

# Quelques mélanges parfaits de cartes

par Aimé LACHAL \*

## I Description du problème

Le problème suivant m'a été soumis par l'un de mes élèves<sup>1</sup> qui a une grande pratique de la magie. On dispose d'une pile de  $2n$  jetons dont les  $n$  du bas sont verts et les  $n$  du haut sont rouges. Il divise la pile en deux parties : l'une contenant les  $n$  jetons verts, l'autre contenant les  $n$  jetons rouges. Avec une dextérité remarquable, de sa seule main droite il prend simultanément les deux piles de jetons, puis procède à un mélange de ces deux dernières pour former une unique pile (de  $2n$  jetons) alternant parfaitement jeton rouge et jeton vert. Cette nouvelle pile est divisée à son tour exactement en son milieu donnant deux tas de  $n$  jetons et notre magicien procède à un nouveau mélange intercalant alternativement un jeton de chaque tas pour former une nouvelle pile de  $2n$  jetons qu'il recoupe de nouveau en deux piles de  $n$  jetons et ainsi de suite.

Après plusieurs expériences (pour  $n \leq 8$ ), notre magicien s'aperçut qu'il retombait au bout d'un certain nombre de tels mélanges sur la pile initiale : les  $n$  jetons du bas sont verts et les  $n$  du haut sont rouges (voir Fig. 1–6 pour  $n = 4$ ). Plus frappant encore, en numérotant et ordonnant les jetons, il semblerait que la première fois que l'on retrouve une pile de  $n$  jetons verts consécutifs et de  $n$  rouges de bas en haut, les jetons soient en fait exactement dans l'ordre initial. Les questions qu'il m'a soumises étaient alors les suivantes : étant donnée une pile de  $2n$  jetons numérotés  $1, 2, \dots, 2n - 1, 2n$  ( $n \in \mathbb{N}^*$ ) et superposés de bas en haut dans l'ordre croissant,

1. le processus de mélange décrit ci-dessus

---

\*Adresse :

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE LYON  
Pôle de Mathématiques  
Bâtiment Léonard de Vinci, 20 avenue Albert Einstein  
69621 Villeurbanne Cedex, FRANCE  
E-mail: aime.lachal@insa-lyon.fr

<sup>1</sup>Anthony Tschirhard, INSA de Lyon, 51<sup>e</sup> promotion

conduit-il nécessairement au classement initial en un temps fini ?

2. si oui, peut-on exprimer en fonction de  $n$  le nombre minimum de mélanges nécessaires pour retrouver le classement initial ?
3. si les  $n$  premiers jetons sont verts et les  $n$  derniers rouges, peut-on arriver au regroupement initial des jetons (la pile du bas constituée de jetons verts, celle du haut de rouges) éventuellement dans le désordre quant à la numérotation ?

Il s'agit d'un problème classique bien connu du monde de la magie des cartes, la manipulation précédente étant souvent faite avec des cartes à jouer. Le jeu habituel de 32 cartes est privilégié car le nombre 32 se décompose en  $2^5$ , ce qui conduit à des propriétés remarquables. Dans la littérature, ce type de problème est abordé sous le vocable anglophone de « chip-shuffle » pour les jetons, de « riffle-shuffle » pour les cartes et plus précisément de « in-shuffle » et de « out-shuffle » selon le placement des cartes initiales de chaque paquet lors d'un mélange. Il a été considéré entre autres par le célèbre informaticien et magicien Elmsley en 1957 ([6]). On trouvera également une large description historique du problème dans la section intitulée « some history of perfect shuffle » de [5].

Les in-shuffles et out-shuffles sont des mélanges très proches. Disposant d'un jeu de cartes que l'on coupe au milieu donnant deux paquets de cartes (un premier et un deuxième), l'in-shuffle du jeu initial consiste à démarrer le processus en plaçant la première carte du bas du premier paquet sur la première carte du bas du deuxième paquet. À l'opposé, l'out-shuffle consiste à démarrer en plaçant la première carte du bas du premier paquet sous la première carte du bas du deuxième paquet. Notons que dans le cas de l'out-shuffle, les première et dernière cartes restent immobiles tout au long de l'expérience. On pourra consulter les sites internet [17, 18] pour un recensement de ces divers mélanges ainsi que d'autres.

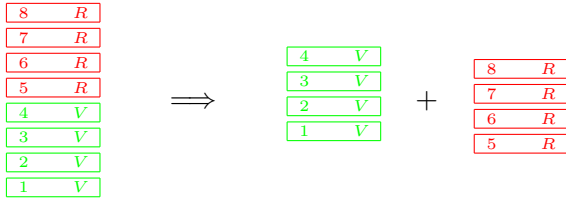


FIG. 1 – Premier découpage

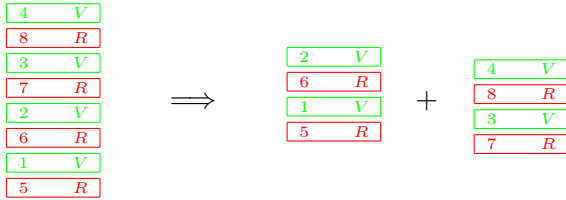


FIG. 2 – Deuxième découpage

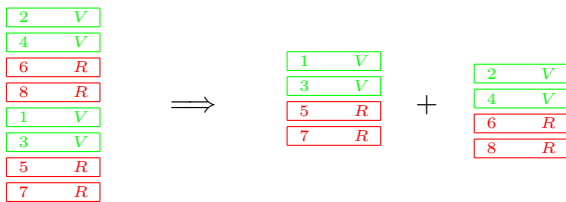


FIG. 3 – Troisième découpage

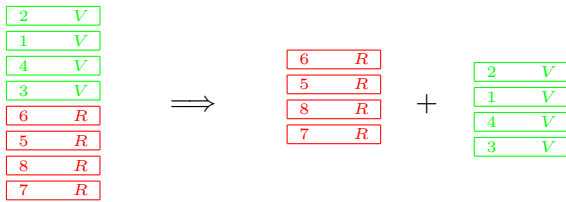


FIG. 4 – Quatrième découpage

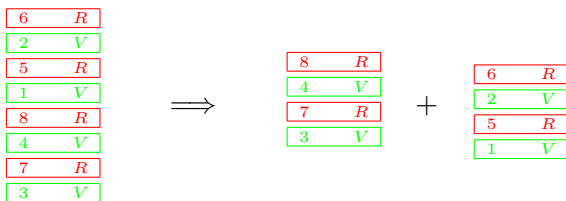


FIG. 5 – Cinquième découpage

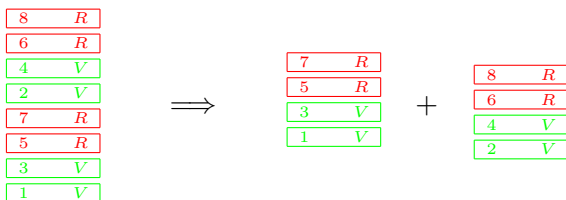


FIG. 6 – Sixième découpage

Elmsley se posait la question plus complexe : est-il possible de déplacer la carte du dessus du paquet à une position donnée à l'avance à l'aide d'une succession de mélanges de nature in-shuffle ou out-shuffle ([6]) ? La réponse est positive et il obtint un procédé pour accomplir une telle manipulation. Inversement, est-il possible de faire apparaître une carte donnée dans le jeu sur le haut du paquet de cartes, voire à une place quelconque selon un procédé similaire ? Récemment, les mathématiciens Diaconis et Graham (le premier auteur est également magicien) ont répondu positivement à la question générale du déplacement d'une carte donnée vers une position donnée. Ils ont proposé un algorithme indiquant le chemin à suivre (succession de in- et out-shuffles, [4]).

Reprenons les questions posées par mon élève. La réponse à la première question est affirmative et la raison en est très simple. Sommairement, on travaille dans un groupe fini de permutations, on revient donc à la position initiale au bout d'un nombre fini d'expériences, il s'agit d'un processus périodique. La réponse à la deuxième question est également affirmative ; c'est un calcul de période et une formule implicite est disponible, voir e.g. les livres de Conway & Guy, [3, p. 163–165], de Herstein & Kaplansky, [8, Chap. 3.4], ou d'Uspensky & Heaslet, [16, p. 244–245]. Néanmoins, une formule explicite ne semble pas accessible excepté pour les cas particuliers où  $n$  est une puissance de 2 à  $\pm 1$  près. La troisième question semble rester à ma connaissance ouverte.

Dans cet article, je détaille le processus de l'in-shuffle – celui de l'out-shuffle s'en déduisant aisément – à l'aide de permutations de l'ensemble  $\{0, 1, 2, \dots, 2n - 1\}$  ou  $\{1, 2, 3, \dots, 2n\}$ . L'un des deux ensembles sera d'une utilisation plus commode que l'autre selon le cas étudié. Les permutations associées à  $\{0, 1, 2, \dots, 2n - 1\}$  sont particulièrement bien adaptées au calcul explicite des itérations successives (correspondant à la succession de mélanges parfaits) par le truchement des écritures binaires. Aussi, je détaille toutes les permutations relatives aux deux numérotations en signalant laquelle permet de formuler le plus simplement possible la période recherchée. Je porte un intérêt particulier aux cas spécifiques mentionnés plus haut, à savoir lorsque  $n$  est une puissance de 2 à  $\pm 1$  près. J'examine également d'autres exemples de mélanges parfaits : les mélanges de Monge qui sont des in/out-shuffles déformés par une symétrie

(voir e.g. [3, 17, 18]). Toute cette analyse permet d'accéder au calcul des périodes de chacun des mélanges décrits ici.

Par souci d'homogénéité des notations, on notera  $f, g, h, \dots$  les permutations relatives à l'énumération  $1, 2, 3, \dots, 2n$  et  $\tilde{f}, \tilde{g}, \tilde{h}, \dots$  celles associées à  $0, 1, 2, \dots, 2n - 1$ . On passe par exemple de la permutation  $f$  à la permutation  $\tilde{f}$  selon la relation  $\tilde{f}(i) = f(i + 1) - 1$  pour tout  $i \in \{0, 1, 2, \dots, 2n - 1\}$ .

Il est remarquable de constater que, bien au-delà de son aspect ludique, ce problème suscite des questions de nature algébrique avancées (théorie des groupes, [5, 7]). L'étude approfondie de certaines permutations mises en jeu a été entreprise indépendamment de ce contexte par Lévy ([9, 10, 11]). Ce problème connaît également des applications notamment en informatique (calcul parallèle, réseaux, [2, 14, 15]). Mentionnons enfin l'existence d'autres types de mélanges d'une importance notoire qui ont retenu l'attention des mathématiciens : les mélanges aléatoires (voir [1] pour plus d'informations concernant ce type de mélange).

### Plan de l'article

- Dans la section II, nous présentons la modélisation du problème en introduisant toutes les permutations relatives aux différents mélanges de cartes. Certaines permutations redondantes ne seront pas nécessairement utiles, mais nous avons choisi de les écrire systématiquement afin de garder une homogénéité de notations ainsi qu'une logique de présentation. Selon les cas étudiés, certaines d'entre elles serviront à calculer la période du mélange en question, alors que d'autres permettront le calcul explicite des itérations successives.
- Dans la section III, nous formulons de manière implicite les réponses relatives au calcul de périodes des mélanges étudiés.
- Dans les sections IV et V, nous calculons explicitement, en faisant appel au calcul binaire, toutes les itérations successives de certaines permutations significatives, dans les cas particuliers où  $n$  est une puissance de 2 à  $\pm 1$  près, ce qui permet de fournir une réponse explicite aux questions posées.
- Dans la section VI, nous examinons briève-

ment le cas d'un jeu contenant un nombre impair de cartes.

- Dans la section VII, nous décrivons un procédé simple pour déplacer une carte donnée vers une position prédéfinie dans le cas où  $n$  est une puissance de 2.
- Nous terminons dans la section VIII par une tentative de généralisation à un paquet de cartes divisible par un nombre supérieur à deux.

## II Modélisation

Le jeu de cartes numérotées de bas en haut dans l'ordre  $1, 2, 3, \dots, 2n$  est coupé en son milieu et donne les deux paquets de cartes numérotées  $1, 2, \dots, n$  pour le premier et  $n + 1, n + 2, \dots, 2n$  pour le deuxième. On constitue un nouveau jeu de  $2n$  cartes en prenant à tour de rôle une carte de chacun des paquets de  $n$  cartes.

### II.1 In-shuffle

Si l'on démarre le mélange par le deuxième paquet (cas d'un in-shuffle), on obtient dans l'ordre la suite de cartes n<sup>os</sup>  $n + 1, 1, n + 2, 2, n + 3, 3, \dots, 2n - 1, n - 1, 2n, n$  (voir Fig. 7).

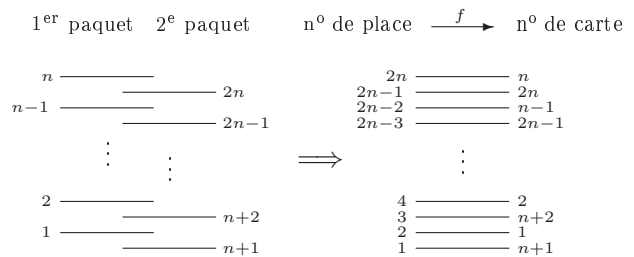


FIG. 7 - In-shuffle, permutation  $f$

Cela se traduit par une correspondance entre numéros d'ordre avant et après mélange : à l'issue du mélange, la première carte porte le n<sup>o</sup>  $n + 1$ , la deuxième le n<sup>o</sup>  $1$ , la troisième le n<sup>o</sup>  $n + 2$ , la quatrième le n<sup>o</sup>  $2$ , etc. De manière générale, la  $i^e$  carte porte le n<sup>o</sup>  $i/2$  lorsque  $i$  est pair et le n<sup>o</sup>  $(i+1)/2+n$  lorsque  $i$  est impair. Cette correspondance définit une permutation  $f$  des entiers  $1, 2, 3, \dots, 2n$  donnant le numéro de la carte se situant à la  $i^e$

position à l'issue du mélange :

$$f(i) = \begin{cases} \frac{i}{2} & \text{si } i \text{ est pair,} \\ \frac{i+1}{2} + n & \text{si } i \text{ est impair,} \end{cases}$$

que l'on peut encore écrire  $f(i) = \lfloor \frac{i+1}{2} \rfloor + \varepsilon(i)n$  où  $\lfloor \cdot \rfloor$  est la fonction partie-entière et  $\varepsilon(i) = 0$  si  $i$  est pair,  $\varepsilon(i) = 1$  si  $i$  est impair.

La permutation réciproque est un peu plus simple à écrire :

$$f^{-1}(j) = \begin{cases} 2j & \text{si } 1 \leq j \leq n, \\ 2j - 2n - 1 & \text{si } n + 1 \leq j \leq 2n. \end{cases}$$

Rappelant la définition d'une congruence arithmétique, «  $a \equiv b \pmod{n}$  » signifie «  $a - b$  est divisible par  $n$  », on a en particulier la congruence remarquable

$$f^{-1}(j) \equiv 2j \pmod{(2n+1)}$$

qui sera utile pour calculer la période de  $f$ . Cette réciproque indique qu'une carte portant un numéro  $j$  entre 1 et  $n$  occupe à l'issue du mélange la place  $n^\circ 2j$ , et qu'une carte portant un numéro  $j$  entre  $n+1$  et  $2n$  occupe la place  $n^\circ 2j - 2n - 1$ . Par exemple, la carte  $n^\circ 1$  occupe la place  $n^\circ 2$ , la carte  $n^\circ 2$  occupe la place  $n^\circ 4, \dots$ , puis la carte  $n^\circ n$  occupe la place  $n^\circ 2n$ , la carte  $n^\circ n+1$  occupe la place  $n^\circ 1$ , la carte  $n^\circ n+2$  occupe la place  $n^\circ 3$ , etc.

Il est utile de transcrire cette modélisation en translatant simplement la numérotation des cartes d'une unité. Cela fournit la permutation  $\tilde{f}$  des entiers  $0, 1, 2, \dots, 2n-1$  définie par  $\tilde{f}(i) = f(i+1) - 1$ , soit :

$$\tilde{f}(i) = \begin{cases} \frac{i}{2} + n & \text{si } i \text{ est pair,} \\ \frac{i-1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

et la permutation réciproque s'écrit :

$$\tilde{f}^{-1}(j) = \begin{cases} 2j + 1 & \text{si } 0 \leq j \leq n-1, \\ 2j - 2n & \text{si } n \leq j \leq 2n-1. \end{cases}$$

Les permutations  $f$  et  $\tilde{f}$  nous permettront de calculer explicitement la période de l'in-shuffle dans les cas particuliers  $n = 2^{p-1}$  et  $n = 2^{p-1} - 1$ .

## II.2 Out-shuffle

Si on démarre le mélange à présent par le premier paquet (cas d'un out-shuffle), on obtient dans l'ordre les cartes  $n^\circ 1, n+1, 2, n+2, 3, n+3, \dots, n-1, 2n-1, n, 2n$  (voir Fig. 8).

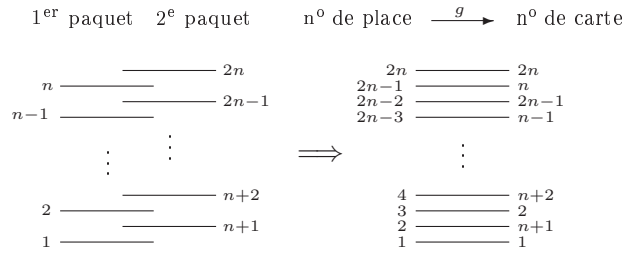


FIG. 8 - Out-shuffle, permutation  $g$

Ce processus définit alors la permutation  $g$  des entiers  $1, 2, \dots, 2n$  suivante :

$$g(i) = \begin{cases} \frac{i}{2} + n & \text{si } i \text{ est pair,} \\ \frac{i+1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

de réciproque

$$g^{-1}(j) = \begin{cases} 2j - 1 & \text{si } 1 \leq j \leq n, \\ 2j - 2n & \text{si } n + 1 \leq j \leq 2n. \end{cases}$$

On observe que  $g(1) = 1$  et  $g(2n) = 2n$ , i.e. les cartes  $n^\circ 1$  et  $2n$  restent immobiles tout au cours de la manipulation.

Retranscrivons cette modélisation en translatant la numérotation des cartes d'une unité. Cela fournit la permutation  $\tilde{g}$  des entiers  $0, 1, 2, \dots, 2n-1$  définie par  $\tilde{g}(i) = g(i+1) - 1$ , soit :

$$\tilde{g}(i) = \begin{cases} \frac{i}{2} & \text{si } i \text{ est pair,} \\ \frac{i-1}{2} + n & \text{si } i \text{ est impair,} \end{cases}$$

et la permutation réciproque s'écrit :

$$\tilde{g}^{-1}(j) = \begin{cases} 2j & \text{si } 0 \leq j \leq n-1, \\ 2j + 1 - 2n & \text{si } n \leq j \leq 2n-1. \end{cases}$$

Notons en particulier la congruence

$$\tilde{g}^{-1}(j) \equiv 2j \pmod{(2n-1)}.$$

La restriction de  $\tilde{g}$  à l'ensemble  $\{1, \dots, 2n-2\}$  est une permutation qui correspond à un in-shuffle de  $2n-2$  cartes. Cette observation indique qu'un out-shuffle de  $2n$  cartes est identique à un in-shuffle de ce jeu auquel on a retiré les première et dernière cartes, donnant ainsi un jeu de  $2n-2$  cartes.

### II.3 Mélange de Monge : première version

Le mélange de Monge consiste à faire passer les cartes d'un jeu complet d'une main à l'autre en intercalant alternativement les cartes l'une au-dessus et au-dessous de l'autre.

#### II.3.1 Première façon de démarrer le processus

On numérote les cartes de 1 à  $2n$ . On commence par prendre la carte n° 1 qui va démarrer le nouveau paquet, puis la carte n° 2 que l'on place au-dessous du nouveau paquet (donc au-dessous de la carte n° 1), puis la carte n° 3 que l'on place au-dessus du nouveau paquet (donc au-dessus de la n° 1), puis la carte n° 4 que l'on place au-dessous du nouveau paquet (donc au-dessous de la n° 2), puis la carte n° 5 que l'on place au-dessus du nouveau paquet (donc au-dessus de la n° 3), et ainsi de suite (voir Fig. 9). On obtient alors dans l'ordre, de bas en haut, les cartes n°s  $2n, 2n-2, 2n-4, \dots, 4, 2, 1, 3, \dots, 2n-3, 2n-1$ . On rencontre donc les cartes de numéros pairs dans l'ordre décroissant puis celles de numéros impairs dans l'ordre croissant.

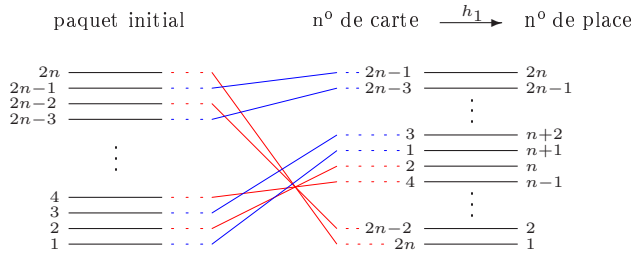


FIG. 9 – Mélange de Monge, permutation  $h_1$

Ce mélange correspond à la permutation  $h_1^{-1}$  des entiers  $1, 2, \dots, 2n$  où  $h_1$  est donnée par

$$h_1(i) = \begin{cases} \frac{i+1}{2} + n & \text{si } i \text{ est impair,} \\ n+1 - \frac{i}{2} & \text{si } i \text{ est pair.} \end{cases}$$

La permutation  $h_1^{-1}$  s'écrit

$$h_1^{-1}(j) = \begin{cases} 2n+2-2j & \text{si } 1 \leq j \leq n, \\ 2j-2n-1 & \text{si } n+1 \leq j \leq 2n. \end{cases}$$

La permutation analogue  $\tilde{h}_1$  associée à la numé-

rotation  $0, 1, 2, \dots, 2n-1$  est donnée par

$$\tilde{h}_1(i) = \begin{cases} \frac{i}{2} + n & \text{si } i \text{ est pair,} \\ n - \frac{i+1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

et sa réciproque par

$$\tilde{h}_1^{-1}(j) = \begin{cases} 2n-1-2j & \text{si } 0 \leq j \leq n-1, \\ 2j-2n & \text{si } n \leq j \leq 2n-1. \end{cases}$$

#### II.3.2 Deuxième façon de démarrer le processus

On commence par prendre la carte n° 1 qui va démarrer le nouveau paquet, puis la carte n° 2 que l'on place à présent au-dessus du nouveau paquet (donc au-dessus de la carte n° 1), puis la carte n° 3 que l'on place au-dessous de la n° 1, puis la carte n° 4 que l'on place au-dessus de la n° 2, puis la carte n° 5 que l'on place au-dessous de la n° 3, et ainsi de suite (voir Fig. 10). On obtient cette fois dans l'ordre, de bas en haut, les cartes n°s  $2n-1, 2n-3, \dots, 3, 1, 2, 4, \dots, 2n-2, 2n$ , c'est-à-dire les cartes de numéros impairs dans l'ordre décroissant puis celles de numéros pairs dans l'ordre croissant.

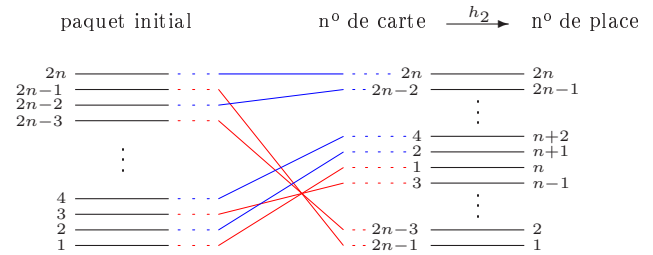


FIG. 10 – Mélange de Monge, permutation  $h_2$

Remarquons que ce mélange se déduit du précédent simplement en retournant le jeu, ou encore en effectuant la symétrie  $j \mapsto 2n+1-j$ . En notant  $h_2^{-1}$  la permutation des entiers  $1, 2, \dots, 2n$  correspondant à ce mélange, on a précisément la relation  $h_2^{-1}(j) = h_1^{-1}(2n+1-j)$  pour tout  $j \in \{1, 2, \dots, 2n\}$ , qui est équivalente à  $h_2(i) = 2n+1-h_1(i)$  pour tout  $i \in \{1, 2, \dots, 2n\}$ . Donc

$$h_2(i) = \begin{cases} \frac{i}{2} + n & \text{si } i \text{ est pair,} \\ n - \frac{i-1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

et

$$h_2^{-1}(j) = \begin{cases} 2n+1-2j & \text{si } 1 \leq j \leq n, \\ 2j-2n & \text{si } n+1 \leq j \leq 2n. \end{cases}$$

La permutation  $\tilde{h}_2$  relative à la numérotation  $0, 1, 2, \dots, 2n - 1$  s'écrit :

$$\tilde{h}_2(i) = \begin{cases} \frac{i-1}{2} + n & \text{si } i \text{ est impair,} \\ n-1 - \frac{i}{2} & \text{si } i \text{ est pair,} \end{cases}$$

et sa réciproque :

$$\tilde{h}_2^{-1}(j) = \begin{cases} 2n-2-2j & \text{si } 0 \leq j \leq n-1, \\ 2j-2n+1 & \text{si } n \leq j \leq 2n-1. \end{cases}$$

## II.4 Mélange de Monge : deuxième version

Une autre version du mélange de Monge consiste à couper le jeu de cartes initialement numérotées  $1, 2, \dots, 2n$  en deux paquets de cartes numérotées  $1, 2, \dots, n$  et  $n+1, n+2, \dots, 2n$ , à retourner le deuxième paquet qui devient ordonné selon  $2n, 2n-1, \dots, n+2, n+1$ , puis de mélanger le premier paquet et le deuxième ainsi retourné via un in-shuffle ou un out-shuffle. Cela donne un mélange « à l'espagnole » : on dispose les deux paquets sous forme d'éventails, on retourne le deuxième éventail (Olé !) et on intercale parfaitement les deux éventails.

### II.4.1 In-shuffle de Monge

On intercale les deux paquets de cartes numérotées  $1, 2, \dots, n$  et  $2n, 2n-1, \dots, n+2, n+1$  en commençant par le deuxième (cas d'un in-shuffle, voir Fig. 11). Cela donne la succession de cartes n<sup>os</sup>  $2n, 1, 2n-1, 2, \dots, n+2, n-1, n+1, n$ .

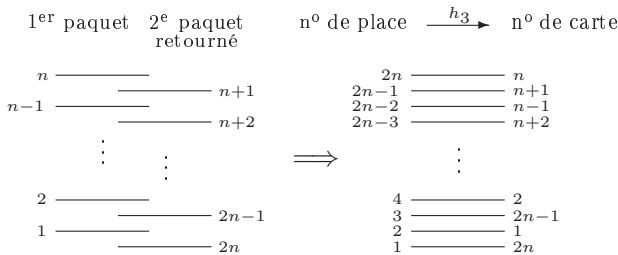


FIG. 11 – Mélange de Monge, permutation  $h_3$

Cette séquence est représentée par la permutation  $h_3$  des entiers  $1, 2, \dots, 2n$  suivante :

$$h_3(i) = \begin{cases} \frac{i}{2} & \text{si } i \text{ est pair,} \\ 2n - \frac{i-1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

de réciproque

$$h_3^{-1}(j) = \begin{cases} 2j & \text{si } 1 \leq j \leq n, \\ 4n+1-2j & \text{si } n+1 \leq j \leq 2n. \end{cases}$$

On a en particulier la congruence importante

$$h_3^{-1}(j) \equiv \pm 2j \pmod{(4n+1)}.$$

Les permutations analogues des entiers  $0, 1, 2, \dots, 2n-1$  sont alors les suivantes :

$$\tilde{h}_3(i) = \begin{cases} \frac{i-1}{2} & \text{si } i \text{ est impair,} \\ 2n-1 - \frac{i}{2} & \text{si } i \text{ est pair,} \end{cases}$$

et

$$\tilde{h}_3^{-1}(j) = \begin{cases} 2j+1 & \text{si } 0 \leq j \leq n-1, \\ 4n-2-2j & \text{si } n \leq j \leq 2n-1. \end{cases}$$

Ce mélange est relié à celui décrit dans II.3.1 selon la relation  $2n+1-h_3(2n+1-i) = h_1(i)$  valable pour tout  $i \in \{1, 2, \dots, 2n\}$ , soit encore en notant  $s$  la symétrie  $i \mapsto 2n+1-i$ ,

$$h_3 = s \circ h_1 \circ s = s \circ h_1 \circ s^{-1}.$$

Les permutations  $h_1$  et  $h_3$  sont donc conjuguées dans le groupe des permutations  $(\mathcal{S}_{2n}, \circ)$ .

### II.4.2 Out-shuffle de Monge

On intercale à présent les deux paquets de cartes numérotées  $1, 2, \dots, n$  et  $2n, 2n-1, \dots, n+2, n+1$  en commençant par le premier (cas d'un out-shuffle, voir Fig. 12). Cela conduit à la séquence de cartes n<sup>os</sup>  $1, 2n, 2, 2n-1, \dots, n-1, n+2, n, n+1$ .

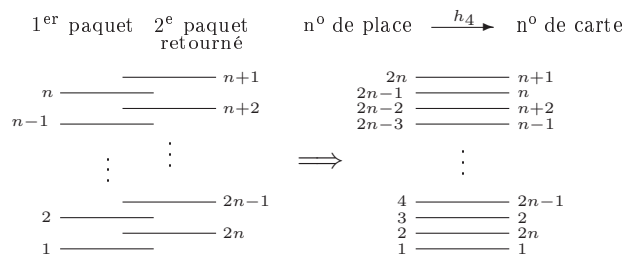


FIG. 12 – Mélange de Monge, permutation  $h_4$

D'où les permutations des entiers  $1, 2, \dots, 2n$  suivantes :

$$h_4(i) = \begin{cases} \frac{i+1}{2} & \text{si } i \text{ est impair,} \\ 2n+1 - \frac{i}{2} & \text{si } i \text{ est pair,} \end{cases}$$

et

$$h_4^{-1}(j) = \begin{cases} 2j - 1 & \text{si } 1 \leq j \leq n, \\ 4n + 2 - 2j & \text{si } n + 1 \leq j \leq 2n. \end{cases}$$

On a  $h_4(1) = 1$ , ce qui signifie que la carte n° 1 reste immobile dans cette manipulation. Les permutations des entiers  $0, 1, 2, \dots, 2n - 1$  associées sont les suivantes :

$$\tilde{h}_4(i) = \begin{cases} \frac{i}{2} & \text{si } i \text{ est pair,} \\ 2n - \frac{i+1}{2} & \text{si } i \text{ est impair,} \end{cases}$$

et

$$\tilde{h}_4^{-1}(j) = \begin{cases} 2j & \text{si } 0 \leq j \leq n - 1, \\ 4n - 1 - 2j & \text{si } n \leq j \leq 2n - 1. \end{cases}$$

On a en particulier la congruence notoire

$$\tilde{h}_4^{-1}(j) \equiv \pm 2j \pmod{(4n - 1)}.$$

À l'instar du mélange de la section II.4.1, ce mélange est relié à celui décrit dans II.3.2 selon

$$h_4 = s \circ h_2 \circ s^{-1}.$$

Les permutations  $h_2$  et  $h_4$  sont donc conjuguées.

Pour résumer et avoir une vision concise des divers mélanges considérés, nous avons défini les permutations  $f$  (in-shuffle),  $g$  (out-shuffle) et  $h_1, h_2, h_3, h_4$  (mélanges de Monge) ainsi que leurs translatées  $\tilde{f}, \tilde{g}, \tilde{h}_1, \tilde{h}_2, \tilde{h}_3, \tilde{h}_4$  et leurs réciproques.

### III Une formulation de la solution du problème

Les mélanges répétés correspondent mathématiquement aux itérations successives des permutations décrites précédemment. Travaillons par exemple avec la permutation de l'in-shuffle  $f$ . L'issue des  $k$  premiers mélanges est représentée par la permutation

$$f^k = \underbrace{f \circ \dots \circ f}_{k \text{ fois}}$$

Plus précisément, la quantité  $f^k(i)$  désigne le numéro de la carte se trouvant à la position n°  $i$ . Ainsi l'intégralité de l'expérience (supposée illimitée...) est modélisée par l'ensemble des itérations successives de  $f$  suivant :  $\{id, f, f^2, f^3, \dots\}$

$= \{f^k, k \in \mathbb{N}\}$ . C'est un sous-ensemble de l'ensemble fini  $\mathcal{S}_{2n}$  des permutations de  $\{1, 2, \dots, 2n\}$ , il est donc fini lui-même et il y a au moins deux entiers distincts  $k$  et  $l$  tels que  $f^k \neq f^l$ . Comme  $f$  est bijective, on a en supposant par exemple que  $k < l$  et en posant alors  $r = l - k$ ,  $f^r = id$ , ou encore  $(f^{-1})^r = id$ . Cela signifie qu'au bout de  $r$  mélanges parfaits, on retombe nécessairement sur l'ordre initial des cartes. Ceci répond affirmativement à la première question posée dans l'introduction.

L'ensemble  $\{f^k, k \in \mathbb{N}\}$ , qui est *a posteriori* identique à  $\{f^k, k \in \mathbb{Z}\}$ , s'écrit en extension selon  $\{id, f, f^2, \dots, f^{r-1}\}$ . Le nombre  $r$  est une période de l'application  $k \in \mathbb{Z} \mapsto f^k \in \mathcal{S}_{2n}$ . Remarquons que la permutation  $\tilde{f}$  qui est définie par  $\tilde{f}(i) = f(i+1) - 1$  vérifie  $\tilde{f}^k(i) = f^k(i+1) - 1$ . Ainsi, l'équation d'inconnue  $r$ ,  $f^r = id$  est équivalente à  $\tilde{f}^r = id$ . Cela signifie que les permutations  $f$  et  $\tilde{f}$  (et aussi  $f^{-1}$  et  $\tilde{f}^{-1}$ ) ont même période, ce qui est bien sûr naturel puisque le retour à l'ordre initial ne dépend pas du choix de la numérotation. Nous pourrions travailler indifféremment avec  $f$  ou  $\tilde{f}$  selon le cas. Le calcul de cette période – le plus petit  $r \geq 1$  tel que  $f^r = id$  – est précisément l'objet de la deuxième question posée dans l'introduction. Une méthode de calcul est proposée dans les théorèmes 1, 4, 6 et 7 ci-dessous, on peut la trouver e.g. dans les divers livres [3, 8, 16] ainsi que dans les articles [6, 12].

La dernière question posée dans l'introduction concerne la possibilité de retrouver, partant d'une pile de  $2n$  jetons contenant de bas en haut  $n$  jetons verts et  $n$  jetons rouges, une pile visuellement identique, mais éventuellement correspondant à un ordre de jetons (s'ils étaient discernables) différent. Cela revient à déterminer pour la permutation  $f$  le plus petit entier  $r' \geq 1$  tel que

$$f^{r'}(\{1, 2, \dots, n\}) = \{1, 2, \dots, n\}$$

et

$$f^{r'}(\{n+1, n+2, \dots, 2n\}) = \{n+1, n+2, \dots, 2n\}.$$

Une des deux égalités est redondante puisque  $f$  est bijective. Il est clair que  $r' \leq r$ . En fait, l'entier  $r'$  divise la période  $r$ . En effet, en effectuant la division euclidienne de  $r$  par  $r'$ , on a  $r = ar' + b$  pour deux entiers  $a$  et  $b$  tels que  $0 \leq b \leq r' - 1$ . Alors, par définition de  $r$ ,  $f^r = f^{(a+1)r' - (r'-b)} = id$ , donc  $f^{r'-b} = (f^{r'})^{a+1}$  et  $f^{r'-b}$  vérifie  $f^{r'-b}(\{1, 2, \dots, n\}) = \{1, 2, \dots, n\}$ .

Par définition de  $r'$ , comme  $1 \leq r' - b \leq r'$ , on a nécessairement  $b = 0$  et donc  $r'$  divise  $r$ . La recherche de  $r'$  semble délicate, nous ne l'aborderons pas dans ce travail.

### III.1 Cas de l'in-shuffle

**Théorème 1** *La période de l'in-shuffle de  $2n$  cartes est le plus petit entier  $r \geq 1$  vérifiant  $2^r \equiv 1 \pmod{2n+1}$ . En d'autres termes,  $r$  est l'ordre de 2 modulo  $(2n+1)$ .*

DÉMONSTRATION. Rappelons la congruence pour la permutation  $f$  associée à l'in-shuffle :

$$f^{-1}(j) \equiv 2j \pmod{2n+1}.$$

On a alors pour tout  $k \in \mathbb{N}$ ,

$$f^{-k}(j) \equiv 2^k j \pmod{2n+1}.$$

La période de  $f$  est donc le plus petit entier  $r \geq 1$  vérifiant  $2^r \equiv 1 \pmod{2n+1}$ . Notons qu'un tel entier existe effectivement. En effet, en adaptant le raisonnement précédent et en rappelant la notation  $a \bmod n$  qui désigne le reste de la division euclidienne de  $a$  par  $n$ , l'ensemble  $\{2^k \bmod (2n+1), k \in \mathbb{N}\}$  est fini, il existe au moins deux entiers distincts  $k$  et  $l$  tels que  $k < l$  et  $2^k \equiv 2^l \pmod{2n+1}$ . Les nombres 2 et  $(2n+1)$  étant premiers entre eux, 2 est inversible modulo  $(2n+1)$  et on peut donc « diviser » par  $2^k$  pour obtenir  $2^{l-k} \equiv 1 \pmod{2n+1}$  avec  $l-k \geq 1$ . □

REMARQUE. Un théorème d'Euler stipule que, si  $\varphi(2n+1)$  est le nombre d'entiers premiers avec  $2n+1$  compris entre 1 et  $2n+1$  (fonction indicatrice d'Euler), on a  $2^{\varphi(2n+1)} \equiv 1 \pmod{2n+1}$ . Ainsi  $\varphi(2n+1)$  est une période de  $f$ . Lorsque  $2n+1$  est premier,  $\varphi(2n+1) = 2n$  et ceci n'est rien d'autre que le petit théorème de Fermat :  $2^{2n} \equiv 1 \pmod{2n+1}$ .

La discussion précédente montre que l'évolution de la  $i^{\text{e}}$  carte ( $i \in \{1, 2, 3, \dots, 2n\}$ ) est décrite par l'orbite de  $i$  sous l'action de  $f$  (ou de manière équivalente de  $f^{-1}$ ) :

$$\begin{aligned} \mathcal{O}(i) &= \{f^k(i), k \in \mathbb{Z}\} \\ &= \{i, f(i), f^2(i), \dots, f^{r-1}(i)\} \\ &= \{2^k i \bmod (2n+1), 0 \leq k \leq r-1\}. \end{aligned}$$

L'orbite de 1 est en particulier

$$\mathcal{O}(1) = \{2^k \bmod (2n+1), 0 \leq k \leq r-1\}.$$

Par définition de  $r$ , le cardinal de  $\mathcal{O}(1)$  est exactement  $r$  :  $\text{card } \mathcal{O}(1) = r$ . Pour les autres  $i$ , on a  $\text{card } \mathcal{O}(i) \leq r$ . On voit par ailleurs, puisque  $\mathcal{O}(1) \subset \{1, 2, 3, \dots, 2n\}$ , que  $r \leq 2n$ . L'égalité  $r = 2n$  signifie que l'on a une seule orbite : pour tout  $i \in \{1, 2, 3, \dots, 2n\}$ ,

$$\mathcal{O}(i) = \{1, 2, 3, \dots, 2n\}.$$

Dans ce cas, une carte donnée visite toutes les places du jeu avant de revenir à sa position initiale.

#### Proposition 2

- Pour tout  $i \in \{1, 2, \dots, n\}$ , le cardinal de l'orbite de  $i$  est un diviseur de celui de l'orbite de 1 :  $\text{card } \mathcal{O}(i)$  divise  $\text{card } \mathcal{O}(1)$ .
- Dans le cas particulier où  $i$  est un nombre premier avec  $2n+1$ , ces orbites ont même cardinal :  $\text{card } \mathcal{O}(i) = \text{card } \mathcal{O}(1)$ .
- Si  $2n+1$  est premier, toutes les orbites ont même cardinal  $r$  et il y a  $2n/r$  orbites distinctes.

DÉMONSTRATION.

• Introduisons le pgcd des entiers  $i$  et  $2n+1$  :  $d_i = \text{pgcd}(i, 2n+1)$  et posons  $r_i = \text{card } \mathcal{O}(i)$  (on a en particulier  $r_1 = r$ ). Le cardinal  $r_i$  est le plus petit entier strictement positif tel que  $2^{r_i} i \equiv i \pmod{2n+1}$ . Cette dernière égalité est équivalente à l'assertion «  $(2n+1)$  divise  $i(2^{r_i} - 1)$  », ou encore «  $(2n+1)/d_i$  divise  $(i/d_i)(2^{r_i} - 1)$  ». Par définition de  $d_i$ , les entiers  $i/d_i$  et  $m_i = (2n+1)/d_i$  sont premiers entre eux, ce qui montre que  $m_i$  divise  $2^{r_i} - 1$ . On voit ainsi que  $r_i = \min\{k \in \mathbb{N}^* : 2^k \equiv 1 \pmod{m_i}\}$ . Prouvons que  $r_i$  divise  $r$ . Comme  $m_i$  divise  $2n+1$ , on a l'implication  $x \equiv y \pmod{2n+1} \implies x \equiv y \pmod{m_i}$ ; on peut alors définir de manière cohérente, entre les groupes multiplicatifs

$$\mathcal{O}(1) = \{2^k \bmod (2n+1), 0 \leq k \leq r-1\}$$

et

$$G_i = \{2^k \bmod m_i, 0 \leq k \leq r_i-1\},$$

un morphisme

$$\phi_i : \begin{array}{ccc} \mathcal{O}(1) & \longrightarrow & G_i \\ 2^k \bmod (2n+1) & \longmapsto & 2^k \bmod m_i \end{array}$$

qui est clairement surjectif. Les groupes  $\mathcal{O}(1)/\ker \phi_i$  et  $G_i$  sont donc isomorphes ce qui montre bien que  $\text{card}(G_i)$  (qui vaut  $r_i$ ) divise  $\text{card } \mathcal{O}(1)$ .

- Lorsque  $i$  est premier avec  $2n+1$ ,  $i$  est

inversible modulo  $(2n + 1)$  et l'application de multiplication par  $i$

$$\begin{aligned} \mathcal{O}(1) &\longrightarrow \mathcal{O}(i) \\ 2^k \bmod (2n + 1) &\longmapsto 2^k i \bmod (2n + 1) \end{aligned}$$

est une bijection entre les orbites  $\mathcal{O}(1)$  et  $\mathcal{O}(i)$ . Les orbites de 1 et de  $i$  ont donc même cardinal (qui vaut  $r$ ).

• Enfin, si  $2n + 1$  est un nombre premier, tout  $i \in \{1, 2, \dots, 2n\}$  est premier avec  $2n + 1$  et donc  $r_i = r$ . La réunion des différentes orbites coïncidant avec  $\{1, 2, \dots, 2n\}$ , il y a alors  $2n/r$  orbites distinctes.  $\square$

EXEMPLE. *Cas d'un jeu de 52 cartes (quatre séries de cartes numérotées de 2 à 10, valet, dame, roi, as, de couleurs carreau, pique, cœur, trèfle).* Ce cas correspond à  $n = 26$ . L'étude de l'in-shuffle de ce jeu s'effectue modulo  $2n + 1 = 53$  qui est premier. En renumérotant toutes les cartes de 1 à 52, il y a une seule orbite :  $\mathcal{O}(1) = \{1, 2, 3, \dots, 52\}$  et l'in-shuffle est de période 52.

EXEMPLE. *Cas d'un jeu de 54 cartes (jeu précédent avec deux jokers différents).* Ce cas correspond à  $n = 27$ . L'étude de l'in-shuffle de ce mélange se mène modulo  $2n + 1 = 55$ . On trouve, en renumérotant toutes les cartes de 1 à 54, quatre orbites distinctes :

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 4, 7, 8, 9, 13, 14, 16, 17, \\ &\quad 18, 26, 28, 31, 32, 34, 36, 43, 49, 52\}, \\ \mathcal{O}(3) &= \{3, 6, 12, 19, 21, 23, 24, 27, 29, 37, \\ &\quad 38, 39, 41, 42, 46, 47, 48, 51, 53, 54\}, \\ \mathcal{O}(5) &= \{5, 10, 15, 20, 25, 30, 35, 40, 45, 50\}, \\ \mathcal{O}(11) &= \{11, 22, 33, 44\}. \end{aligned}$$

On vérifie que les cardinaux de  $\mathcal{O}(3)$ ,  $\mathcal{O}(5)$ ,  $\mathcal{O}(11)$ , valant respectivement 20, 10, 4, divisent le cardinal de  $\mathcal{O}(1)$  qui vaut 20. Ainsi, l'in-shuffle est de période 20.

### Corollaire 3

- La période de l'in-shuffle d'un jeu de  $2^p$  cartes ( $p \geq 1$ ) est  $2p$ .
- La période de l'in-shuffle d'un jeu de  $2^p - 2$  cartes ( $p \geq 2$ ) est  $p$ .

DÉMONSTRATION. Écrivons l'orbite de 1.

• Si  $n = 2^{p-1}$ , alors  $2n + 1 = 2^p + 1$ . On voit que  $2^p \equiv -1 \pmod{(2n + 1)}$ , puis, en élevant au carré, que  $2^{2p} \equiv 1 \pmod{(2n + 1)}$ . D'après

le théorème 1, on tire que  $2p$  est une période de l'in-shuffle. On a ensuite, pour tout  $k \in \{p, p + 1, \dots, 2p\}$ ,  $2^k \equiv 2^p - 2^{k-p} + 1 \pmod{(2n + 1)}$  avec l'encadrement  $1 \leq 2^p - 2^{k-p} + 1 \leq 2n$ . L'orbite de 1 est dans ce cas

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 2^2, \dots, 2^{p-1}, 2^p, \\ &\quad 2^{p+1} \bmod (2n + 1), 2^{p+2} \bmod (2n + 1), \\ &\quad \dots, 2^{2p-1} \bmod (2n + 1)\} \\ &= \{1, 2, 2^2, \dots, 2^{p-1}, 2^p, \\ &\quad 2^p - 1, 2^p - 3, \dots, 2^p - 2^{p-1} + 1\} \\ &= \{2^k, 0 \leq k \leq p - 1\} \\ &\quad \cup \{2^p - 2^k + 1, 0 \leq k \leq p - 1\}. \end{aligned}$$

On constate que  $\text{card } \mathcal{O}(1) = 2p$  et donc que  $2p$  est la période de l'in-shuffle.

• Si  $n = 2^{p-1} - 1$ , alors  $2n + 1 = 2^p - 1$  et donc  $2^p \equiv 1 \pmod{(2n + 1)}$ . Cette fois, l'orbite de 1 est donnée par

$$\mathcal{O}(1) = \{1, 2, 2^2, \dots, 2^{p-1}\}$$

et l'on obtient  $\text{card } \mathcal{O}(1) = p$ . Le nombre  $p$  est la période de l'in-shuffle.  $\square$

REMARQUE. D'après la remarque suivant le théorème 1, on a prouvé au passage que  $p$  divise  $\varphi(2^p - 1)$  et  $2p$  divise  $\varphi(2^p + 1)$ .

EXEMPLE. *Cas d'un jeu de 32 cartes (quatre séries de cartes numérotées de 7 à 10, valet, dame, roi, as, de couleurs carreau, pique, cœur, trèfle).* Ce cas correspond à  $n = 16$  et  $p = 5$ . L'étude de l'in-shuffle de ce jeu se réalise modulo  $2n + 1 = 33$ . En renumérotant les cartes de 1 à 32, l'évolution progressive de la carte n° 1 est décrite selon le cycle

$$\begin{aligned} f^{-1}(1) &= 2, f^{-2}(1) = 4, f^{-3}(1) = 8, f^{-4}(1) = 16, \\ f^{-5}(1) &= 32, f^{-6}(1) = 31, f^{-7}(1) = 29, \\ f^{-8}(1) &= 25, f^{-9}(1) = 17, f^{-10}(1) = 1. \end{aligned}$$

Plus généralement, on trouve quatre orbites distinctes :

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 4, 8, 16, 17, 25, 29, 31, 32\}, \\ \mathcal{O}(3) &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}, \\ \mathcal{O}(5) &= \{5, 7, 10, 13, 14, 19, 20, 23, 26, 28\}, \\ \mathcal{O}(11) &= \{11, 22\}. \end{aligned}$$

On vérifie que les cardinaux de  $\mathcal{O}(3)$ ,  $\mathcal{O}(5)$ ,  $\mathcal{O}(11)$ , valant respectivement 10, 10, 2, divisent le cardinal de  $\mathcal{O}(1)$  qui vaut 10. Ainsi, l'in-shuffle de ce jeu est de période 10 qui coïncide précisément avec  $2p$ .

### III.2 Cas de l'out-shuffle

**Théorème 4** *La période de l'out-shuffle d'un jeu de  $2n$  cartes est le plus petit entier  $s \geq 1$  vérifiant  $2^s \equiv 1 \pmod{2n-1}$ . En d'autres termes,  $s$  est l'ordre de 2 modulo  $(2n-1)$ .*

DÉMONSTRATION. Rappelons la relation remarquable pour la permutation  $\tilde{g}$  associée à l'out-shuffle :

$$\tilde{g}^{-1}(j) \equiv 2j \pmod{2n-1}$$

qui donne pour tout  $k \in \mathbb{N}$ ,

$$\tilde{g}^{-k}(j) \equiv 2^k j \pmod{2n-1}.$$

La période de  $\tilde{g}$  et donc de  $g$  est alors le plus petit entier  $s \geq 1$  vérifiant  $2^s \equiv 1 \pmod{2n-1}$ .  $\square$

REMARQUE. Le théorème 4 découle également du théorème 1 : en effet, il a été observé qu'un out-shuffle de  $2n$  cartes est identique à l'in-shuffle du jeu de  $2(n-1)$  cartes obtenu en retirant les première et dernière cartes.

La discussion précédente montre que l'évolution de la  $i^{\text{e}}$  carte ( $i \in \{0, 1, 2, \dots, 2n-1\}$ ) est décrite par l'orbite de  $i$  sous l'action de  $\tilde{g}$  (ou de manière équivalente de  $\tilde{g}^{-1}$ ) :

$$\begin{aligned} \tilde{O}(i) &= \{\tilde{g}^k(i), k \in \mathbb{Z}\} \\ &= \{i, \tilde{g}(i), \tilde{g}^2(i), \dots, \tilde{g}^{s-1}(i)\} \\ &= \{2^k i \pmod{2n-1}, 0 \leq k \leq s-1\}. \end{aligned}$$

L'orbite de 1 est en particulier

$$\tilde{O}(1) = \{2^k \pmod{2n-1}, 0 \leq k \leq s-1\}.$$

EXEMPLE. *Cas d'un jeu de 52 cartes.* L'étude de l'out-shuffle de ce jeu s'effectue modulo  $2n-1 = 51$ . On trouve, en numérotant les cartes de 0 à 51, les neufs orbites suivantes :

$$\begin{aligned} \tilde{O}(0) &= \{0\}, \\ \tilde{O}(1) &= \{1, 2, 4, 8, 13, 16, 26, 32\}, \\ \tilde{O}(3) &= \{3, 6, 12, 24, 27, 39, 45, 48\}, \\ \tilde{O}(5) &= \{5, 7, 10, 14, 20, 28, 29, 40\}, \\ \tilde{O}(9) &= \{9, 15, 18, 21, 30, 33, 36, 42\}, \\ \tilde{O}(11) &= \{11, 22, 23, 31, 37, 41, 44, 46\}, \\ \tilde{O}(17) &= \{17, 34\}, \\ \tilde{O}(19) &= \{19, 25, 35, 38, 43, 47, 49, 50\}, \\ \tilde{O}(51) &= \{51\}. \end{aligned}$$

Les cardinaux de ces orbites sont 1, 2 ou 8. La période de l'out-shuffle est  $s = 8$ .

EXEMPLE. *Cas d'un jeu de 54 cartes.* L'étude de l'out-shuffle de ce jeu se mène modulo  $2n-1 = 53$  qui est premier. On trouve à présent, en numérotant les cartes de 0 à 53, trois orbites distinctes :

$$\tilde{O}(0) = \{0\}, \quad \tilde{O}(1) = \{1, 2, 3, \dots, 52\}, \quad \tilde{O}(53) = \{53\}.$$

La période dans ce cas est  $s = 52$ .

La remarque suivant le théorème 4 fournit l'analogue suivant du corollaire 3.

#### Corollaire 5

- *La période de l'out-shuffle d'un jeu de  $2^p$  cartes ( $p \geq 1$ ) est  $p$ .*
- *La période de l'out-shuffle d'un jeu de  $2^p + 2$  cartes ( $p \geq 1$ ) est  $2p$ .*

EXEMPLE. *Cas d'un jeu de 32 cartes.* Ce cas correspond à  $n = 16$  et  $p = 5$ . L'étude de l'out-shuffle se réalise modulo  $2n-1 = 31$ . En numérotant les cartes de 0 à 31, l'évolution de la carte  $n^0 1$  est décrite selon le cycle  $\tilde{g}^{-1}(1) = 2, \tilde{g}^{-2}(1) = 4, \tilde{g}^{-3}(1) = 8, \tilde{g}^{-4}(1) = 16, \tilde{g}^{-5}(1) = 1$ . Plus généralement, on trouve huit orbites distinctes :

$$\begin{aligned} \tilde{O}(0) &= \{0\}, \\ \tilde{O}(1) &= \{1, 2, 4, 8, 16\}, \\ \tilde{O}(3) &= \{3, 6, 12, 17, 24\}, \\ \tilde{O}(5) &= \{5, 9, 10, 18, 20\}, \\ \tilde{O}(7) &= \{7, 14, 19, 25, 28\}, \\ \tilde{O}(11) &= \{11, 13, 21, 22, 26\}, \\ \tilde{O}(15) &= \{15, 23, 27, 29, 30\}, \\ \tilde{O}(31) &= \{31\}. \end{aligned}$$

Les cardinaux de ces orbites valent 1 ou 5 et l'out-shuffle de ce jeu est de période 5 qui coïncide précisément avec  $p$ .

### III.3 Cas d'un mélange de Monge

**Théorème 6** *La période commune de  $h_1$  et de  $h_3$  est le plus petit entier  $u \geq 1$  vérifiant l'une des deux congruences  $2^u \equiv 1 \pmod{4n+1}$  ou  $2^u \equiv -1 \pmod{4n+1}$ .*

EXPLICATION DU THÉORÈME. Ou bien il existe une puissance de 2 congrue à  $-1$  modulo  $(4n+1)$

et l'on choisit pour  $u$  la plus petite. Dans ce cas,  $2u$  est l'ordre de 2 modulo  $(4n + 1)$  :  $2^{2u} \equiv 1 \pmod{(4n + 1)}$ . Ou bien il n'existe aucune puissance de 2 congrue à  $-1$  modulo  $(4n + 1)$  et l'on choisit alors pour  $u$  l'ordre de 2 modulo  $(4n + 1)$ .

DÉMONSTRATION. Rappelons tout d'abord que  $h_1$  et  $h_3$  sont conjuguées :  $h_3 = s \circ h_1 \circ s^{-1}$ . Cette propriété s'étend à toutes les itérées :  $h_3^k = s \circ h_1^k \circ s^{-1}$ . Ainsi l'équation  $h_1^k = id$  est équivalente à l'équation  $h_3^k = id$ , prouvant que  $h_1$  et  $h_3$  ont même période. Rappelons la relation

$$h_3^{-1}(j) \equiv \pm 2j \pmod{(4n + 1)}.$$

On a

$$h_3^{-k}(j) \equiv \pm 2^k j \pmod{(4n + 1)},$$

le signe  $\pm$  dépendant de  $j$  et  $k$  est déterminé sans ambiguïté par la contrainte  $1 \leq h_3^{-k}(j) \leq 2n$ . Plus précisément, si  $2^k j$  admet un représentant modulo  $(4n + 1)$  compris entre 1 et  $2n$ , alors  $h_3^{-k}(j)$  coïncide avec ce représentant et on choisit le signe  $+$  dans la congruence :  $h_3^{-k}(j) \equiv +2^k j \pmod{(4n + 1)}$ . Sinon,  $2^k j$  admet un représentant entre  $2n + 1$  et  $4n$  (0 ne peut pas être un représentant car  $2^k$  et  $(4n + 1)$  sont premiers entre eux et  $1 \leq j \leq 2n$ ). Dans ce cas,  $-2^k j$  admet un représentant entre 1 et  $2n$  et l'on choisit le signe  $-$  :  $h_3^{-k}(j) \equiv -2^k j \pmod{(4n + 1)}$ .

Pour avoir en particulier  $h_3^{-k}(1) = 1$ , on doit choisir  $k$  tel que  $2^k \equiv \pm 1 \pmod{(4n + 1)}$ . Considérons donc le plus petit entier  $u \geq 1$  tel que  $2^u \equiv 1 \pmod{(4n + 1)}$  ou  $2^u \equiv -1 \pmod{(4n + 1)}$ . On a ensuite pour tout  $j \in \{1, 2, \dots, 2n\}$ ,  $h_3^{-u}(j) \equiv \pm j \pmod{(4n + 1)}$ , le signe  $\pm$  dépendant de  $j$  et  $u$ . En fait, le représentant de  $-j \pmod{(4n + 1)}$  compris entre 1 et  $4n + 1$  est  $4n + 1 - j$ . Mais ce représentant est supérieur à  $2n$  et la condition  $1 \leq h_3^{-u}(j) \leq 2n$  n'est remplie que dans le cas où  $h_3^{-u}(j) = j$ . Ainsi  $h_3^{-u} = id$  et  $u$  est la période de  $h_3$ .  $\square$

EXEMPLE. *Cas d'un jeu de 52 cartes.* L'étude de ce mélange de Monge s'effectue modulo

$4n + 1 = 105$ . On trouve les orbites suivantes :

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 4, 8, 13, 16, 23, 26, 32, 41, 46, 52\}, \\ \mathcal{O}(3) &= \{3, 6, 9, 12, 18, 24, 27, 33, 36, 39, 48, 51\}, \\ \mathcal{O}(5) &= \{5, 10, 20, 25, 40, 50\}, \\ \mathcal{O}(7) &= \{7, 14, 28, 49\}, \\ \mathcal{O}(11) &= \{11, 17, 19, 22, 29, 31, \\ &\quad 34, 37, 38, 43, 44, 47\}, \\ \mathcal{O}(15) &= \{15, 30, 45\}, \\ \mathcal{O}(21) &= \{21, 42\}, \\ \mathcal{O}(35) &= \{35\}. \end{aligned}$$

Ce mélange a pour période 12.

EXEMPLE. *Cas d'un jeu de 54 cartes.* L'étude de ce mélange de Monge s'effectue modulo  $4n + 1 = 109$ . On trouve les trois orbites suivantes :

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 4, 8, 16, 17, 19, 23, 27, \\ &\quad 32, 33, 34, 38, 41, 43, 45, 46, 54\}, \\ \mathcal{O}(3) &= \{3, 5, 6, 7, 10, 12, 13, 14, 20, \\ &\quad 24, 26, 28, 29, 40, 48, 51, 52, 53\}, \\ \mathcal{O}(9) &= \{9, 11, 15, 18, 21, 22, 25, 30, 31, \\ &\quad 35, 36, 37, 39, 42, 44, 47, 49, 50\}, \end{aligned}$$

Ce mélange a pour période 18.

De manière similaire, la congruence précédemment signalée

$$\tilde{h}_4^{-1}(j) \equiv \pm 2j \pmod{(4n - 1)}$$

fournit la période de  $h_4$ .

**Théorème 7** *La période commune de  $h_2$  et de  $h_4$  est le plus petit entier  $v \geq 1$  vérifiant l'une des deux congruences  $2^v \equiv 1 \pmod{(4n - 1)}$  ou  $2^v \equiv -1 \pmod{(4n - 1)}$ .*

EXEMPLE. *Cas d'un jeu de 52 cartes.* L'étude de ce mélange de Monge s'effectue modulo  $4n - 1 = 103$ . On trouve les deux orbites  $\tilde{\mathcal{O}}(0) = \{0\}$  et  $\tilde{\mathcal{O}}(1) = \{1, 2, 3, \dots, 51\}$ . La période de ce mélange est 51.

EXEMPLE. *Cas d'un jeu de 54 cartes.* L'étude de ce mélange de Monge s'effectue modulo  $4n - 1 = 107$ . On trouve les deux orbites  $\tilde{\mathcal{O}}(0) = \{0\}$  et  $\tilde{\mathcal{O}}(1) = \{1, 2, 3, \dots, 53\}$ . La période de ce mélange est 53.

**Corollaire 8** *La période d'un mélange de Monge de  $2^p$  cartes ( $p \geq 1$ ) est  $p + 1$ .*

DÉMONSTRATION. Pour  $n = 2^{p-1}$ , on a  $4n + 1 = 2^{p+1} + 1$ . Donc  $2^{p+1} \equiv -1 \pmod{(4n + 1)}$  et  $2^{p+1} \equiv 1 \pmod{(4n - 1)}$ . D'après les théorèmes 6 et 7,  $p + 1$  est une période de  $h_1, h_2, h_3$  et  $h_4$ . Dans les deux cas, l'orbite de 1 est l'ensemble  $\{1, 2, 2^2, \dots, 2^p\}$  de cardinal  $p + 1$ , ce qui prouve le corollaire.  $\square$

EXEMPLE. *Cas d'un jeu de 32 cartes.* L'étude du mélange de Monge associé à  $h_3$  s'effectue modulo  $4n + 1 = 65$ . On trouve les orbites suivantes :

$$\begin{aligned} \mathcal{O}(1) &= \{1, 2, 4, 8, 16, 32\}, \\ \mathcal{O}(3) &= \{3, 6, 12, 17, 24, 31\}, \\ \mathcal{O}(5) &= \{5, 10, 15, 20, 25, 30\}, \\ \mathcal{O}(7) &= \{7, 9, 14, 18, 28, 29\}, \\ \mathcal{O}(11) &= \{11, 19, 21, 22, 23, 27\}, \\ \mathcal{O}(13) &= \{13, 26\}. \end{aligned}$$

L'étude du mélange de Monge associé à  $\tilde{h}_4$  s'effectue modulo  $4n - 1 = 63$ . On trouve les orbites suivantes :

$$\begin{aligned} \tilde{\mathcal{O}}(0) &= \{0\}, \\ \tilde{\mathcal{O}}(1) &= \{1, 2, 4, 8, 16, 31\}, \\ \tilde{\mathcal{O}}(3) &= \{3, 6, 12, 15, 24, 30\}, \\ \tilde{\mathcal{O}}(5) &= \{5, 10, 17, 20, 23, 29\}, \\ \tilde{\mathcal{O}}(7) &= \{7, 14, 28\}, \\ \tilde{\mathcal{O}}(9) &= \{9, 18, 27\}, \\ \tilde{\mathcal{O}}(11) &= \{11, 13, 19, 22, 25, 26\}, \\ \tilde{\mathcal{O}}(21) &= \{21\}. \end{aligned}$$

Dans les deux cas, la période est 6 et coïncide bien avec  $p + 1$  (ici  $n = 2^{p-1}$  avec  $p = 5$ ).

### III.4 Quelques valeurs numériques

Nous donnons ci-dessous les périodes des in-shuffles et des mélanges de Monge associés à  $h_1$  et  $h_2$  (baptisés dans le tableau de « in-Monge » et « out-Monge ») pour des jeux de  $2n$  cartes avec  $2n \leq 64$ .

$2n$	2	4	6	8	10	12	14	16
in-shuffle	2	4	3	6	10	12	4	8
in-Monge	2	3	6	4	6	10	14	5
out-Monge	1	3	5	4	9	11	9	5

$2n$	18	20	22	24	26	28	30	32
in-shuffle	18	6	11	20	18	28	5	10
in-Monge	18	10	12	21	26	9	30	6
out-Monge	12	12	7	23	8	20	29	6

$2n$	34	36	38	40	42	44	46	48
in-shuffle	12	36	12	20	14	12	23	21
in-Monge	22	9	30	27	8	11	10	24
out-Monge	33	35	20	39	41	28	12	36

$2n$	50	52	54	56	58	60	62	64
in-shuffle	8	52	20	18	58	60	6	12
in-Monge	50	12	18	14	12	55	50	7
out-Monge	15	51	53	36	44	24	20	7

## IV In-shuffle : cas particuliers

Dans cette partie, nous calculons explicitement les itérations successives de la permutation associée à l'in-shuffle dans les deux cas particuliers  $n = 2^{p-1}$  et  $n = 2^{p-1} - 1$ . L'astuce de calcul consiste à travailler avec les écritures binaires des numéros de cartes.

Nous ne calculerons pas les itérations successives de l'out-shuffle dans les cas  $n = 2^{p-1}$  et  $n = 2^{p-1} + 1$ , l'out-shuffle étant équivalent à l'in-shuffle associé aux cas respectifs  $n = 2^{p-1} - 1$  et  $n = 2^{p-1}$ .

### IV.1 Cas d'un jeu de $2^p$ cartes

Nous nous plaçons dans le cas d'un jeu de  $2^p$  cartes, c'est-à-dire  $n = 2^{p-1}$ . Nous travaillons ici avec  $\tilde{f}$ . Introduisons l'écriture binaire d'un  $i \in \{0, 1, \dots, 2n - 1\}$  :

$$i = \overline{i_{p-1} \dots i_0} = \sum_{k=0}^{p-1} i_k 2^k$$

où les  $i_0, i_1, \dots, i_{p-1}$  sont des bits 0 ou 1. On a en particulier  $n = \underbrace{\overline{10 \dots 0}}_{p-1}$  et  $2n - 1 = \underbrace{\overline{1 \dots 1}}_p$ . Dans

ces conditions, l'image de  $i$  par la permutation  $\tilde{f}$  s'écrit

$$\tilde{f}(i) = \begin{cases} \overline{1i_{p-1} \dots i_1} & \text{si } i_0 = 0, \\ \overline{i_{p-1} \dots i_1} & \text{si } i_0 = 1, \end{cases}$$

soit encore

$$\tilde{f}(i) = \overline{(1 - i_0)i_{p-1} \dots i_1}.$$

#### IV.1.1 Calcul des itérées $\tilde{f}^k(i)$ pour chaque $i$

Avec cette représentation de  $\tilde{f}$ , on voit progressivement que

$$\begin{aligned}\tilde{f}(i) &= \overline{(1-i_0)i_{p-1}\dots i_1}, \\ \tilde{f}^2(i) &= \overline{(1-i_1)(1-i_0)i_{p-1}\dots i_2}\end{aligned}$$

et plus généralement, pour  $0 \leq k \leq p$ ,

$$\tilde{f}^k(i) = \overline{(1-i_{k-1})\dots(1-i_0)i_{p-1}\dots i_k}.$$

Pour  $k = p$ , on obtient

$$\tilde{f}^p(i) = \overline{(1-i_{p-1})\dots(1-i_0)}$$

que l'on peut réécrire

$$\tilde{f}^p(i) = \underbrace{\overline{1-1}}_p - \overline{i_{p-1}\dots i_0} = 2n - 1 - i.$$

Ainsi  $\tilde{f}^p$  est la symétrie des entiers  $0, 1, \dots, 2n-1$ . Cela signifie que dans le cas d'une pile de  $2n$  jetons dont les  $n$  jetons du bas sont verts et les  $n$  du haut sont rouges, on obtient au bout de  $p$  mélanges parfaits une pile inversée : les  $n$  jetons du bas sont rouges et les  $n$  du haut sont verts.

En poursuivant, on trouve pour  $p \leq k \leq 2p$ ,

$$\tilde{f}^k(i) = \overline{i_{k-p-1}\dots i_0(1-i_{p-1})\dots(1-i_{k-p})}$$

pour aboutir finalement à

$$\tilde{f}^{2p}(i) = \overline{i_{p-1}i_{p-2}\dots i_0} = i.$$

On retrouve bien le fait que, dans le cas où  $n = 2^{p-1}$ , le nombre  $2p$  est une période de  $\tilde{f}$  (et aussi de  $f$ ).

#### IV.1.2 Calcul des itérées $\tilde{f}^k(0)$

L'évolution en binaire de la première carte (numéro 0) est intéressante en soi. Les calculs précédents donnent

$$\tilde{f}(0) = \underbrace{\overline{10-0}}_{p-1} = n.$$

Plus généralement, pour  $0 \leq k \leq p$ ,

$$\begin{aligned}\tilde{f}^k(0) &= \overline{\underbrace{1-10-0}_{k \quad p-k}} \\ &= 2^{p-1} + 2^{p-2} + \dots + 2^{p-k} = 2^p - 2^{p-k}\end{aligned}$$

qui conduit à

$$\tilde{f}^p(0) = \underbrace{\overline{1-1}}_p = 2^p - 1 = 2n - 1.$$

Puis, pour  $p \leq k \leq 2p$ ,

$$\tilde{f}^k(0) = \underbrace{\overline{1-1}}_{2p-k} = 2^{2p-k} - 1$$

et finalement  $\tilde{f}^{2p}(0) = 0$ . Ainsi, l'orbite de 0 sous l'action de  $\tilde{f}$  est

$$\begin{aligned}\tilde{\mathcal{O}}(0) &= \{2^p - 2^{p-k}, 1 \leq k \leq p\} \\ &\cup \{2^{2p-k} - 1, p \leq k \leq 2p-1\} \\ &= \{2^k - 1, 1 \leq k \leq p\} \\ &\cup \{2^p - 2^k, 1 \leq k \leq p\}.\end{aligned}$$

On voit que  $\text{card } \tilde{\mathcal{O}}(0) = 2p$ . Le nombre  $2p$  est bien la période de  $\tilde{f}$ .

## IV.2 Cas d'un jeu de $2^p - 2$ cartes

Nous nous plaçons dans le cas où  $n = 2^{p-1} - 1$ . Nous travaillons ici avec  $f$ . Introduisons de nouveau l'écriture binaire d'un  $i \in \{1, 2, \dots, 2n\}$  :  $i = \overline{i_{p-1}\dots i_0}$ . On a  $n+1 = 2^{p-1} = \underbrace{\overline{10-0}}_{p-1}$ . Dans

ces conditions, l'image de  $i$  par la permutation  $f$  s'écrit

$$f(i) = \begin{cases} \overline{i_{p-1}\dots i_1} & \text{si } i_0 = 0, \\ \overline{1i_{p-1}\dots i_1} & \text{si } i_0 = 1, \end{cases}$$

soit encore

$$f(i) = \overline{i_0i_{p-1}\dots i_1}.$$

Dans ce cas, la permutation  $f$  correspond à une simple permutation circulaire des chiffres de la décomposition binaire de la variable :  $(i_0, i_1, \dots, i_{p-1}) \mapsto (i_1, i_2, \dots, i_{p-1}, i_0)$ .

#### IV.2.1 Calcul des itérées $f^k(i)$ pour chaque $i$

On obtient immédiatement, pour  $0 \leq k \leq p$ ,

$$f^k(i) = \overline{i_{k-1}i_{k-2}\dots i_0i_{p-1}\dots i_k}.$$

Finalement pour  $k = p$  :

$$f^p(i) = \overline{i_{p-1}i_{p-2}\dots i_0} = i.$$

Ce procédé est signalé dans [1, 5]. On retrouve le fait que, dans le cas où  $n = 2^{p-1} - 1$ ,  $p$  est une période de  $f$ .

## IV.2.2 Calcul des itérées $f^k(1)$

Examinons l'évolution binaire de la première carte (n° 1) : la permutation circulaire des chiffres donne

$$f(1) = \overbrace{10-0}^{p-1} = 2^{p-1} = n + 1,$$

puis, pour  $0 \leq k \leq p$ ,

$$f^k(1) = \overbrace{10-0}^{p-k} = 2^{p-k}.$$

On arrive finalement à  $f^p(1) = 1$  et  $p$  est bien la période de  $f$ .

## V Mélange de Monge : cas d'un jeu de $2^p$ cartes

Dans toute cette section, nous nous plaçons dans le cas où  $n = 2^{p-1}$ .

### V.1 Version associée à $h_1$

Nous travaillons ici avec la permutation  $\tilde{h}_1$  des entiers  $0, 1, \dots, 2n - 1$ . On a, pour  $i = i_{p-1} \dots i_0$ ,

$$\tilde{h}_1(i) = \begin{cases} \overline{(1-i_0)i_{p-1} \dots i_1} & \text{si } i_0 = 0, \\ \overline{(1-i_0)(1-i_{p-1}) \dots (1-i_1)} & \text{si } i_0 = 1. \end{cases}$$

L'expression de  $\tilde{h}_1(i)$  ci-dessus dépendant de la parité de  $i$ , nous sommes amenés à décomposer l'écriture binaire de  $i$  en blocs de 0 et de 1 consécutifs. Notons  $m$  ( $m \geq 1$ ) le nombre de blocs apparaissant dans  $i$  et  $l_1, l_2, \dots, l_m$  leurs longueurs respectives en partant de la droite vers la gauche ( $l_1, \dots, l_m \geq 1$  et  $l_1 + \dots + l_m = p$ ). Pour  $m = 1$ , on a les deux possibilités  $i = \overline{0-0}$  et  $i = \overline{1-1}$ . Pour  $m \geq 2$ , on a les quatre possibilités génériques :

$$i = \overbrace{\overbrace{0-01-1}^{l_m} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1}}$$

$$i = \overbrace{\overbrace{0-01-1}^{l_m} \dots \overbrace{0-01-1}^{l_2} \overbrace{0-01-1}^{l_1}}$$

$$i = \overbrace{\overbrace{1-10-0}^{l_m} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1}}$$

$$i = \overbrace{\overbrace{1-10-0}^{l_m} \dots \overbrace{0-01-1}^{l_2} \overbrace{0-01-1}^{l_1}}$$

### V.1.1 Calcul des itérées $\tilde{h}_1^k(i)$ pour chaque $i$

Nous considérons par exemple le cas d'un nombre  $i$  se décomposant sous la forme

$$i = \overbrace{\overbrace{1-10-0}^{l_m} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1}}$$

On a

$$\tilde{h}_1(i) = \overbrace{\overbrace{1-10-0}^{l_m+1} \overbrace{1-10-0}^{l_{m-1}} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1-1}}$$

$$\tilde{h}_1^{l_1}(i) = \overbrace{\overbrace{1-10-0}^{l_m+l_1} \overbrace{1-10-0}^{l_{m-1}} \dots \overbrace{1-1}^{l_2}}$$

puis

$$\tilde{h}_1^{l_1+1}(i) = \overbrace{\overbrace{0-0}^{l_m+l_1+1} \overbrace{1-1}^{l_{m-1}} \dots \overbrace{0-0}^{l_2-1}}$$

$$\tilde{h}_1^{l_1+2}(i) = \overbrace{\overbrace{1-0-0}^{l_m+l_1+1} \overbrace{1-1}^{l_{m-1}} \dots \overbrace{0-0}^{l_2-2}}$$

$$\tilde{h}_1^{l_1+l_2}(i) = \overbrace{\overbrace{1-1}^{l_2-1} \overbrace{0-0}^{l_m+l_1+1} \overbrace{1-1}^{l_{m-1}} \dots \overbrace{1-1}^{l_3}}$$

puis

$$\tilde{h}_1^{l_1+l_2+1}(i) = \overbrace{\overbrace{0-0}^{l_2} \overbrace{1-1}^{l_m+l_1+1} \overbrace{0-0}^{l_{m-1}} \dots \overbrace{0-0}^{l_3-1}}$$

$$\tilde{h}_1^{l_1+l_2+l_3}(i) = \overbrace{\overbrace{1-10-0}^{l_3-1} \overbrace{1-1}^{l_2} \overbrace{0-0}^{l_m+l_1+1} \overbrace{1-1}^{l_{m-1}} \dots \overbrace{1-1}^{l_4}}$$

On continue ainsi de suite pour arriver à

$$\tilde{h}_1^{l_1+\dots+l_{m-1}}(i) = \overbrace{\overbrace{1-1}^{l_{m-1}-1} \overbrace{0-0}^{l_{m-2}} \dots \overbrace{0-0}^{l_2} \overbrace{1-1}^{l_m+l_1+1}}$$

$$\tilde{h}_1^{l_1+\dots+l_{m-1}+1}(i) = \overbrace{\overbrace{0-01-1}^{l_{m-1}} \overbrace{1-1}^{l_{m-2}} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_m+l_1}}$$

$$\tilde{h}_1^{l_1+\dots+l_m+1}(i) = \overbrace{\overbrace{1-10-0}^{l_m} \overbrace{1-10-0}^{l_{m-1}} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1}}$$

Finalement, le résultat de la dernière étape s'écrit exactement

$$\tilde{h}_1^{p+1}(i) = i.$$

Les calculs menés ci-dessus s'étendent aisément aux autres formes possibles de décompositions binaires par blocs de  $i$  quitte à faire  $l_1 = 0$  ou/et  $l_m = 0$ .

### V.1.2 Calcul des itérées $\tilde{h}_1^k(0)$

Les calculs de la section précédente donnent en particulier les itérations successives de  $\tilde{h}_1$  en 0 :

$$\tilde{h}_1(0) = \overbrace{10-0}^{p-1} = n, \quad \tilde{h}_1^2(0) = \overbrace{110-0}^{p-2}.$$

Plus généralement, on a pour  $0 \leq k \leq p$ ,

$$\tilde{h}_1^k(0) = \overbrace{1-10-0}^k \overbrace{0}^{p-k}$$

jusqu'à

$$\tilde{h}_1^p(0) = \overbrace{1-1}^p = 2n-1$$

et enfin  $\tilde{h}_1^{p+1}(0) = 0$ .

## V.2 Version associée à $h_2$

En ce qui concerne la permutation  $\tilde{h}_2$  des entiers  $0, 1, \dots, 2n-1$ , on a pour  $i = \overline{i_{p-1} \dots i_0}$ ,

$$\tilde{h}_2(i) = \begin{cases} \overline{i_0(1-i_{p-1}) \dots (1-i_1)} & \text{si } i_0 = 0, \\ \overline{i_0 i_{p-1} \dots i_1} & \text{si } i_0 = 1, \end{cases}$$

### V.2.1 Calcul des itérées $\tilde{h}_2^k(i)$ pour chaque $i$

Considérons de nouveau l'exemple où

$$i = \overbrace{1-10-0}^{l_m} \overbrace{\dots}^{l_{m-1}} \overbrace{1-10-0}^{l_2} \overbrace{0}^{l_1}.$$

On a

$$\begin{aligned} \tilde{h}_2(i) &= \overbrace{0-01-1}^{l_{m+1}} \overbrace{\dots}^{l_{m-1}} \overbrace{0-01-1}^{l_2} \overbrace{0}^{l_1-1} \\ \tilde{h}_2^2(i) &= \overbrace{10-01-1}^{l_{m+1}} \overbrace{\dots}^{l_{m-1}} \overbrace{0-01-1}^{l_2} \overbrace{0}^{l_1-2} \\ &\vdots \\ \tilde{h}_2^{l_1}(i) &= \overbrace{1-10-01-1}^{l_{l_1-1}} \overbrace{\dots}^{l_{m+1}} \overbrace{0-0}^{l_{l_1-1}} \overbrace{0}^{l_2} \end{aligned}$$

puis

$$\begin{aligned} \tilde{h}_2^{l_1+1}(i) &= \overbrace{0-01-10-0}^{l_1} \overbrace{\dots}^{l_{m+1}} \overbrace{1-1}^{l_{l_1-1}} \\ &\vdots \\ \tilde{h}_2^{l_1+l_2}(i) &= \overbrace{1-10-01-10-0}^{l_2-1} \overbrace{\dots}^{l_1} \overbrace{0-0}^{l_{m+1}} \overbrace{0}^{l_{m-1}} \overbrace{0}^{l_3} \end{aligned}$$

puis

$$\begin{aligned} \tilde{h}_2^{l_1+l_2+1}(i) &= \overbrace{0-01-10-01-1}^{l_2} \overbrace{\dots}^{l_1} \overbrace{1-1}^{l_{m+1}} \overbrace{0}^{l_{m-1}} \overbrace{0}^{l_3-1} \\ &\vdots \\ \tilde{h}_2^{l_1+l_2+l_3}(i) &= \overbrace{1-10-01-10-01-1}^{l_3-1} \overbrace{\dots}^{l_2} \overbrace{0-0}^{l_1} \overbrace{0}^{l_{m+1}} \overbrace{0}^{l_{m-1}} \overbrace{0}^{l_4} \end{aligned}$$

On continue ainsi de suite pour arriver à

$$\begin{aligned} \tilde{h}_2^{l_1+\dots+l_{m-1}}(i) &= \overbrace{1-10-0}^{l_{m-1}-1} \overbrace{\dots}^{l_{m-2}} \overbrace{1-10-0}^{l_1} \overbrace{0}^{l_{m+1}} \\ \tilde{h}_2^{l_1+\dots+l_{m-1}+1}(i) &= \overbrace{0-01-1}^{l_{m-1}} \overbrace{\dots}^{l_{m-2}} \overbrace{0-01-1}^{l_1} \overbrace{0}^{l_m} \\ &\vdots \\ \tilde{h}_2^{l_1+\dots+l_m}(i) &= \overbrace{1-10-0}^{l_{m-1}} \overbrace{\dots}^{l_{m-1}} \overbrace{0-01}^{l_1} \\ \tilde{h}_2^{l_1+\dots+l_m+1}(i) &= \overbrace{1-10-0}^{l_m} \overbrace{\dots}^{l_{m-1}} \overbrace{1-10-0}^{l_2} \overbrace{0}^{l_1} \end{aligned}$$

Finalement, la dernière étape donne exactement

$$\tilde{h}_2^{p+1}(i) = i.$$

### V.2.2 Calcul des itérées $\tilde{h}_2^k(0)$

Les itérations successives de  $\tilde{h}_2$  en 0 s'écrivent

$$\tilde{h}_2(0) = \overbrace{01-1}^{p-1} = n-1, \quad \tilde{h}_2^2(0) = \overbrace{101-1}^{p-2}.$$

Plus généralement, on a pour  $0 \leq k \leq p$ ,

$$\tilde{h}_2^k(0) = \overbrace{1-101-1}^{k-1} \overbrace{0}^{p-k}$$

jusqu'à

$$\tilde{h}_2^p(0) = \overbrace{1-10}^{p-1} = 2n-2$$

et enfin  $\tilde{h}_2^{p+1}(0) = 0$ .

## VI Cas d'un jeu contenant un nombre impair de cartes

On considère ici rapidement le cas d'un jeu de  $2n+1$  cartes, cas étudié dans [12]. Dans cette situation, le coupage de ce jeu en deux parties peut se faire de deux manières : soit à la  $n^e$  carte, soit à la  $(n+1)^e$ . En d'autres termes, après coupage, le premier paquet contient  $n$  cartes et le deuxième en contient  $n+1$ , ou bien le premier paquet contient

$n + 1$  cartes et le deuxième en contient  $n$ . On intercale alors le paquet de  $n$  cartes dans celui de  $n + 1$ .

Examinons les deux situations possibles.

- *Premier coupage* : le jeu de cartes numérotées dans l'ordre  $1, 2, 3, \dots, 2n, 2n + 1$  est coupé en deux paquets de cartes numérotées  $1, 2, \dots, n$  pour le premier et  $n + 1, n + 2, \dots, 2n, 2n + 1$  pour le deuxième. On constitue un nouveau jeu de  $2n + 1$  cartes en intercalant le premier paquet dans le deuxième, donnant ainsi la suite de cartes  $n^{\text{os}} n + 1, 1, n + 2, 2, \dots, n - 1, 2n, n, 2n + 1$  (voir Fig. 13). On observe que la carte  $n^{\text{o}} (2n + 1)$  reste immobile et qu'en la retirant du jeu, cette manipulation est identique à l'in-shuffle du jeu des  $2n$  cartes restantes.

- *Deuxième coupage* : le jeu de cartes renumérotées dans l'ordre  $0, 1, 2, 3, \dots, 2n$  est coupé à présent en deux paquets de cartes numérotées  $0, 1, 2, \dots, n$  pour le premier et  $n + 1, n + 2, \dots, 2n$  pour le deuxième. On forme un nouveau jeu de  $2n + 1$  cartes en intercalant le deuxième paquet dans le premier, fournissant ainsi la suite de cartes  $n^{\text{os}} 0, n + 1, 1, n + 2, 2, \dots, 2n - 1, n - 1, 2n, n$  (voir Fig. 13). Dans ce cas, la carte  $n^{\text{o}} 0$  reste immobile ; en la retirant du jeu, cette manipulation est identique à l'in-shuffle du jeu des  $2n$  cartes restantes.

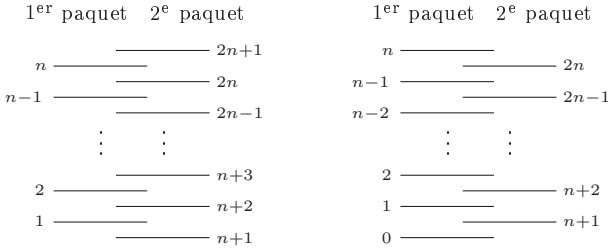


FIG. 13 – Jeu à un nombre impair de cartes

En conclusion, on a le résultat suivant.

**Théorème 9** *La période du mélange parfait de  $2n + 1$  cartes est l'ordre de 2 modulo  $(2n + 1)$ .*

## VII Déplacement d'une carte vers une position donnée dans le cas d'un jeu de $2^p$ cartes

Dans cette section, nous considérons le problème d'Elmsley consistant à déterminer une suc-

cession d'in- et d'out-shuffles déplaçant une carte donnée à une position donnée. Nous nous plaçons dans le cas simple d'un jeu de  $2^p$  cartes ( $p \geq 1$ ) et renvoyons le lecteur à [4] où une procédure algorithmique est proposée dans le cas général. Les cartes sont numérotées de bas en haut  $0, 1, 2, \dots, 2^p - 1$ .

### VII.1 Procédure générale

Rappelons que les déplacements de la carte  $n^{\text{o}} j$  où  $j = \overline{j_{p-1} \dots j_0}$ , par un in- et un out-shuffles sont représentés, en posant pour simplifier les notations  $\tilde{f}^{-1} = \mathfrak{f}$  et  $\tilde{g}^{-1} = \mathfrak{g}$ , par

$$\begin{aligned} \mathfrak{f}(j) &= \overline{j_{p-2} \dots j_0 (1 - j_{p-1})}, \\ \mathfrak{g}(j) &= \overline{j_{p-2} \dots j_0 j_{p-1}}. \end{aligned}$$

Si l'on effectue consécutivement  $k_1$  in-,  $k_2$  out-,  $k_3$  in-,  $k_4$  out-,  $\dots$ ,  $k_{m-1}$  in- et  $k_m$  out-shuffles où  $k_1, k_2, \dots, k_m$  sont des nombres positifs (éventuellement  $k_1, k_m$  pouvant être nuls) de somme  $p$ , la carte  $n^{\text{o}} j$  se retrouve à la position de numéro

$$i = (\mathfrak{g}^{k_m} \circ \mathfrak{f}^{k_{m-1}} \circ \dots \circ \mathfrak{g}^{k_4} \circ \mathfrak{f}^{k_3} \circ \mathfrak{g}^{k_2} \circ \mathfrak{f}^{k_1})(j).$$

Déterminons explicitement l'écriture binaire du numéro  $i$ . On a

$$\mathfrak{f}^{k_1}(j) = \overline{j_{p-k_1-1} \dots j_0 (1 - j_{p-1}) \dots (1 - j_{p-k_1})}$$

puis

$$\begin{aligned} (\mathfrak{g}^{k_2} \circ \mathfrak{f}^{k_1})(j) &= \overline{j_{p-k_1-k_2-1} \dots j_0} \\ &= \overline{(1 - j_{p-1}) \dots (1 - j_{p-k_1}) j_{p-k_1-1} \dots j_{p-k_1-k_2}} \end{aligned}$$

puis

$$\begin{aligned} (\mathfrak{f}^{k_3} \circ \mathfrak{g}^{k_2} \circ \mathfrak{f}^{k_1})(j) &= \overline{j_{p-k_1-k_2-k_3-1} \dots j_0} \\ &= \overline{(1 - j_{p-1}) \dots (1 - j_{p-k_1})} \\ &= \overline{j_{p-k_1-1} \dots j_{p-k_1-k_2}} \\ &= \overline{(1 - j_{p-k_1-k_2-1}) \dots (1 - j_{p-k_1-k_2-k_3})}. \end{aligned}$$

De proche en proche, on arrive à

$$\begin{aligned} (\mathfrak{f}^{k_{m-1}} \circ \mathfrak{g}^{k_{m-2}} \circ \dots \circ \mathfrak{g}^{k_2} \circ \mathfrak{f}^{k_1})(j) &= \overline{j_{p-k_1-\dots-k_{m-1}-1} \dots j_0} \\ &= \overline{(1 - j_{p-1}) \dots (1 - j_{p-k_1}) j_{p-k_1-1} \dots j_{p-k_1-k_2}} \\ &\dots \\ &= \overline{(1 - j_{p-k_1-\dots-k_{m-2}-1}) \dots (1 - j_{p-k_1-\dots-k_{m-1}})} \end{aligned}$$

$$= \frac{\overline{j_{k_m-1} \dots j_0(1-j_{p-1}) \dots (1-j_{p-k_1})}}{\overline{j_{p-k_1-1} \dots j_{p-k_1-k_2}}} \dots \overline{(1-j_{k_m+k_{m-1}-1}) \dots (1-j_{k_m})}$$

et enfin à

$$\begin{aligned} & (\mathfrak{g}^{k_m} \circ \mathfrak{f}^{k_{m-1}} \circ \dots \circ \mathfrak{g}^{k_2} \circ \mathfrak{f}^{k_1})(j) \\ &= \frac{\overline{(1-j_{p-1}) \dots (1-j_{p-k_1}) \underbrace{j_{p-k_1-1} \dots j_{p-k_1-k_2}}_{k_2}}}{\dots} \dots \frac{\overline{(1-j_{k_m+k_{m-1}-1}) \dots (1-j_{k_m}) \underbrace{j_{k_m-1} \dots j_0}_{k_m}}}{\dots} \end{aligned}$$

En d'autres termes, les bits de  $i$  coïncident avec les bits de  $j$  ou leur complémentaire (le complémentaire d'un bit  $j$  étant  $1-j$ ) selon la règle suivante : de gauche à droite,

- les  $k_1$  premiers bits de  $i$  sont les complémentaires de ceux des  $k_1$  premiers de  $j$ ,
- les  $k_2$  bits de  $i$  suivants sont identiques aux  $k_2$  suivants de  $j$ ,
- les  $k_3$  bits de  $i$  suivants sont les complémentaires des  $k_3$  suivants de  $j$ ,
- les  $k_4$  bits de  $i$  suivants sont identiques aux  $k_4$  suivants de  $j$ ,
- etc.

Ce calcul permet d'élaborer un algorithme pour déplacer une carte de numéro donné  $j$  vers une position de numéro donné  $i$  ( $i \neq j$ ). On décompose  $i$  et  $j$  en écriture binaire :  $i = \overline{i_{p-1} \dots i_0}$  et  $j = \overline{j_{p-1} \dots j_0}$ . Puis on compare les bits de  $i$  et  $j$  situé à chaque même place et l'on fait apparaître dans  $i$  des blocs de bits successifs identiques à ceux de  $j$  et des blocs de bits successifs complémentaires à ceux de  $j$ . On décompose ainsi  $i$  en « blocs de coïncidence » et « blocs de complémentarité » avec ceux de  $j$ . Plus précisément, en introduisant la suite des longueurs de ces blocs

$$\begin{aligned} \lambda_1 &= \min\{k \geq 0 : i_k = 1 - j_k\}, \\ \lambda_2 &= \min\{k \geq \lambda_1 : i_{k+\lambda_1} = j_{k+\lambda_1}\}, \\ \lambda_3 &= \min\{k \geq \lambda_2 : i_{k+\lambda_2} = 1 - j_{k+\lambda_2}\}, \\ \lambda_4 &= \min\{k \geq \lambda_3 : i_{k+\lambda_3} = j_{k+\lambda_3}\}, \\ &\vdots \end{aligned}$$

on a, s'il y a  $m$  tels blocs ( $\lambda_1 + \dots + \lambda_m = p$  avec  $\lambda_1, \lambda_m \geq 0$  et  $\lambda_2, \dots, \lambda_{m-1} \geq 1$ ),

$$i = \underbrace{\overline{(1-j_{p-1}) \dots (1-j_{p-\lambda_m})}}_{\lambda_m}$$

$$\begin{aligned} & \frac{\overline{j_{p-\lambda_m-1} \dots j_{p-\lambda_m-\lambda_{m-1}}}}{\dots} \dots \frac{\overline{(1-j_{\lambda_1+\lambda_2-1}) \dots (1-j_{\lambda_1})}}{\lambda_2} \\ & \frac{\overline{j_{\lambda_1-1} \dots j_0}}{\lambda_1} \end{aligned}$$

Les calculs précédents montrent, en choisissant  $k_1 = \lambda_m, k_2 = \lambda_{m-1}, \dots, k_m = \lambda_1$ , que

$$(\mathfrak{g}^{\lambda_1} \circ \mathfrak{f}^{\lambda_2} \circ \dots \circ \mathfrak{g}^{\lambda_{m-1}} \circ \mathfrak{f}^{\lambda_m})(j) = i.$$

Cela indique que  $\lambda_m$  in-,  $\lambda_{m-1}$  out-,  $\dots$ ,  $\lambda_2$  in- et  $\lambda_1$  out-shuffles mènent la carte n°  $j$  à la position n°  $i$ . En d'autres termes, le procédé recherché se schématise selon la succession suivante (de gauche à droite) :

$$\underbrace{I - IO - O}_{\lambda_m} \dots \underbrace{I - IO - O}_{\lambda_1}.$$

D'un point de vue pratique, on effectue un out-shuffle chaque fois que l'on rencontre, dans la lecture de gauche à droite des écritures binaires de  $i$  et  $j$ , une coïncidence de bits et un in-shuffle lorsque l'on rencontre une complémentarité de bits. Notons que les numéros  $i$  et  $j$  jouent un rôle symétrique dans cette analyse. Ainsi, ce processus qui déplace la carte n°  $j$  à la place n°  $i$  déplace également la carte n°  $i$  à la position n°  $j$ .

EXEMPLE. Considérons le cas d'un jeu de 32 cartes numérotées  $0, 1, 2, \dots, 31$ . On souhaite déplacer la carte n° 19 vers la position n° 7. On écrit les nombres 7 et 19 en binaire  $7 = \overline{00111}$  et  $19 = \overline{10011}$ , on superpose les deux séries de bits et on compare les paires de bits verticaux. Lorsque l'on a une paire de bits identiques, on inscrit un out-shuffle ; lorsque l'on a une paire de bits différents, on inscrit un in-shuffle. Cela donne concrètement :

0	0	1	1	1
1	0	0	1	1
-	-	-	-	-
I	O	I	O	O

L'algorithme pour amener la carte n° 19 à la place n° 7 est schématisé par la succession d'in- et d'out-shuffles  $IOIOO$ , soit :  $\mathfrak{f}(19) = 6$ ,  $\mathfrak{g}(6) = 12$ ,  $\mathfrak{f}(12) = 25$ ,  $\mathfrak{g}(25) = 19$ ,  $\mathfrak{g}(19) = 7$ . Globalement,

$$(\mathfrak{g}^2 \circ \mathfrak{f} \circ \mathfrak{g} \circ \mathfrak{f})(19) = 7.$$

L'algorithme pour amener la carte n° 7 à la place n° 19 est le même :  $f(7) = 15$ ,  $g(15) = 30$ ,  $f(30) = 28$ ,  $g(28) = 25$ ,  $g(25) = 19$ , qui donne

$$(g^2 \circ f \circ g \circ f)(7) = 19.$$

On observe que cette procédure est loin d'être optimale dans le premier cas puisque seul un out-shuffle suffit à déplacer la carte n° 19 vers la position n° 7 :  $g(19) = 7$ ... Néanmoins, elle a l'avantage de fonctionner systématiquement. D'ailleurs dans le deuxième cas, nous avons vérifié à l'aide de Maple qu'aucune composition de moins de cinq in-/out-shuffles ne permettait la manipulation requise ; dans ce cas, l'algorithme se révèle optimal. Dans [4], les auteurs proposent un algorithme minimal pour exécuter le déplacement souhaité et cet algorithme est valable dans le cas d'un jeu contenant un nombre quelconque de cartes.

## VII.2 Déplacement de la carte du dessous du paquet vers une position donnée

Examinons le déplacement de la carte du dessous du paquet, i.e. la carte n° 0, vers la position donnée n°  $i$ . Les calculs précédents donnent immédiatement

$$\begin{aligned} (g^{k_m} \circ f^{k_{m-1}} \circ \dots \circ g^{k_2} \circ f^{k_1})(0) \\ = \overbrace{\overbrace{1-10-0}^{k_1} \dots \overbrace{1-10-0}^{k_{m-1}} \overbrace{1-10-0}^{k_m}} \end{aligned}$$

Introduisons la décomposition binaire de  $i$  par blocs

$$i = \overbrace{\overbrace{1-10-0}^{l_m} \dots \overbrace{1-10-0}^{l_2} \overbrace{1-10-0}^{l_1}}$$

où les  $l_1, \dots, l_m$  sont les longueurs positives des blocs de bits de  $i$  lus de droite à gauche. Éventuellement, on posera  $l_m = 0$  si la décomposition démarre par un bloc de 0 et  $l_1 = 0$  si elle finit par un bloc de 1. La règle précédente nous enseigne que

$$(g^{l_1} \circ f^{l_2} \circ \dots \circ g^{l_{m-1}} \circ f^{l_m})(0) = i.$$

Dans le cas où  $l_m = 0$ , c'est-à-dire dans le cas où la décomposition de  $i$  commence par un bloc de 0, puisque  $g(0) = 0$  (un out-shuffle n'affecte pas la carte n° 0), on peut retirer la manipulation redondante  $g^{l_{m-1}}$  ci-dessus pour obtenir

$$(g^{l_1} \circ f^{l_2} \circ \dots \circ g^{l_{m-3}} \circ f^{l_{m-2}})(0) = i.$$

Ainsi, en effectuant successivement  $l_m$  in-,  $l_{m-1}$  out-, ...,  $l_2$  in- et  $l_1$  out-shuffles, la carte n°  $i$  se retrouve au bas du paquet. C'est le fameux algorithme proposé par Elmsley [6]. D'un point de vue pratique, comme cela est mentionné dans [4], [5] et [6], on suit le schéma d'in/out-shuffles dicté par l'écriture binaire de  $i$  de gauche à droite en interprétant un bit 1 par un in-shuffle  $I$  et un bit 0 par un out-shuffle  $O$ , le premier bloc de  $O$  étant omis lorsque  $l_m = 0$  :

$$\underbrace{I-O-O}_{l_m} \dots \underbrace{I-O-O}_{l_2} \underbrace{I-O-O}_{l_1}.$$

REMARQUE. En fait, la procédure précédemment décrite pour amener la carte n° 0 à la position n°  $i$  reste valable pour un jeu de  $2n$  cartes,  $n$  étant un nombre quelconque. En effet, rappelons que pour  $j \in \{0, 1, \dots, n-1\}$ ,  $f(j) = 2j+1$  et  $g(j) = 2j$ . Soit alors un  $j \in \{0, 1, \dots, n-1\}$  d'écriture binaire  $j = \overline{j_{p-1} \dots j_0}$ . Pour un tel  $j$ , on a

$$f(j) = \overline{j_{p-1} \dots j_0 1}, \quad g(j) = \overline{j_{p-1} \dots j_0 0}.$$

Plus généralement, si  $\overline{j_{p-1} \dots j_0 \overbrace{1-1}^k} \leq 2n-1$ ,

(cette condition montrant que  $\overline{j_{p-1} \dots j_0 \overbrace{1-1}^{k-1}} \leq n-1$  et que l'utilisation de l'expression de  $f$  ci-dessus est licite), alors

$$f^k(j) = \overline{j_{p-1} \dots j_0 \overbrace{1-1}^k}.$$

De même, si  $\overline{j_{p-1} \dots j_0 \overbrace{0-0}^k} \leq 2n-1$ , alors

$$g^k(j) = \overline{j_{p-1} \dots j_0 \overbrace{0-0}^k}.$$

Ainsi, pour  $l_m$  tel que  $\overline{1-1}^{l_m} \leq 2n-1$ , on a

$$f^{l_m}(0) = \overline{1-1}^{l_m},$$

puis, pour  $l_{m-1}$  tel que  $\overline{1-10-0}^{l_{m-1}} \leq 2n-1$ , on a

$$(g^{l_{m-1}} \circ f^{l_m})(0) = \overline{1-10-0}^{l_{m-1} l_m}.$$

De manière générale, si les nombres  $l_1, \dots, l_m$  vérifient  $\overline{1-10-0}^{l_m} \dots \overline{1-10-0}^{l_2} \overline{1-10-0}^{l_1} \leq 2n-1$ , alors

$$(g^{l_1} \circ \dots \circ f^{l_m})(0) = \overline{1-10-0}^{l_m} \dots \overline{1-10-0}^{l_2} \overline{1-10-0}^{l_1}.$$

Cette dernière égalité prouve que la carte n° 0 peut effectivement atteindre n'importe quelle position  $i \in \{1, 2, \dots, 2n - 1\}$ .

### VII.3 Déplacement de la carte du dessus du paquet vers une position donnée

De manière analogue, regardons le déplacement de la carte du dessus du paquet, i.e. la carte n°  $2^p - 1$ , vers la position n°  $i$ . Puisque  $2^p - 1$  admet la simple décomposition binaire  $\underbrace{\overline{1-1}}_p$ , on a,

en inversant l'ordre de  $f$  et  $g$  dans les calculs précédents et en se souvenant que  $g(2^p - 1) = 2^p - 1$ ,

$$\begin{aligned} & (f^{k_m} \circ g^{k_{m-1}} \circ \dots \circ f^{k_2} \circ g^{k_1})(2^p - 1) \\ &= (f^{k_m} \circ g^{k_{m-1}} \circ \dots \circ f^{k_2})(2^p - 1) \\ &= \underbrace{\overline{1-10-0}}_{k_1} \dots \underbrace{\overline{1-10-0}}_{k_{m-1} \quad k_m}. \end{aligned}$$

Donc, pour atteindre la position  $i$  avec

$$i = \underbrace{\overline{1-10-0}}_{l_m \quad l_{m-1}} \dots \underbrace{\overline{1-10-0}}_{l_2 \quad l_1},$$

on suivra le schéma

$$\underbrace{I-IO-O}_{l_{m-1} \quad l_{m-2}} \dots \underbrace{O-OI-I}_{l_2 \quad l_1}.$$

### VII.4 Déplacement d'une carte donnée vers le dessous du paquet

Regardons maintenant le déplacement d'une carte de numéro donné  $i$  vers le dessous du paquet, i.e. vers la position n° 0. Avec la même décomposition binaire de  $i$ , on a

$$(g^{l_1} \circ f^{l_2} \circ \dots \circ g^{l_{m-1}} \circ f^{l_m})(i) = 0.$$

Puisque  $g(0) = 0$ , on peut omettre la manipulation redondante  $g^{l_1}$  ci-dessus pour obtenir

$$(f^{l_2} \circ g^{l_3} \circ \dots \circ g^{l_{m-1}} \circ f^{l_m})(i) = 0.$$

Ainsi, le schéma suivant déplace la carte n°  $i$  au-dessous du paquet :

$$\underbrace{I-IO-O}_{l_m \quad l_{m-1}} \dots \underbrace{O-OI-I}_{l_3 \quad l_2}.$$

### VII.5 Déplacement d'une carte donnée vers le dessus du paquet

Enfin, le déplacement de la carte de numéro donné  $i$  vers le dessus du paquet, i.e. vers la position n°  $2^p - 1$ , est décrit par la relation

$$(f^{l_1} \circ g^{l_2} \circ \dots \circ f^{l_{m-1}} \circ g^{l_m})(i) = 2^p - 1.$$

Ainsi, le schéma suivant, en omettant le dernier bloc de  $O$  lorsque  $l_1 = 0$ , déplace la carte n°  $i$  au-dessus du paquet :

$$\underbrace{O-OI-I}_{l_m} \dots \underbrace{O-OI-I}_{l_2 \quad l_1}.$$

## VIII Généralisation : $k$ paquets de $n$ cartes

On dispose de  $k$  paquets de  $n$  cartes, donc de  $kn$  cartes que l'on numérote de 1 à  $kn$  ou de 0 à  $kn-1$ . Cette situation peut se réaliser avec le concours de  $k$  joueurs installés à une table ronde, ayant chacun un jeu de  $n$  cartes en supposant que toutes les cartes sont différentes : le premier joueur a un jeu de cartes numérotées de bas en haut  $1, 2, \dots, n$ , le deuxième a un jeu de cartes numérotées de bas en haut  $n+1, n+2, \dots, 2n$ , etc., le  $k^e$  a un jeu de cartes numérotées de bas en haut  $(k-1)n+1, (k-2)n+2, \dots, kn$ . On réalise un in-shuffle ou un out-shuffle en prenant une carte à partir du haut du paquet à chaque joueur dans un ordre circulaire jusqu'à épuisement des cartes. On constitue ainsi un nouveau jeu de  $kn$  cartes que l'on recoupe en  $k$  paquets de  $n$  cartes que l'on redistribue à chaque joueur et l'on reproduit la manipulation *ad lib*. Cette généralisation est abordée dans [13].

### VIII.1 In-shuffle

Dans le cas d'un in-shuffle généralisé, on commence par prélever la carte de dessus au premier joueur, puis celle de dessus au deuxième que l'on place sous la précédente, etc., puis celle de dessus au dernier joueur que l'on place au-dessous des précédentes. On recommence à partir du premier joueur et ainsi de suite jusqu'à épuisement des cartes. On obtient de la sorte un paquet de cartes réparties de bas en haut selon la succession  $(k-1)n+1, (k-2)n+1, \dots, 2n+1, n+1, 1,$

puis  $(k-1)n+2, (k-2)n+2, \dots, 2n+2, n+2, 2$ ,  
puis  $(k-1)n+3, (k-2)n+3, \dots, 2n+3, n+3, 3$ ,  
et ainsi de suite jusqu'à  $kn, (k-1)n, \dots, 3n, 2n, n$   
(voir Fig. 14).

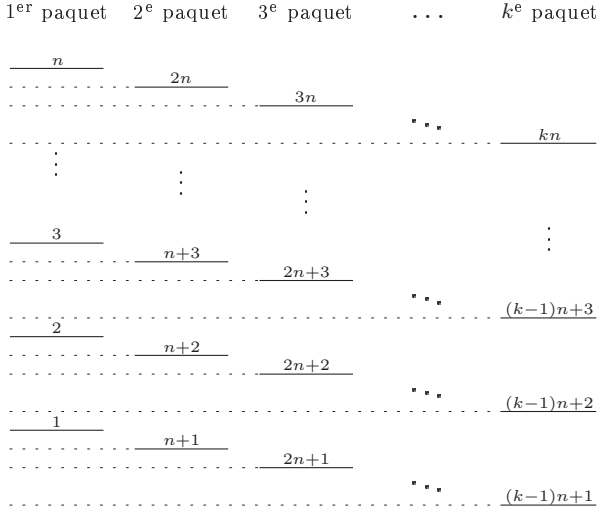


FIG. 14 – In-shuffle généralisé

L'in-shuffle généralisé est mathématiquement décrit par la permutation  $f$  des entiers  $1, 2, \dots, kn$  suivante (voir Fig. 15) :

$$f(i) = \begin{cases} \frac{i-1}{k} + (k-1)n+1 & \text{si } i \equiv 1 \pmod{k}, \\ \frac{i-2}{k} + (k-2)n+1 & \text{si } i \equiv 2 \pmod{k}, \\ \vdots & \\ \frac{i-k+1}{k} + n+1 & \text{si } i \equiv k-1 \pmod{k}, \\ \frac{i}{k} & \text{si } i \equiv 0 \pmod{k}. \end{cases}$$

De manière plus condensée, pour  $l \in \{0, 1, 2, \dots, k-1\}$  et  $i \equiv l \pmod{k}$ ,

$$f(i) = \frac{i-l}{k} + (k-l)n+1.$$

La réciproque de  $f$  est donnée par

$$f^{-1}(j) = \begin{cases} kj & \text{si } 1 \leq j \leq n, \\ kj - (kn+1) & \text{si } n+1 \leq j \leq 2n, \\ kj - 2(kn+1) & \text{si } 2n+1 \leq j \leq 3n, \\ \vdots & \\ kj - (k-1)(kn+1) & \text{si } (k-1)n+1 \leq j \leq kn. \end{cases}$$

La forme générique est, pour  $l \in \{0, 1, 2, \dots, k-1\}$  et  $ln+1 \leq j \leq (l+1)n$ ,

$$f^{-1}(j) = kj - l(kn+1).$$

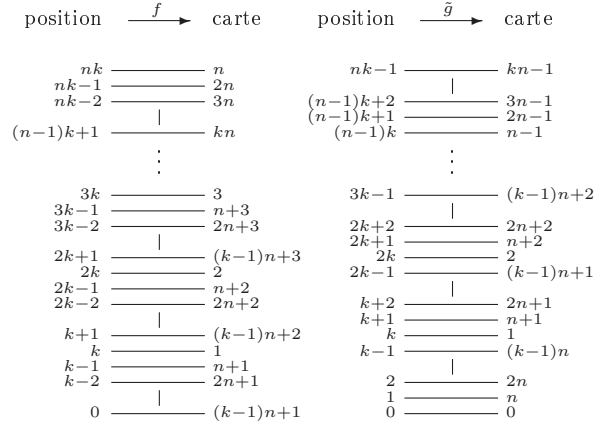


FIG. 15 – Mélanges généralisés, permutations  $f$  et  $\tilde{g}$

On note en particulier la congruence

$$f^{-1}(j) \equiv kj \pmod{(kn+1)}.$$

Cette observation conduit à la formulation suivante de la période de  $f$ .

**Théorème 10** *La période de  $f$  est l'ordre de  $k$  modulo  $(kn+1)$ , c'est-à-dire le premier entier  $r \geq 1$  tel que  $k^r \equiv 1 \pmod{(kn+1)}$ .*

**Corollaire 11** *Si  $n$  est de la forme  $k^{p-1}$  pour un  $p \geq 1$ , alors la période de  $f$  est  $2p$ .*

**DÉMONSTRATION.** Lorsque  $n = k^{p-1}$ , alors  $kn+1 = k^p + 1$  et  $k^p \equiv -1 \pmod{(kn+1)}$ . On a donc  $k^{2p} \equiv 1 \pmod{(kn+1)}$  qui prouve que  $f^{2p} = id$ . Par ailleurs, l'orbite de la carte n° 1 sous l'action de la permutation  $f$  est

$$\mathcal{O}(1) = \{1, k, k^2, \dots, k^{p-1}, k^p - k^{p-1}, k^p - k^{p-2}, \dots, k^p - k, k^p - 1\}$$

qui est de cardinal  $2p$ . C'est la période de  $f$ .  $\square$

## VIII.2 Out-shuffle

Dans le cas d'un out-shuffle généralisé, on commence par prélever la carte de dessus au dernier joueur, puis celle de dessus à l'avant-dernier que l'on place sous la précédente, etc., puis celle de dessus au premier joueur. On recommence à partir du dernier joueur et ainsi de suite jusqu'à épuisement des cartes. On obtient alors la répartition des cartes de bas en haut selon la succession  $0, n, 2n, \dots, (k-2)n, (k-1)n$ , puis

$1, n + 1, 2n + 1, \dots, (k - 2)n + 1, (k - 1)n + 1$ , puis  $2, n + 2, 2n + 2, \dots, (k - 2)n + 2, (k - 1)n + 2$ , et ainsi de suite jusqu'à  $n - 1, 2n - 1, 3n - 1, \dots, (k - 1)n - 1, kn - 1$  (voir Fig. 16).

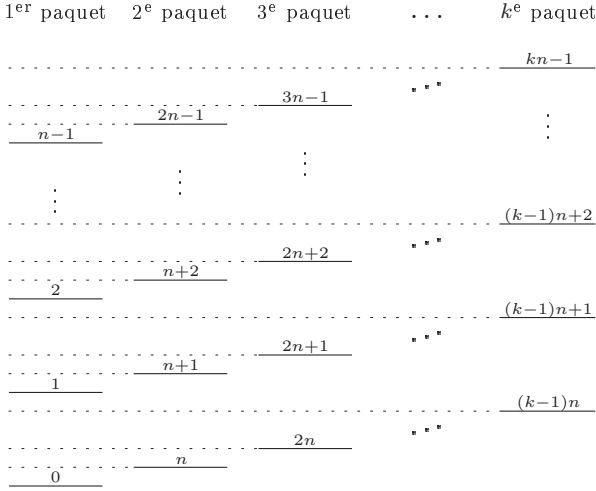


FIG. 16 – Out-shuffle généralisé

L'out-shuffle généralisé est modélisé par la permutation  $\tilde{g}$  des entiers  $0, 1, 2, \dots, kn - 1$  suivante (voir Fig. 15) :

$$\tilde{g}(i) = \begin{cases} \frac{i}{k} & \text{si } i \equiv 0 \pmod{k}, \\ \frac{i-1}{k} + n & \text{si } i \equiv 1 \pmod{k}, \\ \frac{i-2}{k} + 2n & \text{si } i \equiv 2 \pmod{k}, \\ \vdots & \\ \frac{i-k+1}{k} + (k-1)n & \text{si } i \equiv k-1 \pmod{k}. \end{cases}$$

La réciproque de  $\tilde{g}$  est donnée par

$$\tilde{g}^{-1}(j) = \begin{cases} kj & \text{si } 0 \leq j \leq n-1, \\ kj - (kn-1) & \text{si } n \leq j \leq 2n-1, \\ kj - 2(kn-1) & \text{si } 2n \leq j \leq 3n-1, \\ \vdots & \\ kj - (k-1)(kn-1) & \text{si } (k-1)n \leq j \leq kn-1. \end{cases}$$

On a en particulier la congruence

$$\tilde{g}^{-1}(j) \equiv kj \pmod{(kn-1)}$$

qui conduit à la formulation suivante de la période de  $\tilde{g}$ .

**Théorème 12** *La période de  $\tilde{g}$  est l'ordre de  $k$  modulo  $(kn - 1)$ , c'est-à-dire le premier entier  $s \geq 1$  tel que  $k^s \equiv 1 \pmod{(kn - 1)}$ .*

**Corollaire 13** *Si  $n$  est de la forme  $k^{p-1}$  pour un  $p \geq 1$ , alors la période de  $\tilde{g}$  est  $p$ .*

DÉMONSTRATION. Lorsque  $n = k^{p-1}$ , on a  $kn - 1 = k^p - 1$  et alors  $k^p \equiv 1 \pmod{(kn + 1)}$ . On a donc  $\tilde{g}^p = id$ . L'orbite de la carte  $n^0 1$  sous l'action de la permutation  $\tilde{g}$  est simplement

$$\tilde{O}(1) = \{1, k, k^2, \dots, k^{p-1}\}$$

qui est de cardinal  $p$ . C'est la période de  $\tilde{g}$ .  $\square$

REMERCIEMENTS. J'adresse mes sincères remerciements à deux de mes élèves, Matthieu Bacconnier et Anthony Tschirhard (INSA de Lyon, 51<sup>e</sup> promotion), le premier pour son aide relative aux calculs numériques présentés dans la section III.4, le second pour m'avoir soumis ces problèmes de mélange qui auront abouti au présent travail. D'autres remerciements s'adressent à Philippe Biane pour m'avoir communiqué certaines références sur le sujet.

## Références

- [1] P. Biane. Combien de fois faut-il battre un jeu de carte? *Gaz. Math.* 91 (2002), 4–10.
- [2] P.-Y. Chen, D.-H. Lawrie, P.-C. Yew & D.-A. Podera. Interconnection networks using shuffles. *Computer*, December(1981), 55–64.
- [3] J.-H. Conway & R.-K. Guy. *The book of numbers*, Springer-Verlag, 1996.
- [4] P. Diaconis & R. Graham. The solutions to Elmsley's Problem. *Mathematics Magazine* (2006).
- [5] P. Diaconis, R.L. Graham & W.M. Kantor. The mathematics of perfect shuffles. *Advances in Applied Mathematics* 4, No. 2 (1983), 175–191.
- [6] A. Elmsley. Mathematics of the weave shuffle. *The Pentagram* 11 (1957), 70–71, 78–79 and 85.
- [7] S.-W. Golomb. Permutations by cutting and shuffling. *SIAM Rev.* 3 (1961), 293–297.
- [8] I.-N. Herstein & I. Kaplansky. *Matters Mathematical*, Harper & Row, 1974.
- [9] P. Lévy. Étude d'une classe de permutations. *C. R. Acad. Sci.* 227 (1948), 422–423 et 578–579.

- [10] P. Lévy. Sur deux classes de permutations. C. R. Acad. Sci. 228 (1949), 1089–1090.
- [11] P. Lévy. Sur quelques classes de permutations. Compositio Math. 8 (1950), 1–48.
- [12] S.-B. Morris. The basic mathematics of the Faro shuffle. Pi Mu Epsilon J. 6 (1973), 85–92.
- [13] S.-B. Morris & R.-E. Hartwig. The generalized Faro shuffle. Discrete Math. 15 (1976), 333–346.
- [14] J.-T. Schwartz. Ultracomputers. ACM Trans. Program. Language Systems 2 (1980), 484–521.
- [15] H.-S. Stone. Parallel processing with the perfect shuffle. IEEE Trans. Comput. 2 (1971), 153–161.
- [16] J.-V. Uspensky & M.-A. Heaslet. Elementary number theory, McGraw Hill, 1939.
- [17] Shuffling, Wikipedia, the free encyclopedia.  
<http://en.wikipedia.org/wiki/Shuffling>
- [18] Shuffle, Wolfram Mathworld.  
<http://mathworld.wolfram.com/Shuffle.html>  
<http://mathworld.wolfram.com/RifleShuffle.html>  
<http://mathworld.wolfram.com/In-Shuffle.html>  
<http://mathworld.wolfram.com/Out-Shuffle.html>  
<http://mathworld.wolfram.com/MongesShuffle.html>