)$: en particulier, si $\mathscr{D}_n(t) \leq \frac{1}{4}$, alors pour tout $k \geq 1$: $\mathscr{D}_n(k.t) \leq 2^{-k-1}$.*

Définition. Pour $\varepsilon > 0$, on définit $t_{mix}^{(n)}(\varepsilon) := \inf\{t \in \mathbb{N} \,|\, \mathscr{D}_n(t) \leq \varepsilon\}$. On note $t_{mix}^{(n)} := t_{mix}^{(n)}(\frac{1}{4})$: la proposition précédente assure qu'à partir de $t = t_{mix}^{(n)}$ le mélange progresse très rapidement. Le temps $t_{mix}^{(n)}(\varepsilon)$, ou parfois $t_{mix}^{(n)}$ précisément, est appelé *temps de mélange* de la chaîne de Markov $(S_t)_{t\in\mathbb{N}}$.

Exemple. La formule donnée en 1.3.1 permet le calcul exact de $t \mapsto \mathscr{D}_n(t)$ à n fixé, par ordinateur. Pour $n = 52$, les valeurs de $\mathscr{D}_{52}(t)$ jusqu'à $t = 10$ sont données dans [BD, Table 1], et représentées ci-dessous (la ligne rouge représente le seuil $\frac{1}{4}$). On observe en particulier que $t_{mix}^{(52)} = 8$. Remarquons la brusque amélioration du mélange entre la quatrième et la huitième itération du riffle shuffle, présageant du phénomène de *cutoff* que nous démontrerons par la suite.



t	0	1	2	3	4	5	6	7	8	9	10
$\mathscr{D}_{52}(t)$	1.000	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043

2.2 Un premier encadrement du temps de mélange

Si on considère plutôt $n \to \infty$, le but est d'obtenir de bonnes bornes sur $t_{mix}^{(n)}(\varepsilon)$, voire un équivalent si possible. Nous montrons dans un premier temps comment, dans le cas du riffle shuffle, des méthodes élémentaires permettent d'obtenir un excellent encadrement de $t_{mix}^{(n)}(\varepsilon)$. La minoration et la majoration reposent chacune sur un théorème très général, valable pour n'importe quelle chaîne de Markov irréductible apériodique sur un espace d'états fini.

2.2.1 Minoration par une méthode géométrique

Théorème. *Pour tout* $\varepsilon > 0$ *:* $t_{mix}^{(n)}(\varepsilon) \geq \dfrac{\ln(1-\varepsilon) - \ln\left(\max\limits_{\sigma \in \mathfrak{S}_n} \pi(\sigma)\right)}{\ln \Delta}$*, où* $\Delta := \max\limits_{\sigma \in \mathfrak{S}_n} \#\{\tau \,|\, P(\sigma,\tau) > 0\}$.

Proposition 2.2.1. *Pour tout* $\varepsilon > 0$ *:* $\liminf \dfrac{t_{mix}^{(n)}(\varepsilon)}{\log_2(n)} \geq 1$*. On note cela* $t_{mix}^{(n)}(\varepsilon) \gtrsim \log_2(n)$.

Démonstration.
La description uniforme montre qu'un 2-shuffle ne peut prendre que $\#\mathscr{C}_2(n) = 2^n$ valeurs différentes au maximum, ainsi $\Delta \leq 2^n$. Soit $\varepsilon > 0$, le théorème assure donc que $t_{mix}^{(n)}(\varepsilon) \geq \frac{\ln(1-\varepsilon)+\ln(n!)}{n\ln(2)}$. Enfin, la formule de Stirling donne l'équivalent $\ln(n!) \sim n\ln(n)$, d'où $t_{mix}^{(n)}(\varepsilon) \gtrsim \frac{\ln(n)}{\ln(2)} = \log_2(n)$. □

Remarque. Notre étude des nombres eulériens à venir montre qu'en réalité $\Delta = 2^n - n$, ainsi il n'y a eu aucune perte de qualité lors de la majoration $\Delta \leq 2^n$ ci-dessus.

2.2.2 Majoration par un argument de couplage

Théorème. *Soit Q un noyau de couplage de P. Pour chaque $(\sigma, \tau) \in \mathfrak{S}_n^2$, on se donne une chaîne de Markov $(X_t, Y_t)_{t\in\mathbb{N}}$ de loi initiale $\delta_{(\sigma,\tau)}$ et de matrice de transition Q, et on pose $T_{\sigma,\tau} := \inf\{t \,|\, X_t = Y_t\}$. Alors pour tout $t \in \mathbb{N}$: $\mathscr{D}_n(t) \leq \max\limits_{(\sigma,\tau)\in\mathfrak{S}_n^2} \mathbb{P}(T_{\sigma,\tau} > t)$.*

Nous n'allons pas appliquer ce théorème à P directement, mais plutôt au noyau dual P^*, en utilisant le fait que l'étude du temps de mélange pour P et pour P^* est strictement la même :

Proposition 2.2.2. *Posons $\mathscr{D}_n^*(t) := \mathrm{d_{tv}}((P^*)^t(\mathrm{Id}, \cdot\,), \pi)$, alors $\mathscr{D}_n = \mathscr{D}_n^*$.*

Démonstration.
Notons μ_t (resp. ν_t) la convolution de μ (resp. μ_*) avec elle-même t fois, alors quel que soit $t \in \mathbb{N}$:

$$\mathscr{D}_n(t) = \sum_{\sigma\in\mathfrak{S}_n} \left(\frac{1}{n!} - \mu_t(\sigma)\right)_+ = \sum_{\sigma\in\mathfrak{S}_n} \left(\frac{1}{n!} - \mu_t(\sigma^{-1})\right)_+ = \sum_{\sigma\in\mathfrak{S}_n} \left(\frac{1}{n!} - \nu_t(\sigma)\right)_+ = \mathscr{D}_n^*(t)\,. \qquad \square$$

Proposition 2.2.3. *Pour tout $\varepsilon > 0$: $\limsup \dfrac{t_{mix}^{(n)}(\varepsilon)}{2\log_2(n)} \leq 1$. On note cela $t_{mix}^{(n)}(\varepsilon) \lesssim 2\log_2(n)$.*

Démonstration.
Soit $(\sigma, \tau) \in \mathfrak{S}_n^2$. On se donne une famille indépendante $(U_i(t))_{1\leq i\leq n, t\geq 1}$ de variables uniformes sur $\{1, 2\}$, et on définit $(X_t, Y_t)_{t\in\mathbb{N}}$ comme suit :

- On pose $X_0 = \sigma$, et pour $t \geq 1$ on définit X_t où l'ordre de i et j est l'ordre lexicographique sur les mots associés $M_i(t) := (U_i(t), U_i(t-1), \ldots, U_i(1))$ et $M_j(t) := (U_j(t), U_j(t-1), \ldots, U_j(1))$, avec départage par l'ordre dans σ ;
- On pose $Y_0 = \tau$, et pour $t \geq 1$ on définit Y_t comme pour X_t à la différence que l'on départage par l'ordre dans τ ;

La même preuve qu'en 1.2.8 montre qu'on peut écrire $X_t = \sigma \circ R_1^{-1} \circ \cdots \circ R_t^{-1}$ où les $(R_t)_{t\geq 1}$ sont des 2-shuffle indépendants, et $Y_t = \tau \circ {R'}_1^{-1} \circ \cdots \circ {R'}_t^{-1}$ où les $(R'_t)_{t\geq 1}$ sont des 2-shuffle indépendants. On est donc exactement dans le cadre du théorème 1.3.2, ce qui assure que $(X_t, Y_t)_{t\in\mathbb{N}}$ est un couplage du noyau P^*, de loi initiale $\delta_{(\sigma,\tau)}$.
Si deux cartes i et j vérifient $M_i(t) \neq M_j(t)$, alors il n'y a pas de départage par σ et τ : l'ordre de i et j est le même dans X_t et dans Y_t, donné par l'ordre lexicographique sur $M_i(t)$ et $M_j(t)$. Par conséquent, si les mots $M_1(t), \ldots, M_n(t)$ sont deux-à-deux distincts, alors $X_t = Y_t$: on en déduit l'inclusion d'évènements $\{T_{\sigma,\tau} > t\} \subset \{\exists\ i \neq j \mid M_i(t) = M_j(t)\}$ d'où $\mathbb{P}(T_{\sigma,\tau} > t) \leq \sum_{i\neq j} \mathbb{P}(M_i(t) = M_j(t)) = \frac{n(n-1)}{2}\frac{1}{2^t}$. D'après le théorème précédent, $\mathscr{D}_n(t) \leq \frac{n(n-1)}{2}\frac{1}{2^t}$. En particulier, pour tout $\alpha > 2$: $\mathscr{D}_n(\lceil \alpha \log_2(n)\rceil) \xrightarrow[n\to\infty]{} 0$, ce qui signifie précisément que pour tout $\varepsilon > 0$: $t_{mix}^{(n)}(\varepsilon) \lesssim 2\log_2(n)$. $\square$

2.3 Cutoff pour le riffle shuffle

En résumé, nous avons obtenu que pour tout $\varepsilon > 0$: $\log_2(n) \lesssim t_{mix}^{(n)}(\varepsilon) \lesssim 2\log_2(n)$. Nous allons montrer que le juste équivalent se trouve exactement au milieu, en $\frac{3}{2}\log_2(n)$, et nous obtiendrons même le deuxième terme du développement asymptotique. Notre méthode se base sur l'observation suivante, qui découle immédiatement de notre définition de $\mathscr{D}_n(t)$:

Proposition 2.3.1. *$\mathscr{D}_n(t) = \mathbb{E}((1 - n!P^t(\mathrm{Id}, \Sigma))_+)$, où Σ suit la loi uniforme sur $\mathfrak{S}_n$.*

Comme $P^t(\mathrm{Id}, \sigma)$ ne dépend que de $r(\sigma)$, on en vient à étudier les propriétés de la variable aléatoire $r(\Sigma)$. Notons que $r(\Sigma) \overset{\text{loi}}{=} r(\Sigma^{-1}) = 1 + d(\Sigma) = 1 + \sum_{i=1}^{n-1} \mathbf{1}_{\Sigma(i)>\Sigma(i+1)}$: les $\mathbf{1}_{\Sigma(i)>\Sigma(i+1)}$ sont des variables de Bernoulli de paramètre $\frac{1}{2}$ non indépendantes, mais on peut espérer que $r(\Sigma)$ vérifie une propriété type théorème central limite. Nous montrons ceci dans la partie qui suit, inspirée de [Tan] et [Fel].

2.3.1 Théorème central limite pour les nombres eulériens

Définition. Pour $j \in \{0, \dots, n-1\}$, on définit le *nombre eulérien* $a_{n,j} := \#\{\sigma \in \mathfrak{S}_n \,|\, d(\sigma) = j\}$.

Remarque. Comme $r(\Sigma) \overset{\text{loi}}{=} 1 + d(\Sigma)$, on a pour tout $k \in \{1, \dots, n\}$: $\mathbb{P}(r(\Sigma) = k) = \dfrac{a_{n,k-1}}{n!}$.

Proposition 2.3.2. *$a_{n+1,j} = (n - j + 1)a_{n,j-1} + (j + 1)a_{n,j}$, où $a_{n,-1} = a_{n,n} = 0$ par convention.*

Démonstration.
On définit la surjection $s : \mathfrak{S}_{n+1} \longrightarrow \mathfrak{S}_n$ où $s(\sigma)$ est obtenue en retirant à σ l'entier $n+1$ dans son écriture en ligne. On voit facilement que $d(s(\sigma)) \in \{d(\sigma) - 1, d(\sigma)\}$ d'où :

$$a_{n+1,j} = \sum_{\substack{\tau \in \mathfrak{S}_n \\ d(\tau) = j-1}} \#\{\sigma \in \mathfrak{S}_{n+1} \,|\, d(\sigma) = j \text{ et } s(\sigma) = \tau\} + \sum_{\substack{\tau \in \mathfrak{S}_n \\ d(\tau) = j}} \#\{\sigma \in \mathfrak{S}_{n+1} \,|\, d(\sigma) = j \text{ et } s(\sigma) = \tau\}.$$

- Si $d(\tau) = j - 1$, on doit rajouter une descente pour obtenir $d(\sigma) = j$, donc on doit insérer $n+1$ soit tout au début soit au milieu d'une montée. Comme τ contient $n - j$ montées, cela fait $n - j + 1$ emplacements possibles au total. Ainsi, τ possède $n - j + 1$ antécédents par s qui ont j descentes.
- Si $d(\tau) = j$, pour obtenir $d(\sigma) = j$ on doit insérer $n+1$ soit tout à la fin soit au milieu d'une descente, ce qui fait $j + 1$ emplacements possibles. Ainsi, τ possède $j + 1$ antécédents par s qui ont j descentes.

On obtient donc bien la formule annoncée. □

Cette relation de récurrence permet d'obtenir une formule explicite pour les nombres eulériens :

Proposition 2.3.3. $a_{n,j} = \displaystyle\sum_{i=0}^{j} (-1)^i \binom{n+1}{i} (j + 1 - i)^n.$

Démonstration.
On vérifie par récurrence sur n que cette formule est vraie pour tout j. Pour $n = 1$, le calcul est immédiat. Soit donc $n \geq 1$ tel que la proposition soit vraie pour n, on veut montrer que $a_{n+1,j}$ est égal à :

$$\sum_{i=0}^{j}(-1)^i\binom{n+2}{i}(j+1-i)^{n+1} = (j+1)\sum_{i=0}^{j}(-1)^i\binom{n+2}{i}(j+1-i)^n - \sum_{i=1}^{j}(-1)^i\, i\binom{n+2}{i}(j+1-i)^n .$$

On étudie séparément $S_1 := \sum_{i=0}^{j}(-1)^i\binom{n+2}{i}(j+1-i)^n$ et $S_2 := \sum_{i=1}^{j}(-1)^i\, i\binom{n+2}{i}(j+1-i)^n$.

- La relation de Pascal et l'hypothèse de récurrence donnent :
$$\begin{aligned} S_1 &= \sum_{i=0}^{j}(-1)^i\binom{n+1}{i}(j+1-i)^n + \sum_{i=1}^{j}(-1)^i\binom{n+1}{i-1}(j+1-i)^n \\ &= \sum_{i=0}^{j}(-1)^i\binom{n+1}{i}(j+1-i)^n - \sum_{i=0}^{j-1}(-1)^i\binom{n+1}{i}(j-i)^n \\ &= a_{n,j} - a_{n,j-1}. \end{aligned}$$
- $S_2 = -\sum_{i=0}^{j-1}(-1)^i\,(i+1)\binom{n+2}{i+1}(j-i)^n$,
or $(i+1)\binom{n+2}{i+1} = (n+2)\binom{n+1}{i}$ donc par hypothèse de récurrence : $S_2 = -(n+2)a_{n,j-1}$.

On en conclut que

$$\sum_{i=0}^{j}(-1)^i\binom{n+2}{i}(j+1-i)^{n+1} = (j+1)S_1 - S_2 = (n-j+1)a_{n,j-1} + (j+1)a_{n,j} = a_{n+1,j} ,$$

où la dernière inégalité vient de 2.3.2. Ceci termine la récurrence. □

On se donne désormais $X_1, \ldots, X_n$ indépendantes uniformes sur $[0,1]$. On pose $S_n := X_1 + \ldots + X_n$ et on note F_n la fonction de répartition de S_n.

Lemme 2.3.4. *S_n admet la densité f_n définie pour $x \leq n$ par $f_n(x) = \frac{1}{(n-1)!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}(x-i)_+^{n-1}$, où $x_+^n := (x_+)^n$ si $n \geq 1$ et $x_+^0 := \mathbf{1}_{x\geq 0}$. Ainsi, pour tout $x \in [0,n]$: $F_n(x) = \frac{1}{n!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}(x-i)_+^n$.*

Démonstration.
La deuxième assertion découle immédiatement de la première par intégration. On montre la première assertion par récurrence sur $n \geq 1$. Pour $n = 1$, le résultat est évident. Supposons le résultat vrai pour $n \geq 1$, alors S_{n+1} admet la densité f_{n+1} définie pour $x \leq n+1$ par :

$$f_{n+1}(x) = (f_n * \mathbf{1}_{[0,1]})(x) = \int_0^1 f_n(x-y)\,\mathrm{d}y = \int_{x-1}^{x} f_n(y)\,\mathrm{d}y = \frac{1}{(n-1)!}\sum_{i=0}^{n}(-1)^i\binom{n}{i}\int_{x-1}^{x}(y-i)_+^{n-1}\,\mathrm{d}y ,$$

où on a utilisé l'hypothèse de récurrence. On obtient donc que :

$$f_{n+1}(x) = \frac{1}{n!}\left(\sum_{i=0}^{n}(-1)^i\binom{n}{i}(x-i)_+^n + \sum_{i=0}^{n}(-1)^{i+1}\binom{n}{i}(x-1-i)_+^n\right) .$$

- La première somme vaut $x_+^n + \sum_{i=1}^{n+1}(-1)^i\binom{n}{i}(x-i)_+^n$, car le terme ajouté $i = n+1$ est nul.

- La deuxième somme vaut $\sum_{i=1}^{n+1}(-1)^i\binom{n}{i-1}(x-i)_+^n$ après changement d'indice.

La relation de Pascal termine la récurrence : $f_{n+1}(x) = x_+^n + \frac{1}{n!}\sum_{i=1}^{n+1}(-1)^i\binom{n+1}{i}(x-i)_+^n$. □

Proposition 2.3.5. $r(\Sigma) \overset{loi}{=} 1 + \lfloor S_n \rfloor$.

Démonstration.
Soit $j \in \{0, \dots, n-1\}$. D'après le lemme précédent :

$$\mathbb{P}(\lfloor S_n \rfloor = j) = F_n(j+1) - F_n(j) = \int_j^{j+1} f_n(y)\,\mathrm{d}y = f_{n+1}(j+1) = \frac{1}{n!}\sum_{i=0}^{n+1}(-1)^i\binom{n+1}{i}(j+1-i)^n,$$

où on reconnaît l'expression de $a_{n,j} = \mathbb{P}(r(\Sigma) = j+1)$ calculée en 2.3.3. □

Corollaire 2.3.6. $\frac{r(\Sigma) - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \overset{loi}{\longrightarrow} \mathscr{N}(0,1)$.

Démonstration.
Le théorème central limite donne $\frac{S_n - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \overset{\text{loi}}{\longrightarrow} \mathscr{N}(0,1)$, d'où également $\frac{1 + S_n - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \overset{\text{loi}}{\longrightarrow} \mathscr{N}(0,1)$ par le lemme de Slutsky. D'autre part, comme $r(\Sigma) \overset{\text{loi}}{=} 1 + \lfloor S_n \rfloor$, on a pour tout $x \in \mathbb{R}$:

$$\mathbb{P}\left(\frac{1 + S_n - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \le x\right) \le \mathbb{P}\left(\frac{r(\Sigma) - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \le x\right) \le \mathbb{P}\left(\frac{S_n - \frac{n}{2}}{\sqrt{\frac{n}{12}}} \le x\right).$$

La caractérisation de la convergence en loi par les fonctions de répartition conclut, puisque les membres aux extrémités convergent vers $\Phi(x)$ où Φ désigne la fonction de répartition de la loi $\mathscr{N}(0,1)$. □

2.3.2 Théorème de Bayer-Diaconis

Rappelons que pour tout $\varepsilon > 0$: $\log_2(n) \lesssim t_{mix}^{(n)}(\varepsilon) \lesssim 2\log_2(n)$. Il est donc naturel de chercher un équivalent du temps de mélange en $\alpha\log_2(n)$, avec $\alpha \in [1,2]$. Nous commençons par un calcul déterministe, celui de la loi de S_t lorsque $t \sim \alpha\log_2(n)$, qui fait l'objet de la proposition suivante.

Remarque. Nous prolongeons ici $t \mapsto \mathscr{D}_n(t)$ à une fonction continue sur $\mathbb{R}_+$ de la manière suivante. Pour tout $\sigma \in \mathfrak{S}_n$ et tout $t \in \mathbb{N}$, on a $P^t(\mathrm{Id}, \sigma) = \frac{(2^t - r(\sigma)+1)(2^t - r(\sigma)+2)\cdots(2^t - r(\sigma)+n)}{n!\,2^{tn}}$ d'après 1.3.1. Cette formule ayant également un sens pour $t \notin \mathbb{N}$, on définit $P^t(\mathrm{Id}, \sigma)$ pour tout $t \in \mathbb{R}_+$ par la même formule, ce qui permet de définir également $\mathscr{D}_n(t) := \sum_{\sigma\in\mathfrak{S}_n}(\frac{1}{n!} - P^t(\mathrm{Id},\sigma))_+ = \mathbb{E}((1 - n!P^t(\mathrm{Id},\Sigma))_+)$ pour tout $t \in \mathbb{R}_+$.

Notation. On note $\tilde{t}_{mix}^{(n)}(\varepsilon) := \inf\{t \in \mathbb{R}_+ \mid \mathscr{D}_n(t) \le \varepsilon\} \in\ ]t_{mix}^{(n)}(\varepsilon) - 1, t_{mix}^{(n)}(\varepsilon)]$.

Proposition 2.3.7. *On pose $t = \log_2(cn^\alpha)$, où $\alpha \in [1,2]$ et $c > 0$ sont fixés. Soit $\sigma \in \mathfrak{S}_n$ possédant $r = \frac{n}{2} + h$ suites croissantes, où $-\frac{n}{2} + 1 \leq h \leq \frac{n}{2}$. Alors :*

$$n!P^t(\mathrm{Id}, \sigma) = \exp\left(- \frac{h}{cn^{\alpha-1}} - \frac{1}{24c^2n^{2\alpha-3}} + \frac{1}{2cn^{\alpha-1}} - \frac{h^2}{2c^2n^{2\alpha-1}} + O(n^{4-3\alpha}) \right) ,$$

où la constante du $O(n^{4-3\alpha})$ ne dépend pas de h.

Démonstration.

$$n!P^t(\mathrm{Id}, \sigma) = \frac{(2^t - r + 1)(2^t - r + 2) \cdots (2^t - r + n)}{(2^t)^n} = \prod_{i=1}^{n} \left(1 + \frac{i - r}{2^t} \right) ,$$

d'où après le changement d'indice $i \leftrightarrow n - i$ et en posant $x_i := \dfrac{n - r - i}{2^t} = \dfrac{\frac{n}{2} - h - i}{cn^\alpha}$:

$$n!P^t(\mathrm{Id}, \sigma) = \prod_{i=0}^{n-1} (1 + x_i) = \exp\left(\sum_{i=0}^{n-1} \ln(1 + x_i) \right) .$$

Pour tout i : $\ln(1+x_i) = x_i - \frac{x_i^2}{2} + O(n^{3-3\alpha})$. Comme la constante de ce $O(n^{3-3\alpha})$ ne dépend pas de i, on en déduit par sommation que : $\displaystyle\sum_{i=0}^{n-1} \ln(1+x_i) = \frac{1}{cn^\alpha} \sum_{i=0}^{n-1} \left(\frac{n}{2} - h - i \right) - \frac{1}{2c^2n^{2\alpha}} \sum_{i=0}^{n-1} \left(\frac{n}{2} - h - i \right)^2 + O(n^{4-3\alpha})$.

- $\displaystyle\sum_{i=0}^{n-1} \left(\frac{n}{2} - h - i \right) = n\left(\frac{n}{2} - h \right) - \frac{n(n-1)}{2} = n\left(-h + \frac{1}{2} \right)$.
- $$\begin{aligned} \sum_{i=0}^{n-1} \left(\frac{n}{2} - h - i \right)^2 &= n\left(\frac{n}{2} - h \right)^2 - 2\left(\frac{n}{2} - h \right) \frac{n(n-1)}{2} + \frac{n(n-1)(2n-1)}{6} \\ &= \left(\frac{1}{4} - \frac{1}{2} + \frac{1}{3} \right) n^3 + \left(-h + h + \frac{1}{2} - \frac{1}{6} - \frac{1}{3} \right) n^2 + \left(h^2 - h + \frac{1}{6} \right) n \\ &= \frac{n^3}{12} + nh^2 + O(n^2) , \end{aligned}$$

  où la constante du $O(n^2)$ ne dépend pas de h.

On obtient finalement $\displaystyle\sum_{i=0}^{n-1} \ln(1 + x_i) = - \frac{h + \frac{1}{2}}{cn^{\alpha-1}} - \frac{1}{24c^2n^{2\alpha-3}} - \frac{h^2}{2c^2n^{2\alpha-1}} + O(n^{2-2\alpha}) + O(n^{4-3\alpha})$,
ce qui conclut puisque $2 - 2\alpha \leq 4 - 3\alpha$. □

Posons $h(\sigma) := r(\sigma) - \frac{n}{2}$. Heuristiquement, $h(\Sigma)$ est de l'ordre de $\sqrt{n}$ d'après 2.3.6, donc la formule précédente semble indiquer que le changement de régime survient en $\alpha = \frac{3}{2}$. Ceci se vérifie aisément :

Corollaire 2.3.8. *Pour $\alpha = \frac{3}{2}$, on a $n!P^t(\mathrm{Id}, \Sigma) \xrightarrow{loi} \exp\left(-\frac{Z}{\sqrt{12}c} - \frac{1}{24c^2} \right)$, où $Z \sim \mathscr{N}(0,1)$.*

Démonstration.
On sait d'après 2.3.6 que $\dfrac{h(\Sigma)}{\sqrt{\frac{n}{12}}} \xrightarrow{\text{loi}} Z$, d'où par la proposition précédente :

$$n!P^t(\mathrm{Id}, \Sigma) = \exp\left(- \frac{1}{\sqrt{12}c} \underbrace{\frac{h(\Sigma)}{\sqrt{\frac{n}{12}}}}_{\xrightarrow{\text{loi}} Z} - \frac{1}{24c^2} - \frac{1}{24c^2n} \underbrace{\left(\frac{h(\Sigma)}{\sqrt{\frac{n}{12}}} \right)^2}_{\xrightarrow{\text{loi}} Z^2} + O(n^{-\frac{1}{2}}) \right) .$$

Le lemme de Slutsky conclut. □

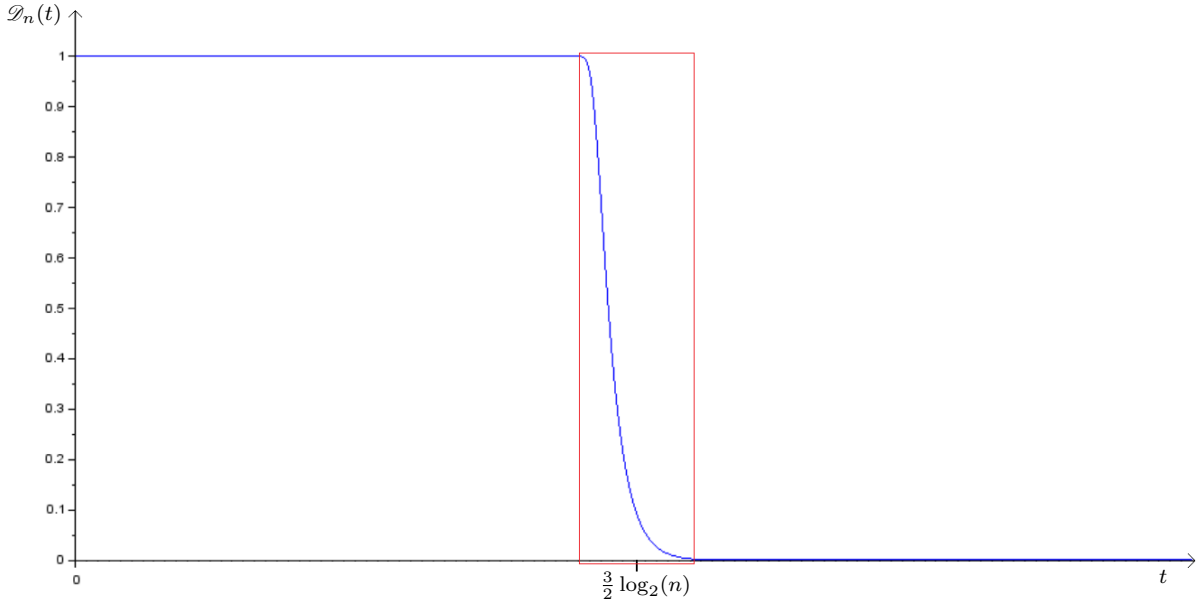
Théorème 2.3.9. *Pour tout $\theta \in \mathbb{R}$: $\mathscr{D}_n(\frac{3}{2}\log_2(n)+\theta) \xrightarrow[n\to\infty]{} \varphi(\theta) := 1-2\Phi\left(\frac{-1}{4.2^\theta\sqrt{3}}\right)$, où Φ est la fonction de répartition de la loi $\mathcal{N}(0,1)$. Autrement dit, pour tout $\varepsilon > 0$: $t_{mix}^{(n)}(\varepsilon) = \frac{3}{2}\log_2(n) + \varphi^{-1}(\varepsilon) + o(1)$. En particulier, pour tout $\varepsilon > 0$, on a $t_{mix}^{(n)}(\varepsilon) \sim \frac{3}{2}\log_2(n)$: il y a cutoff pour le riffle shuffle.*

Démonstration.
On pose $c = 2^\theta$, et $t = \log_2(cn^{\frac{3}{2}}) = \frac{3}{2}\log_2(n) + \theta$. La variable aléatoire $(1 - n!P^t(\mathrm{Id}, \Sigma))_+$ est bornée, donc d'après 2.3.8 : $\mathscr{D}_n(t) = \mathbb{E}((1 - n!P^t(\mathrm{Id}, \Sigma))_+) \xrightarrow[n\to\infty]{} \mathbb{E}\left(\left(1 - \exp\left(-\frac{Z}{\sqrt{12}c} - \frac{1}{24c^2}\right)\right)_+\right)$.
Il reste à calculer cette espérance. Comme $\exp\left(-\frac{z}{\sqrt{12}c} - \frac{1}{24c^2}\right) \leq 1$ si et seulement si $z \geq \frac{-1}{4c\sqrt{3}}$, on a :

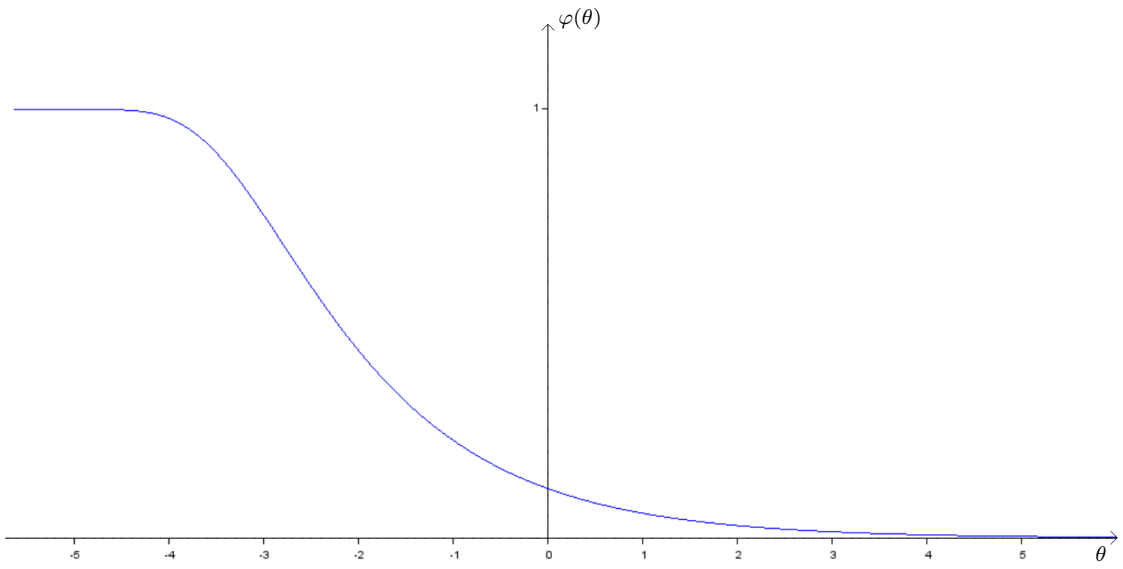
$$\begin{aligned}
\mathbb{E}\left(\left(1 - \exp\left(-\frac{Z}{\sqrt{12}c} - \frac{1}{24c^2}\right)\right)_+\right) &= \mathbb{E}\left(\left(1 - \exp\left(-\frac{Z}{\sqrt{12}c} - \frac{1}{24c^2}\right)\right)\mathbf{1}_{Z\geq\frac{-1}{4c\sqrt{3}}}\right) \\
&= \int_{\frac{-1}{4c\sqrt{3}}}^{+\infty}\left(1 - e^{-\frac{z}{\sqrt{12}c}-\frac{1}{24c^2}}\right)\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}\,\mathrm{d}z \\
&= \left(1 - \Phi\left(\frac{-1}{4c\sqrt{3}}\right)\right) - \int_{\frac{-1}{4c\sqrt{3}}}^{+\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}-\frac{z}{\sqrt{12}c}-\frac{1}{24c^2}}\,\mathrm{d}z \\
&= 1 - \Phi\left(\frac{-1}{4c\sqrt{3}}\right) - \int_{\frac{-1}{4c\sqrt{3}}}^{+\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{\left(z+\frac{1}{\sqrt{12}c}\right)^2}{2}}\,\mathrm{d}z \\
&= 1 - \Phi\left(\frac{-1}{4c\sqrt{3}}\right) - \int_{\frac{1}{4c\sqrt{3}}}^{+\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}\,\mathrm{d}x \\
&= 1 - \Phi\left(\frac{-1}{4c\sqrt{3}}\right) - \left(1 - \Phi\left(\frac{1}{4c\sqrt{3}}\right)\right) \\
&= 1 - 2\Phi\left(\frac{-1}{4c\sqrt{3}}\right).
\end{aligned}$$

□

Le phénomène de cutoff signifie que, pour n grand, l'allure de $t \mapsto \mathscr{D}_n(t)$ est comme suit, avec une descente brutale de 1 à 0 autour de $\frac{3}{2}\log_2(n)$:



Le théorème montre même que cette descente se fait sur un intervalle dont la largeur est d'ordre 1, et qu'un zoom sur cette fenêtre (en rouge ci-dessus) fait apparaître la fonction φ :



3 Sur une conjecture de Bayer-Diaconis-McGrath

3.1 Présentation du problème

Nous considérons le jeu suivant. Un deck de n cartes est mélangé suivant un a-shuffle. Le joueur fait une proposition pour deviner la première carte en partant du haut. Celle-ci est ensuite révélée (*feedback*), puis le joueur fait une proposition pour deviner la deuxième carte, qui est révélée à son tour etc. Quelle est la stratégie qui permet au joueur de deviner correctement le maximum de cartes en moyenne ? Etant donné que le joueur peut proposer une même carte autant de fois qu'il le souhaite, il s'agit de faire le choix optimal pour chacune des n propositions indépendamment. Il faut donc déterminer, pour tout m, quelle est la carte la plus probable en $(m+1)$-ème position du deck mélangé sachant les m premières cartes.

Dans [BD], les auteurs conjecturent que la meilleure carte à proposer est la première carte (i.e. la plus petite) d'une suite maximale de cartes consécutives parmi les cartes qui n'ont pas encore été révélées. Nous appellerons cela la conjecture/stratégie BDM (Bayer-Diaconis-McGrath).

Exemple. Supposons $n = 8$. Si la première carte est le 6 et la deuxième carte est le 2, alors cette stratégie préconise de proposer la carte 3, car la plus longue suite restante de cartes consécutives est $\{3, 4, 5\}$:

(les cartes déjà révélées seront toujours représentées barrées d'une croix)

L'intuition derrière la stratégie BDM est assez simple. Plutôt qu'un deck déjà mélangé au début du jeu, imaginons plutôt un croupier qui suit la description multinomiale pour effectuer un a-shuffle *au fur et à mesure* du jeu : le croupier découpe le deck en a paquets multinomiaux, le joueur devine la première carte, le croupier tire la première carte (i.e. choisit un paquet avec probabilité proportionnelle à sa taille et prend la carte en haut de ce paquet) et la révèle au joueur, celui-ci devine la deuxième carte, le croupier tire la deuxième carte etc. Le joueur est dos au croupier tout au long du jeu, et ne connaît donc pas l'état des paquets. Il est tenté, à chaque étape du jeu, de proposer une carte qui est en haut de son paquet à ce stade, puisque les autres cartes ne peuvent pas être tirées par le croupier. Or les seules cartes dont le joueur est certain qu'elles soient en haut de leurs paquets respectifs sont celles qui sont en tête d'une série de cartes consécutives restantes : en effet, une telle carte est soit le 1 (qui est évidemment en haut de son paquet) soit une carte j telle que $j-1$ a déjà été tirée (et qui était donc soit en haut de son paquet depuis le début, soit juste en-dessous de $j-1$ au début et en haut de son paquet depuis que $j-1$ a été tirée). Enfin, parmi ces options supposées intéressantes, il peut paraître logique de sélectionner une suite de longueur maximale : on imagine que sa première carte se situera en moyenne dans un paquet d'autant plus gros, et donc d'autant plus probable.

Nous montrons que la meilleure carte à proposer est bien l'une de celles qui sont en tête d'une suite de cartes consécutives restantes, mais qu'en général le choix d'une suite de taille maximale n'est pas optimal.

3.2 Notations utilisées

Nous utiliserons ici la description uniforme : on se donne donc (P, S) de loi uniforme sur $\mathscr{C}_a(n)$.

Notation. Soit $\mathbf{i} = (i_1, \dots, i_m)$ le vecteur indiquant les m premières cartes successivement révélées au joueur.

Notation. On note $\mathscr{C}_a^{\mathbf{i}}(n)$ l'ensemble des $(p, \sigma) \in \mathscr{C}_a(n)$ tels que $\sigma(1) = i_1, \dots, \sigma(m) = i_m$, et on note $\mathscr{P}_a^{\mathbf{i}}(n)$ l'ensemble des $p \in \mathscr{P}_a(n)$ tels qu'il existe $\sigma \in \mathfrak{S}_n$ telle que $(p, \sigma) \in \mathscr{C}_a^{\mathbf{i}}(n)$.

Notation. On note $\mathbb{P}_{\mathbf{i}} := \mathbb{P}(\,\cdot \mid S(1) = i_1, \dots, S(m) = i_m)$, $\mathbb{E}_{\mathbf{i}}$ l'espérance correspondante, et $\mathscr{L}_{\mathbf{i}}(X)$ la loi d'une variable aléatoire X sous $\mathbb{P}_{\mathbf{i}}$: ainsi, $\mathscr{L}_{\mathbf{i}}((P, S)) = \mathrm{Unif}(\mathscr{C}_a^{\mathbf{i}}(n))$. Remarquons que si $m = 0$ on retrouve simplement $\mathbb{P}$.

Le but est donc d'identifier la carte i_{m+1} qui maximise $\mathbb{P}_{\mathbf{i}}(S(m+1) = i_{m+1})$.

Notation. On note $\pi = (\pi_1, \dots, \pi_q)$ la partition ordonnée de $\{1, \dots, n\} \setminus \{i_1, \dots, i_m\}$ décrivant les suites de cartes consécutives restantes dans le deck. On note $r_k := \#\pi_k$.

Exemple. Dans l'exemple précédent, on a $n = 8$, $\mathbf{i} = (6, 2)$, $\pi_1 = \{1\}$, $\pi_2 = \{3, 4, 5\}$, $\pi_3 = \{7, 8\}$.

Définition. Une coupe est dite *obligatoire* lorsque P contient une coupe à cet emplacement $\mathbb{P}_{\mathbf{i}}-$p.s. Si P contient plusieurs coupes à un emplacement obligatoire, **seule l'une d'elle est considérée comme obligatoire**.

Remarque. Ainsi, $\mathscr{P}_a^{\mathbf{i}}(n)$ est l'ensemble des $p \in \mathscr{P}_a(n)$ contenant les coupes obligatoires.

Exemple. Si $\mathbf{i} = (6, 1, 5)$, les coupes obligatoires sont aux emplacements 5 et 4 : en effet on a nécessairement une coupe entre 5 et 6 puisque le 6 est venu avant le 5, et on a nécessairement une coupe entre 4 et 5 puisque le 5 est venu avant le 4.

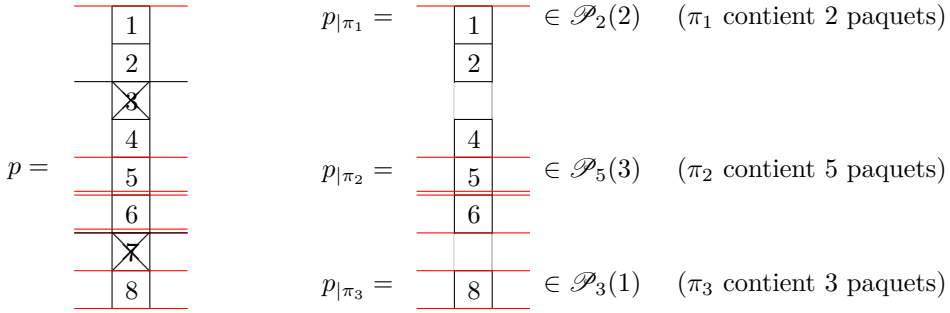
Définition. Si $p \in \mathscr{P}_a^{\mathbf{i}}(n)$, on dit qu'une coupe est *dans* π_k lorsqu'elle est adjacente à π_k et **non obligatoire**. Si $\pi_k = \{j, j+1, \dots, j+r_k-1\}$, les coupes qui sont dans π_k sont donc celles qui sont aux emplacements $j-1, j, \dots, j+r_k-1$ sauf la coupe obligatoire à l'emplacement $j+r_k-1$ s'il y en a une. En notant $b-1$ le nombre de coupes qui sont dans π_k, on dit que π_k *contient* b paquets.

Notation. Si $p \in \mathscr{P}_a^{\mathbf{i}}(n)$, on note $p_{|\pi_k}$ la restriction de p à π_k, i.e. l'élément de $\mathscr{P}_b(r_k)$ obtenu à partir de p en ne gardant que π_k et les $b-1$ coupes qui sont dans π_k. Les coupes qui ne sont pas dans π_k (k fixé) seront notées $p \setminus \pi_k$, et les coupes qui ne sont dans aucun des π_k seront notées $p \setminus \pi$.

Notation. Si $(p,\sigma) \in \mathscr{C}_a^{\mathbf{i}}(n)$, on note $\sigma_{\pi_k} \in \mathfrak{S}_{r_k}$ l'ordre relatif dans σ des éléments de π_k (numérotés de 1 à r_k dans l'ordre croissant).

Définition. Si $p \in \mathscr{P}_a^{\mathbf{i}}(n)$, on dit que $\tau \in \mathfrak{S}_{r_k}$ est *p-compatible pour* π_k lorsque τ est un ordre relatif possible pour p des cartes de π_k.

Exemple. Supposons $n = 8$, $a = 9$, $\mathbf{i} = (3,7)$, d'où $\pi_1 = \{1,2\}$, $\pi_2 = \{4,5,6\}$, $\pi_3 = \{8\}$. Soit p définie comme suit, où les deux coupes obligatoires apparaissent en noir :



La seule permutation p-compatible pour π_1 est 1 2. Tous les ordres relatifs des cartes 4,5,6 sont possibles, donc les permutations p-compatibles pour π_2 sont 1 2 3, 1 3 2, 2 1 3, 2 3 1, 3 1 2, 3 2 1.
Soit par exemple $\sigma = 3\ 7\ 6\ 1\ 4\ 5\ 2\ 8$, on a bien $(p,\sigma) \in \mathscr{C}_9^{\mathbf{i}}(8)$. Les cartes de π_1 apparaissent dans l'ordre "1 2" donc $\sigma_{\pi_1} = 1\ 2$. Les cartes de π_2 apparaissent dans l'ordre "6 4 5" donc $\sigma_{\pi_2} = 3\ 1\ 2$.

3.3 Condition nécessaire pour une stratégie optimale

Nous montrons qu'à chaque étape du jeu, la meilleure carte à proposer est l'une de celles qui sont en tête d'une suite de cartes consécutives restantes. Commençons par vérifier ceci pour $m = 0$:

Proposition 3.3.1. *La carte 1 est la proposition optimale pour la toute première carte du deck ; elle est même strictement optimale. Autrement dit,* $\forall\, j \in \{2,\dots,n\} : \mathbb{P}(S(1) = 1) > \mathbb{P}(S(1) = j)$.

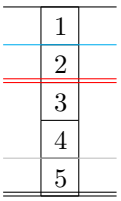
Démonstration.
Nous avons obtenu des formules explicites en 1.2.7 mais celles-ci sont difficiles à exploiter. Il existe cependant une preuve particulièrement simple. Les seuls découpages $p \in \mathscr{P}_a(n)$ qui peuvent engendrer un entrelacement commençant par j sont ceux qui possèdent une coupe à l'emplacement $j-1 \in \{1,\dots,n-1\}$.
Posons $\begin{cases} X & := \{p \in \mathscr{P}_a(n) \mid p \text{ contient au moins une coupe à l'emplacement } j-1\} \\ Y & := \{p \in \mathscr{P}_a(n) \mid p \text{ contient au moins une coupe à l'emplacement } n-j+1\} \end{cases}$ et $f : X \to Y$
où $f(p)$ est défini comme suit, avec $p[e]$ (resp. $f(p)[e]$) le nombre de coupes à l'emplacement e dans p (resp. dans $f(p)$) :

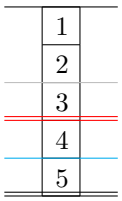
- $f(p)[0] = p[0]$;
- pour tout $e \in \{1,\dots,n-j\}$: $f(p)[e] = p[e+j-1]$;
- $f(p)[n-j+1] = p[j-1]$;

- pour tout $e \in \{n-j+2, \dots, n-1\}$: $f(p)[e] = p[e+j-n-1]$;
- $f(p)[n] = p[n]$.

Il est clair que f est bijective. De plus, $f(p)$ a la même structure en paquets que p (i.e. p et $f(p)$ ont autant de paquets de chaque taille), et le paquet contenant j dans p est de même taille que le paquet contenant 1 dans $f(p)$: on en conclut que $f(p)$ engendre exactement autant d'entrelacements commençant par 1 que p n'engendre d'entrelacements commençant par j. Ceci établit l'inégalité large. Remarquons enfin que $Y \neq \mathscr{P}_a(n)$, d'où l'inégalité stricte puisque pour tout $p \in \mathscr{P}_a(n)$ il existe au moins un entrelacement p-compatible commençant par 1. □

Exemple. Voici une illustration de la bijection f pour $n = 5$, $a = 8$, $j = 3$:

$p =$ 

$f(p) =$ 

La proposition suivante va nous permettre, quel que soit m, de toujours nous ramener au cas $m = 0$ que nous venons de traiter.

Proposition 3.3.2. *Soient $k \in \{1, \dots, q\}$ fixé, et p_0 une famille d'entiers entre 0 et n représentant les emplacements des coupes qui sont en-dehors de π_k. On note c le cardinal de p_0, $b := a - c$ et $A := \{P \setminus \pi_k = p_0\}$. Alors, sous $\mathbb{P}_{\mathbf{i}}$ et sachant A, $(P_{|\pi_k}, S_{\pi_k})$ suit la loi uniforme sur $\mathscr{C}_b(r_k)$. En particulier, sous $\mathbb{P}_{\mathbf{i}}$ et sachant A, S_{π_k} a la loi d'un b-shuffle.*

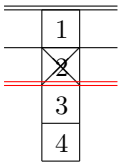
Démonstration.
Posons $E := \{(p, \sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid p \setminus \pi_k = p_0\}$ et $F := \mathscr{C}_b(r_k)$. On sait que $\mathscr{L}_{\mathbf{i}}((P,S)|A) = \mathrm{Unif}(E)$, et on veut montrer que $\mathscr{L}_{\mathbf{i}}((P_{|\pi_k}, S_{\pi_k})|A) = \mathrm{Unif}(F)$. En posant $f : \left| \begin{array}{ccc} E & \longrightarrow & F \\ (p,\sigma) & \longmapsto & (p_{|\pi_k}, \sigma_{\pi_k}) \end{array} \right.$, il suffit donc de montrer que tout les éléments de F ont le même nombre d'antécédents par f.
Soit $(p', \sigma') \in F$. Pour un antécédent (p, σ), le choix de p est unique car forcé par p' et p_0. Il reste donc à montrer que, pour ce p, le cardinal de $T := \{\sigma \mid f(p,\sigma) = (p', \sigma')\}$ ne dépend pas de (p', σ'). Or, il est facile de voir que

$$T = \bigsqcup_{\substack{\tau_l,\, l \neq k \\ \tau_l \, p-\text{compatible pour } \pi_l}} \{\sigma \in \mathfrak{S}_n \,|\, \sigma(1) = i_1, \dots, \sigma(m) = i_m \,,\, \sigma_{\pi_l} = \tau_l \ \forall\, l \neq k \,,\, \sigma_{\pi_k} = \sigma'\} \ , \text{ d'où}$$

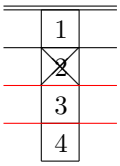
$$\#T = \sum_{\substack{\tau_l,\, l \neq k \\ \tau_l \, p-\text{compatible pour } \pi_l}} \binom{n-m}{r_1, \dots, r_q} = \#\{(\tau_l)_{l \neq k} \mid \tau_l \ p-\text{compatible pour } \pi_l \ \forall\, l\} \binom{n-m}{r_1, \dots, r_q} .$$

Si $l \neq k$, la p-compatibilité de τ_l pour π_l ne dépend que de p_0, ainsi $\#T$ ne dépend pas de (p', σ'). □

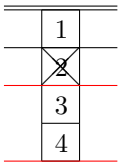
Exemple. Voici une illustration pour $n = 4$, $a = 6$, $\mathbf{i} = (2)$ ($\pi_1 = \{1\}$, $\pi_2 = \{3,4\}$), $k = 2$, $p_0 = (0,0,1)$ ($b = 3$). Ecrivons la liste des éléments de $\mathscr{C}_6^{(2)}(4)$ qui sont tels que les coupes en-dehors de $\{3,4\}$, représentées en noir, soient aux emplacements $(0,0,1)$:



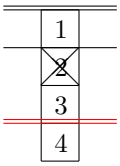
2 1 3 4
2 3 1 4
2 3 4 1



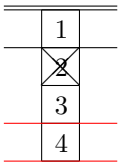
2 1 3 4
2 1 4 3
2 3 1 4
2 3 4 1
2 4 1 3
2 4 3 1



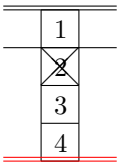
2 1 3 4
2 3 1 4
2 3 4 1



2 1 3 4
2 1 4 3
2 3 1 4
2 3 4 1
2 4 1 3
2 4 3 1



2 1 3 4
2 1 4 3
2 3 1 4
2 3 4 1
2 4 1 3
2 4 3 1



2 1 3 4
2 3 1 4
2 3 4 1

On compte 18 occurrences de "3 4" et 9 occurrences de "4 3", ainsi $\mathbb{P}_{\mathbf{i}}(S_{\{3,4\}} = 1\ 2 \,|\, A) = \frac{18}{27} = \frac{2}{3}$ et $\mathbb{P}_{\mathbf{i}}(S_{\{3,4\}} = 2\ 1 \,|\, A) = \frac{9}{27} = \frac{1}{3}$. On vérifie aisément qu'il s'agit bien de la loi d'un 3-shuffle sur 2 cartes. Dans la preuve du théorème, on a ici $\#T = 3$.

Ainsi, quitte à fixer les coupes qui sont hors de π_k, S_{π_k} se comporte sous $\mathbb{P}_{\mathbf{i}}$ comme un riffle shuffle : on devrait donc réussir à montrer grâce à 3.3.1 que, parmi les cartes de π_k, c'est bien la première qui a tendance à arriver avant les autres. Cependant, on ne veut pas seulement qu'elle arrive plus souvent **avant les autres** : on veut qu'elle arrive plus souvent **tout de suite**, c'est-à-dire en $(m+1)$-ième position. La proposition suivante règle ce problème : l'ordre relatif des cartes de π_k est indépendant du fait que la $(m+1)$-ième carte soit dans π_k ou pas.

Proposition 3.3.3. *Soit $k \in \{1, \dots, q\}$ fixé. Alors, sous $\mathbb{P}_{\mathbf{i}}$, S_{π_k} et $\mathbf{1}_{\{S(m+1)\in\pi_k\}}$ sont indépendantes.*

Démonstration.
Soit $\tau \in \mathfrak{S}_{r_k}$, on veut montrer que $\mathbb{P}_{\mathbf{i}}(S_{\pi_k} = \tau) = \mathbb{P}_{\mathbf{i}}(S_{\pi_k} = \tau \mid S(m+1) \in \pi_k)$.

- Comme $\mathscr{L}_{\mathbf{i}}((P,S)) = \mathrm{Unif}(\mathscr{C}_a^{\mathbf{i}}(n))$, on a $\mathbb{P}_{\mathbf{i}}(S_{\pi_k} = \tau) = \dfrac{\#\{(p,\sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid \sigma_{\pi_k} = \tau\}}{\#\mathscr{C}_a^{\mathbf{i}}(n)}$.
  Pour $p \in \mathscr{P}_a^{\mathbf{i}}(n)$, notons $c_p(l)$ le nombre de $\tau_l \in \mathfrak{S}_{r_l}$ qui sont p-compatibles pour π_l, alors

  $$\#\mathscr{C}_a^{\mathbf{i}}(n) = \sum_{p \in \mathscr{P}_a^{\mathbf{i}}(n)} \left(\prod_l c_p(l)\right) \binom{n-m}{r_1, \dots, r_q},$$

  en effet : on choisit d'abord p, puis on choisit l'ordre relatif des cartes de chaque π_l ($c_p(l)$ choix pour chaque l) ainsi que leurs emplacements. De même :

  $$\#\{(p,\sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid \sigma_{\pi_k} = \tau\} = \sum_{p \in \mathscr{P}_a^{\mathbf{i}}(n)} \left(\prod_{l \neq k} c_p(l)\right) \binom{n-m}{r_1, \dots, r_q} \mathbf{1}_{\{\tau \text{ est } p\text{-compatible pour } \pi_k\}},$$

  en effet : on choisit d'abord p tel que τ soit p-compatible pour π_k, puis on choisit l'ordre relatif des cartes de chaque π_l (sauf π_k dont l'ordre est forcé) ainsi que leurs emplacements.
- On a $\mathbb{P}_{\mathbf{i}}(S_{\pi_k} = \tau \mid S(m+1) \in \pi_k) = \dfrac{\#\{(p,\sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid \sigma_{\pi_k} = \tau\ ,\ \sigma(m+1) \in \pi_k\}}{\#\{(p,\sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid \sigma(m+1) \in \pi_k\}}$.
  Par le même raisonnement que précédemment, à la seule différence que que l'une des cartes de π_k

est placée de force en $(m+1)$-ième position, le dénominateur est égal à

$$\sum_{p\in\mathscr{P}_a^{\mathbf{i}}(n)}\left(\prod_l c_p(l)\right)\binom{n-m-1}{r_1,\,\ldots\,,r_{k-1},r_k-1,r_{k+1},\,\ldots\,,r_q}$$

tandis que le numérateur est égal à

$$\sum_{p\in\mathscr{P}_a^{\mathbf{i}}(n)}\left(\prod_{l\neq k} c_p(l)\right)\binom{n-m-1}{r_1,\,\ldots\,,r_{k-1},r_k-1,r_{k+1},\,\ldots\,,r_q}\mathbf{1}_{\{\tau \text{ est } p\text{-compatible pour } \pi_k\}}\ .$$

- En conclusion :
$\mathbb{P}_{\mathbf{i}}(S_{\pi_k}=\tau)=\dfrac{\sum_{p\in\mathscr{P}_a^{\mathbf{i}}(n)}\left(\prod_{l\neq k} c_p(l)\right)\mathbf{1}_{\{\tau \text{ est } p\text{-compatible pour } \pi_k\}}}{\sum_{p\in\mathscr{P}_a^{\mathbf{i}}(n)}\left(\prod_l c_p(l)\right)}=\mathbb{P}_{\mathbf{i}}(S_{\pi_k}=\tau\mid S(m+1)\in\pi_k).$

□

Théorème 3.3.4. *Soit $k\in\{1,\ldots,q\}$ fixé. Alors la carte en tête de π_k est une proposition strictement meilleure que n'importe quelle autre carte de π_k. Autrement dit, en notant $j_1<\cdots<j_{r_k}$ les éléments de π_k, on a $\forall\ s\in\{2,\ldots,r_k\}$: $\mathbb{P}_{\mathbf{i}}(S(m+1)=j_1)>\mathbb{P}_{\mathbf{i}}(S(m+1)=j_s)$.*

Démonstration.
Commençons par remarquer que

$$\mathbb{P}_{\mathbf{i}}(S(m+1)=j_1)=\mathbb{P}_{\mathbf{i}}(S(m+1)\in\pi_k\,,\,S_{\pi_k}(1)=1)=\mathbb{P}_{\mathbf{i}}(S(m+1)\in\pi_k)\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1)\ ,$$

où la deuxième égalité vient de 3.3.3. De même : $\mathbb{P}_{\mathbf{i}}(S(m+1)=j_s)=\mathbb{P}_{\mathbf{i}}(S(m+1)\in\pi_k)\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=s)$. Ainsi, il suffit de montrer que $\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1)>\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=s)$. En écrivant

$$\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1)=\sum_{p_0}\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1\mid P\setminus\pi_k=p_0)\,\mathbb{P}_{\mathbf{i}}(P\setminus\pi_k=p_0)\ ,$$

où $\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1\mid P\setminus\pi_k=p_0)>\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=s\mid P\setminus\pi_k=p_0)$ pour tout p_0 d'après une utilisation conjointe de 3.3.2 et de 3.3.1, on peut conclure que

$$\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=1)>\sum_{p_0}\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=s\mid P\setminus\pi_k=p_0)\,\mathbb{P}_{\mathbf{i}}(P\setminus\pi_k=p_0)=\mathbb{P}_{\mathbf{i}}(S_{\pi_k}(1)=s)\ .$$

□

Corollaire 3.3.5. *Pour $a=2$, la stratégie BDM est optimale.*

Démonstration.
On propose en premier la carte 1, que l'on sait optimale par 3.3.1. Tant que toutes les propositions sont correctes, on propose ensuite les cartes 2, puis 3, puis 4 etc., qui sont optimales d'après 3.3.4. A la première erreur, si on tombe sur la carte j alors qu'on en avait proposé une autre, cela signifie qu'il y a une coupe en position $j-1$: comme $a=2$, cette coupe est unique, on connaît alors l'état exact des deux paquets jusqu'à la fin du jeu. La meilleure carte à proposer à chaque instant est celle qui est en haut du plus gros paquet, et c'est bien celle-ci que la stratégie BDM préconise. □

Cependant, nous allons désormais voir que la stratégie BDM n'est pas optimale en général pour les autres valeurs de a.

3.4 Réfutation de la conjecture BDM

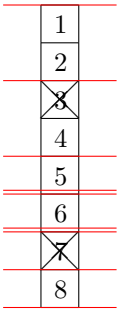
Dans cette partie, nous montrons le résultat suivant :

Théorème. *Pour $a \in \{3,4\}$, et quel que soit $n \geq 13$, la stratégie BDM n'est pas optimale.*

Notation. Pour $p \in \mathscr{P}_a^{\mathbf{i}}(n)$ et $j \notin \{i_1, \dots, i_m\}$, on note $h_p(j)$ la taille du paquet contenant la carte j une fois les m premières cartes tirées (en voyant le mélange comme étant effectué au fur et à mesure du jeu, via la description multinomiale comme expliqué au début de cette section).

Exemple. Supposons $n = 8$, $a = 9$, $\mathbf{i} = (3, 7)$, et p définie comme suit :

$p =$



Au départ, le paquet contenant la carte 4 est $\{3, 4\}$. Cependant, une fois les cartes 3 et 7 tirées, ce paquet est réduit à $\{4\}$: on a donc ici $h_p(4) = 1$.

Notation. On note désormais j_k la première (i.e. la plus petite) carte de π_k.

Proposition 3.4.1. *Pour tout $k \in \{1, \dots, q\}$:* $\mathbb{P}_{\mathbf{i}}(S(m+1) = j_k) = \dfrac{\mathbb{E}_{\mathbf{i}}(h_P(j_k))}{n-m}$.

Démonstration.
On écrit $\mathbb{P}_{\mathbf{i}}(S(m+1) = j_k) = \sum_s \mathbb{P}_{\mathbf{i}}(S(m+1) = j_k \mid h_P(j_k) = s)\mathbb{P}_{\mathbf{i}}(h_P(j_k) = s)$.
Sachant que le paquet contenant j_k est de taille s à ce stade du jeu, la carte en tête de ce paquet (i.e. j_k) est choisie avec probabilité $\frac{s}{n-m}$, d'où $\mathbb{P}_{\mathbf{i}}(S(m+1) = j_k) = \sum_s \dfrac{s}{n-m}\,\mathbb{P}_{\mathbf{i}}(h_P(j_k) = s) = \dfrac{\mathbb{E}_{\mathbf{i}}(h_P(j_k))}{n-m}$. □

Pour montrer que la stratégie BDM n'est pas optimale, nous allons donc tâcher d'exhiber un cas où il existe $k \neq l$ tels qu'on ait à la fois $r_k > r_l$ et $\mathbb{E}_{\mathbf{i}}(h_P(j_k)) < \mathbb{E}_{\mathbf{i}}(h_P(j_l))$. Nous allons utiliser un système complet d'évènements sur lesquels ces espérances sont faciles à calculer : c'est l'objectif des quelques résultats qui suivent.

Proposition 3.4.2. *Soient $k \in \{1, \dots, q\}$ fixé, et p_0 une famille d'entiers entre 0 et n représentant les emplacements des coupes qui sont en-dehors de π_k. On note c le cardinal de p_0, $b := a - c$ et $A := \{P \setminus \pi_k = p_0\}$. Alors, sous $\mathbb{P}_{\mathbf{i}}$ et sachant A, $P_{|\pi_k}$ suit la loi multinomiale de paramètres $(r_k, \frac{1}{b}, \dots, \frac{1}{b})$.*

Démonstration.
C'est immédiat d'après 3.3.2. □

Proposition 3.4.3. *Soient $a_1, \dots, a_q$ des entiers, p'_0 une famille d'entiers entre 0 et n représentant les emplacements des coupes qui ne sont dans aucun des π_k, et $A := \{P \setminus \pi = p'_0\} \cap \bigcap_{k=1}^{q} \{\pi_k \text{ contient } a_k \text{ paquets}\}$. Alors, sous $\mathbb{P}_{\mathbf{i}}$ et sachant A, chaque $P_{|\pi_k}$ suit la loi multinomiale de paramètres $(r_k, \frac{1}{a_k}, \dots, \frac{1}{a_k})$.*

Démonstration.
Soient $j_1, \dots, j_{a_k}$ des entiers de somme r_k, on écrit :

$$\mathbb{P}_{\mathbf{i}}(P_{|\pi_k} = (j_1, \dots, j_{a_k}) \mid A) = \sum_{p_0} \mathbb{P}_{\mathbf{i}}(P_{|\pi_k} = (j_1, \dots, j_{a_k}) \mid P \setminus \pi_k = p_0\,)\, \mathbb{P}_{\mathbf{i}}(P \setminus \pi_k = p_0 \mid A)\ ,$$

où la somme porte sur tous les p_0 (emplacements possibles des coupes en-dehors de π_k) qui sont possibles sachant A i.e. tels que $A \cap \{P \setminus \pi_k = p_0\} = \{P \setminus \pi_k = p_0\}$. On applique maintenant 3.4.2 à chaque p_0 pour obtenir que $\mathbb{P}_{\mathbf{i}}(P_{|\pi_k} = (j_1, \dots, j_{a_k}) \mid P \setminus \pi_k = p_0\,) = \binom{r_k}{j_1\,,\,\dots\,,\,j_{a_k}}$. On conclut finalement que

$$\mathbb{P}_{\mathbf{i}}(P_{|\pi_k} = (j_1, \dots, j_{a_k}) \mid A) = \sum_{p_0} \binom{r_k}{j_1\,,\,\dots\,,\,j_{a_k}} \mathbb{P}_{\mathbf{i}}(P \setminus \pi_k = p_0 \mid A) = \binom{r_k}{j_1\,,\,\dots\,,\,j_{a_k}}\ . \qquad \square$$

Lemme 3.4.4. *Soit $(X_1, \dots, X_a)$ suivant la loi multinomiale de paramètres $(n, \frac{1}{a}, \dots, \frac{1}{a})$, on note X^* le premier X_i non nul en parcourant les indices dans l'ordre croissant. Alors $\mathbb{E}(X^*) = \frac{n}{a^n} \sum_{s=1}^{a} s^{n-1}$.*

Démonstration.
$\mathbb{E}(X^*) = \sum_{s=1}^{a} \mathbb{E}(X_s \mathbf{1}_{\{X_1 = \dots = X_{s-1} = 0\}}) = \sum_{s=1}^{a} \mathbb{E}(X_s \,|\, X_1 = \dots = X_{s-1} = 0) \mathbb{P}(X_1 = \dots = X_{s-1} = 0)$, or $\mathbb{E}(X_s \,|\, X_1 = \dots = X_{s-1} = 0) = \dfrac{n}{a - s + 1}$ (car la loi de $(X_s, \dots, X_a)$ sachant $\{X_1 = \dots = X_{s-1} = 0\}$ est multinomiale de paramètres $(n, \frac{1}{a-s+1}, \dots, \frac{1}{a-s+1})$) et $\mathbb{P}(X_1 = \dots = X_{s-1} = 0) = \left(\dfrac{a - s + 1}{a}\right)^n$. On obtient bien le résultat annoncé. $\square$

Proposition 3.4.5. *Soient $a_1, \dots, a_q$ des entiers, p'_0 une famille d'entiers entre 0 et n représentant les emplacements des coupes qui ne sont dans aucun des π_k, et $A := \{P \setminus \pi = p'_0\} \cap \bigcap_{k=1}^{q} \{\pi_k \text{ contient } a_k \text{ paquets}\}$. Alors pour tout $k \in \{1, \dots, q\}$: $\mathbb{E}_{\mathbf{i}}(h_P(j_k) \,|\, A) = \dfrac{r_k}{a_k^{r_k}} \sum_{s=1}^{a_k} s^{r_k - 1}$.*

Démonstration.
C'est immédiat d'après 3.4.3 et 3.4.4 : en effet, le paquet contenant j_k est précisément le premier paquet non vide de $P_{|\pi_k}$. $\square$

Il nous reste enfin à savoir estimer $\mathbb{P}_{\mathbf{i}}(A)$. Le calcul suivant va nous aider pour cela.

Proposition 3.4.6. *Soient $a_1, \dots, a_q$ des entiers, p'_0 une famille d'entiers entre 0 et n représentant les emplacements des coupes qui ne sont dans aucun des π_k. Alors $c_{\mathbf{a}} = \binom{n-m}{r_1\,,\,\dots\,,\,r_q} a_1^{r_1} \cdots a_q^{r_q}$, où on a posé $c_{\mathbf{a}} := \#\{(p, \sigma) \in \mathscr{C}_a^{\mathbf{i}}(n) \mid \ p \setminus \pi = p'_0 \ \text{ et } \ \pi_k \text{ contient } a_k \text{ paquets } \forall\ k\}$.*

Démonstration.
Comme $p \setminus \pi$ est forcé (égal à p'_0), choisir p revient à choisir la décomposition en paquets de chaque π_k, et ensuite le nombre de possibilités pour σ à p fixé est donné par le coefficient multinomial habituel :

$$\begin{aligned}
c_{\mathbf{a}} &= \sum_{x_{1,1}+\ldots+x_{1,a_1}=r_1} \cdots \sum_{x_{q,1}+\ldots+x_{q,a_q}=r_q} \binom{n-m}{x_{1,1},\ldots,x_{1,a_1},\ \ldots\ ,x_{q,1},\ldots,x_{q,a_q}} \\
&= \sum_{x_{1,1}+\ldots+x_{1,a_1}=r_1} \cdots \sum_{x_{q,1}+\ldots+x_{q,a_q}=r_q} \binom{r_1}{x_{1,1},\ldots,x_{1,a_1}} \cdots \binom{r_q}{x_{q,1},\ldots,x_{q,a_q}} \binom{n-m}{r_1,\ldots,r_q} \\
&= \binom{n-m}{r_1,\ldots,r_q} \left(\sum_{x_{1,1}+\ldots+x_{1,a_1}=r_1} \binom{r_1}{x_{1,1},\ldots,x_{1,a_1}} \right) \cdots \left(\sum_{x_{q,1}+\ldots+x_{q,a_q}=r_q} \binom{r_q}{x_{q,1},\ldots,x_{q,a_q}} \right) \\
&= \binom{n-m}{r_1\ ,\ \ldots\ ,\ r_q} a_1^{r_1} \cdots a_q^{r_q}\ .
\end{aligned}$$

□

Nous arrivons maintenant au résultat final.

Théorème 3.4.7. *Pour $a = 3$, et quel que soit $n \geq 12$, la stratégie BDM n'est pas optimale.*

Démonstration.

- Premier cas : n pair.
  Notre contre-exemple est obtenu pour $m = 1$ et $i_1 = \frac{n}{2} + 1$. On a donc $q = 2$, $\pi_1 = \{1, \ldots, \frac{n}{2}\}$, $\pi_2 = \{\frac{n}{2} + 2, \ldots, n\}$, $j_1 = 1$, $j_2 = \frac{n}{2} + 2$, $r_1 = \frac{n}{2} =: r$, $r_2 = r - 1$. La situation est particulièrement simple, car nécessairement $P \setminus \pi = (\frac{n}{2})$ (c'est la coupe obligatoire) et on n'a donc que deux possibilités : la deuxième coupe est soit dans π_1, soit dans π_2.

  - Première possibilité : π_1 contient 2 paquets et π_2 contient 1 paquet.
    D'après 3.4.6, il existe $2^r \binom{n-1}{r}$ telles combinaisons, sur l'ensemble desquelles la taille moyenne du paquet contenant j_2 est $r - 1$ et 3.4.5 assure que la taille moyenne du paquet contenant j_1 est $\dfrac{r}{2^r} \displaystyle\sum_{s=1}^{2} s^{r-1} = \dfrac{r}{2^r}(1 + 2^{r-1})$.
  - Deuxième possibilité : π_1 contient 1 paquet et π_2 contient 2 paquets.
    D'après 3.4.6, il existe $2^{r-1} \binom{n-1}{r}$ telles combinaisons, sur l'ensemble desquelles la taille moyenne du paquet contenant j_1 est r et 3.4.5 assure que que la taille moyenne du paquet contenant j_2 est $\dfrac{r-1}{2^{r-1}} \displaystyle\sum_{s=1}^{2} s^{r-2} = \dfrac{r-1}{2^{r-1}}(1 + 2^{r-2})$.

  On fait la moyenne pondérée sur ces deux cas de figure pour obtenir les formules suivantes :

$$\begin{aligned}
\mathbb{E}_{\mathbf{i}}(h_P(j_1)) &= \frac{2^r \binom{n-1}{r} \frac{r}{2^r}(1 + 2^{r-1}) + 2^{r-1} \binom{n-1}{r} r}{2^r \binom{n-1}{r} + 2^{r-1} \binom{n-1}{r}} = \frac{r(2^r + 1)}{3.2^{r-1}}\ , \\
\mathbb{E}_{\mathbf{i}}(h_P(j_2)) &= \frac{2^r \binom{n-1}{r}(r-1) + 2^{r-1} \binom{n-1}{r} \frac{r-1}{2^{r-1}}(1 + 2^{r-2})}{2^r \binom{n-1}{r} + 2^{r-1} \binom{n-1}{r}} = \frac{(r-1)(2^r + 2^{r-2} + 1)}{3.2^{r-1}}\ ,
\end{aligned}$$

  d'où $\mathbb{E}_{\mathbf{i}}(h_P(j_1)) - \mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \dfrac{2^r + 1 - (r-1)2^{r-2}}{3.2^{r-1}}$.

  Une simple étude de suite permet de vérifier que ceci est négatif si et seulement si $r \geq 6$ i.e. $n \geq 12$. Ainsi, pour $n \geq 12$, la deuxième carte du deck a plus de chances d'être la $\frac{n}{2} + 2$ que la 1, malgré le fait que $\frac{n}{2} + 2$ soit dans une moins longue suite de cartes consécutives restantes.

- Deuxième cas : n impair.
  Notre contre-exemple est obtenu pour $m = 1$ et $i_1 = \frac{n+3}{2}$. En notant toujours $r := r_1 = \frac{n+1}{2}$, la différence avec le cas pair est que $r_2 = r - 2$. Le même raisonnement fonctionne cependant et donne :

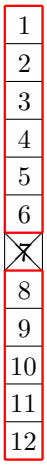
$$\mathbb{E}_{\mathbf{i}}(h_P(j_1)) = \frac{2^r\binom{n-1}{r}\frac{r}{2^r}(1+2^{r-1}) + 2^{r-2}\binom{n-1}{r}r}{2^r\binom{n-1}{r} + 2^{r-2}\binom{n-1}{r}} = \frac{r(2^{r-1}+2^{r-2}+1)}{5.2^{r-2}} \ ,$$

$$\mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{2^r\binom{n-1}{r}(r-2) + 2^{r-2}\binom{n-1}{r}\frac{r-2}{2^{r-2}}(1+2^{r-3})}{2^r\binom{n-1}{r} + 2^{r-2}\binom{n-1}{r}} = \frac{(r-2)(2^r+2^{r-3}+1)}{5.2^{r-2}} \ ,$$

  d'où $\mathbb{E}_{\mathbf{i}}(h_P(j_1)) - \mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{3.2^{r-1}+2-3(r-2)2^{r-3}}{5.2^{r-2}}$.

  On vérifie que ceci est négatif si et seulement si $r \geq 7$ i.e. $n \geq 13$. □

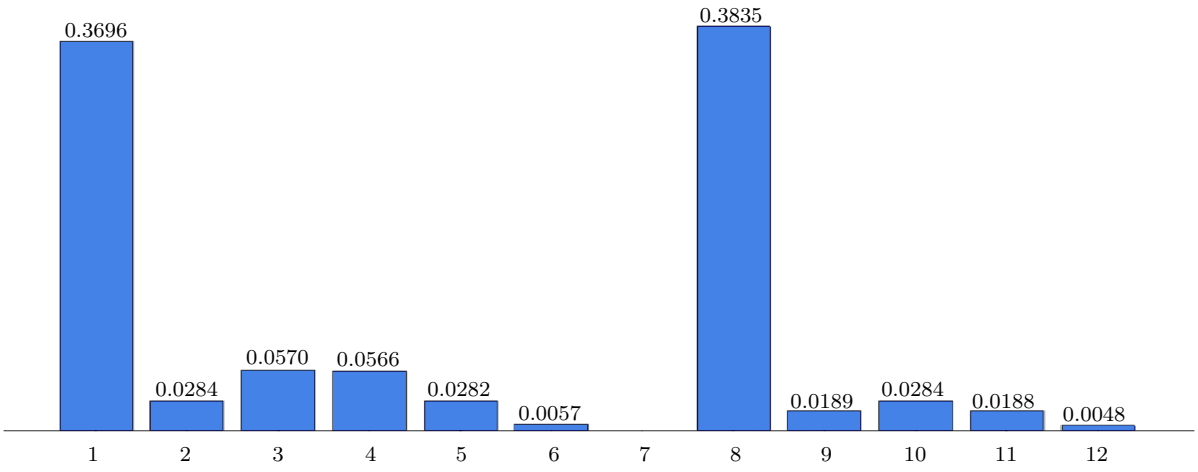
Exemple. Pour $n = 12$, $a = 3$, $\mathbf{i} = (7)$, la stratégie BDM dicte de proposer la carte 1 :



Les formules précédentes permettent en fait de calculer que :

- $\mathbb{E}_{\mathbf{i}}(h_P(1)) = \frac{65}{16} = 4,0625$ d'où $\mathbb{P}_{\mathbf{i}}(S(2) = 1) = \frac{\mathbb{E}_{\mathbf{i}}(h_P(1))}{11} = \frac{65}{176} \approx 0,3693$.
- $\mathbb{E}_{\mathbf{i}}(h_P(8)) = \frac{135}{32} = 4,21875$ d'où $\mathbb{P}_{\mathbf{i}}(S(2) = 8) = \frac{\mathbb{E}_{\mathbf{i}}(h_P(8))}{11} = \frac{135}{352} \approx 0,3835$.

Sachant que la première carte est la 7, la deuxième carte a donc environ $38,35\%$ de chances d'être la 8 et seulement $36,93\%$ de chances d'être la 1. Ceci est conforté par l'histogramme suivant qui représente, suite à 1 million de simulations par ordinateur d'un 3-shuffle sur 12 cartes conditionné à ce que la première carte soit la 7, les fréquences obtenues pour chaque valeur de la deuxième carte :



Remarque. Une conséquence de ce théorème est qu'une stratégie optimale se doit, contrairement à la stratégie BDM, de dépendre de a en général : en effet, si $n = 12$ et $\mathbf{i} = (7)$, la meilleure carte à proposer n'est pas la même si $a = 2$ (carte 1) ou si $a = 3$ (carte 8).

La stratégie BDM n'est évoquée dans [BD] que pour le cas où a est une puissance de 2, et notre contre-exemple porte sur $a = 3$. Cependant, le cas $a = 4$ n'est pas plus difficile :

Théorème 3.4.8. *Pour $a = 4$, et quel que soit $n \geq 13$, la stratégie BDM n'est pas optimale.*

Démonstration.

- Premier cas : n pair.
  Notre contre-exemple est obtenu pour $m = 2$ et $\mathbf{i} = (\frac{n}{2} + 1, n)$. On a donc $q = 2$, $\pi_1 = \{1, \dots, \frac{n}{2}\}$, $\pi_2 = \{\frac{n}{2} + 2, \dots, n-1\}$, $j_1 = 1$, $j_2 = \frac{n}{2} + 2$, $r_1 = \frac{n}{2} =: r$, $r_2 = r - 2$. Ce cas est pratiquement identique au cas n impair pour $a = 3$, se rajoute simplement un troisième cas de figure où la deuxième coupe est à l'emplacement n. D'après 3.4.6, il existe $\binom{n-2}{r}$ telles combinaisons, et sur chacune d'elles le paquet contenant j_1 est de taille r et le paquet contenant j_2 est de taille $r - 2$. On obtient :

$$\mathbb{E}_{\mathbf{i}}(h_P(j_1)) = \frac{2^r\binom{n-2}{r}\frac{r}{2^r}(1 + 2^{r-1}) + 2^{r-2}\binom{n-2}{r}r + \binom{n-2}{r}r}{2^r\binom{n-2}{r} + 2^{r-2}\binom{n-2}{r} + \binom{n-2}{r}} \ ,$$
$$\mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{2^r\binom{n-2}{r}(r-2) + 2^{r-2}\binom{n-2}{r}\frac{r-2}{2^{r-2}}(1 + 2^{r-3}) + \binom{n-2}{r}(r-2)}{2^r\binom{n-2}{r} + 2^{r-2}\binom{n-2}{r} + \binom{n-2}{r}} \ ,$$

  d'où après calcul $\mathbb{E}_{\mathbf{i}}(h_P(j_1)) - \mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \dfrac{3.2^{r-1} + 4 - 3(r-2)2^{r-3}}{5.2^{r-2} + 1}$.

  On vérifie que ceci est négatif si et seulement si $r \geq 7$ i.e. $n \geq 14$.

- Deuxième cas : n impair.
  Notre contre-exemple est obtenu pour $m = 2$ et $\mathbf{i} = (\frac{n+1}{2}, n)$. En notant toujours $r := r_1 = \frac{n-1}{2}$, on a cette fois $r_2 = r - 1$. Ce cas est pratiquement identique au cas n pair pour $a = 3$, se rajoute simplement un troisième cas de figure où la deuxième coupe est à l'emplacement n. D'après 3.4.6, il existe $\binom{n-2}{r}$ telles combinaisons, et sur chacune d'elles le paquet contenant j_1 est de taille r et le paquet contenant j_2 est de taille $r - 1$. On obtient :

$$\mathbb{E}_{\mathbf{i}}(h_P(j_1)) = \frac{2^r\binom{n-2}{r}\frac{r}{2^r}(1 + 2^{r-1}) + 2^{r-1}\binom{n-2}{r}r + \binom{n-2}{r}r}{2^r\binom{n-2}{r} + 2^{r-1}\binom{n-2}{r} + \binom{n-2}{r}} \ ,$$
$$\mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{2^r\binom{n-2}{r}(r-1) + 2^{r-1}\binom{n-2}{r}\frac{r-1}{2^{r-1}}(1 + 2^{r-2}) + \binom{n-2}{r}(r-1)}{2^r\binom{n-2}{r} + 2^{r-1}\binom{n-2}{r} + \binom{n-2}{r}} \ ,$$

  d'où après calcul $\mathbb{E}_{\mathbf{i}}(h_P(j_1)) - \mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \dfrac{2^r + 2 - (r-1)2^{r-2}}{3.2^{r-1} + 1}$.

  On vérifie que ceci est négatif si et seulement si $r \geq 6$ i.e. $n \geq 13$. □

Exemple. Pour $n = 13$, $a = 4$, $\mathbf{i} = (7, 13)$, la stratégie BDM dicte de proposer la carte 1 :

Les formules précédentes permettent en fait de calculer que :

- $\mathbb{E}_{\mathbf{i}}(h_P(1)) = \frac{396}{97} \approx 4,0825$ d'où $\mathbb{P}_{\mathbf{i}}(S(2)=1) = \frac{\mathbb{E}_{\mathbf{i}}(h_P(1))}{11} = \frac{36}{97} \approx 0,3711$.
- $\mathbb{E}_{\mathbf{i}}(h_P(8)) = \frac{410}{97} \approx 4,2268$ d'où $\mathbb{P}_{\mathbf{i}}(S(2)=8) = \frac{\mathbb{E}_{\mathbf{i}}(h_P(8))}{11} = \frac{410}{1067} \approx 0,3843$.

Sachant que les deux premières cartes sont la 7 et la 13, la troisième carte a donc environ $38,43\%$ de chances d'être la 8 et seulement $37,11\%$ de chances d'être la 1.

3.5 Zones d'erreur de la stratégie BDM

Nous avons vu que, dès la deuxième carte du paquet, la stratégie BDM désigne parfois la mauvaise option. Afin de comprendre ce phénomène et d'être éventuellement capable de déterminer une stratégie optimale, il peut être utile de calculer le vrai choix optimal de la deuxième carte, et de voir quelles valeurs de la première carte (et donc quel état des π_k) mettent la stratégie BDM en défaut. Ce qui suit n'est qu'une observation graphique, dans le cas $n = 52$ et $a \in \{3, 4\}$, de ces zones d'erreur de la stratégie BDM pour la deuxième carte i.e. pour $m = 1$.

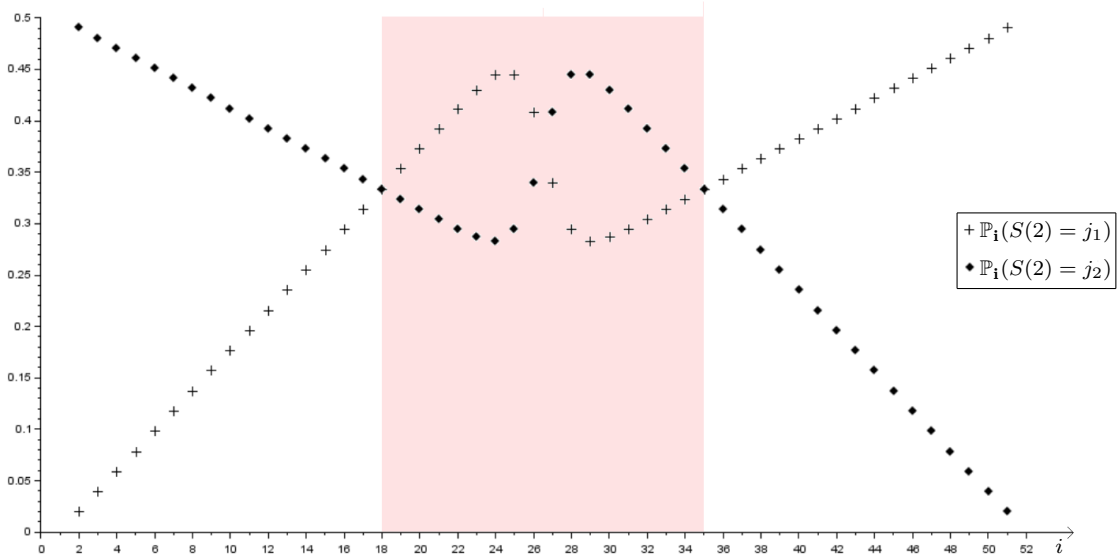
Notons $i = i_1$. On suppose que $2 \leq i \leq n-1$, sans quoi $q = 1$ et la stratégie optimale est connue. On a alors $r_1 = i-1$, $j_1 = 1$, $r_2 = n-i$, $j_2 = i+1$.

- Cas $a = 3$.
  Les calculs exacts pour $i = \frac{n}{2}$ (cas pair) ou $i = \frac{n+3}{2}$ (cas impair) ont été effectués en 3.4.7, mais on peut en faire de même pour n'importe quelle valeur de i. Il y a une unique coupe en-dehors de π, donc seulement deux cas de figure. On obtient au final :

$$\mathbb{E}_{\mathbf{i}}(h_P(j_1)) = \frac{2^{i-1}\binom{n-1}{i-1}\frac{i-1}{2^{i-1}}(1+2^{i-2}) + 2^{n-i}\binom{n-1}{i-1}(i-1)}{2^{i-1}\binom{n-1}{i-1} + 2^{n-i}\binom{n-1}{i-1}} = \frac{(i-1)(1+2^{i-2}+2^{n-i})}{2^{i-1}+2^{n-i}},$$

$$\mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{2^{i-1}\binom{n-1}{i-1}(n-i) + 2^{n-i}\binom{n-1}{i-1}\frac{n-i}{2^{n-i}}(1+2^{n-i-1})}{2^{i-1}\binom{n-1}{i-1} + 2^{n-i}\binom{n-1}{i-1}} = \frac{(n-i)(1+2^{i-1}+2^{n-i-1})}{2^{i-1}+2^{n-i}}.$$

  Pour $n = 52$, les probabilités $\mathbb{P}_{\mathbf{i}}(S(2) = j_1)$ et $\mathbb{P}_{\mathbf{i}}(S(2) = j_2)$ en fonction de i sont représentées ci-dessous, où la zone d'erreur de la stratégie BDM apparaît en rouge :

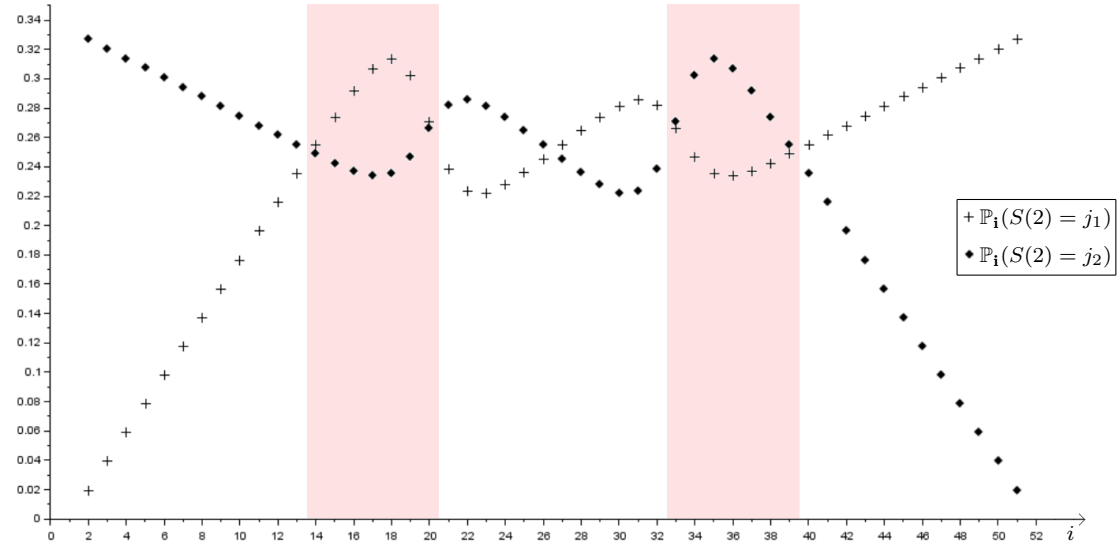


On constate que la stratégie BDM commet une erreur lorsque $18 < i < 35$, l'erreur maximale étant commise pour $i = 24$ ou $i = 29$. Par exemple, pour $i = 24$, on a $\mathbb{P}_{\mathbf{i}}(S(2) = 1) \approx 0.444$ et $\mathbb{P}_{\mathbf{i}}(S(2) = 25) \approx 0.283$ alors que la stratégie BDM recommande la carte 25.

- Cas $a = 4$.
  Il y a deux coupes en-dehors de π, donc trois cas de figure. Dans le premier (resp. le deuxième, resp. le troisième), π_1 et π_2 contiennent respectivement 3 et 1 (resp. 2 et 2, resp. 1 et 3) paquets :

$$\mathbb{E}_{\mathbf{i}}(h_P(j_1)) = \frac{3^{i-1}\frac{i-1}{3^{i-1}}(1+2^{i-2}+3^{i-2}) + 2^{i-1}2^{n-i}\frac{i-1}{2^{i-1}}(1+2^{i-2}) + 3^{n-i}(i-1)}{3^{i-1}+2^{i-1}2^{n-i}+3^{n-i}},$$
$$\mathbb{E}_{\mathbf{i}}(h_P(j_2)) = \frac{3^{i-1}(n-i) + 2^{i-1}2^{n-i}\frac{n-i}{2^{n-i}}(1+2^{n-i-1}) + 3^{n-i}\frac{n-i}{3^{n-i}}(1+2^{n-i-1}+3^{n-i-1})}{3^{i-1}+2^{i-1}2^{n-i}+3^{n-i}}.$$

  Pour $n = 52$, on a cette fois-ci deux zones d'erreur disjointes :



La stratégie BDM commet une erreur lorsque $14 \leq i \leq 20$ ou $33 \leq i \leq 39$, l'erreur maximale étant commise pour $i = 18$ ou $i = 35$. Par exemple, pour $i = 18$, on a $\mathbb{P}_{\mathbf{i}}(S(2) = 1) \approx 0.314$ et $\mathbb{P}_{\mathbf{i}}(S(2) = 19) \approx 0.235$ alors que la stratégie BDM recommande la carte 19.

Références

[BD] Dave Bayer et Persi Diaconis, « Trailing the dovetail shuffle to its lair », *The Annals of Applied Probability*, Vol.2, No.2, pp.294–313 (1992).

[Tan] S. Tanny, « A probabilistic interpretation of eulerian numbers », *Duke Math. J.*, Vol.40, No.4, pp.717-722 (1973).

[Fel] William Feller, *An introduction to probability theory and its applications Vol. 2*, 2nd edition, Wiley (1971).