Quadrature

Magazine de mathématiques pures et épicées

La mathématique ouvre plus d'une fenêtre sur plus d'un monde

Résultats du prix de fantaisies

Mélanges parfaits (I)

Nombres brésiliens

Sommes de carrés dans un corps fini

n°76

Magazine trimestriel
Avril-Juin 2010
8,50 euros
ISSN 1142-2785

9 782759 805044

EDP SCIENCES

Quadrature n° 76 (2010) 13–25

DOI: 10.1051/quadrature/2010001

[Combinatoire]

Mélanges parfaits de cartes (I)

In-shuffles et out-shuffles

par Aimé Lachal*

Résumé.
Dans cet article, suivi d'un article compagnon qui paraîtra dans le prochain numéro de *Quadrature*, on étudie quelques mélanges de cartes bien connus du monde de la magie. On examine en détail l'éventualité de reconstituer le jeu de cartes initial après plusieurs mélanges consécutifs. Il s'agit mathématiquement d'un problème de systèmes dynamiques discrets pour lequel on recherche explicitement une période. Les calculs reposant sur des considérations algébriques élémentaires, l'article se veut accessible à un large public.

I Description du problème

Le problème suivant m'a été soumis par l'un de mes élèves[1] 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 jetons rouges et jetons verts. 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 les jetons 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 $n \leqslant 8$), 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 (figures 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 $1, 2, \ldots, 2n-1, 2n$ ($n \in \mathbb{N}^*$) et superposés de bas en haut dans l'ordre croissant,

1. Le processus de mélange décrit ci-dessus 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) 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 priviligié 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

* 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

[1] Anthony Tschirhard, INSA de Lyon, 51e promotion.

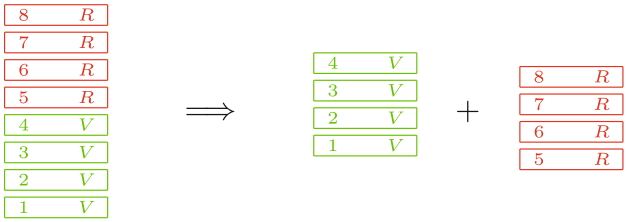


Figure 1. Premier découpage.

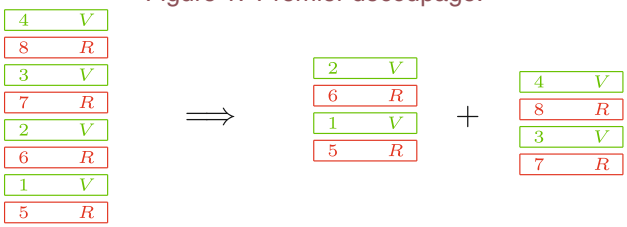


Figure 2. Deuxième découpage.

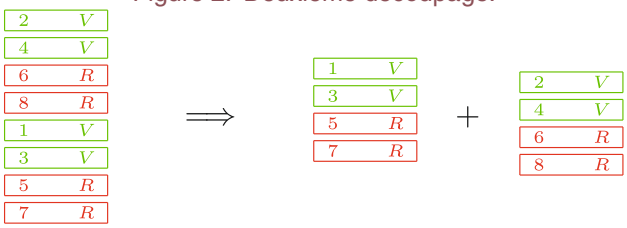


Figure 3. Troisième découpage.

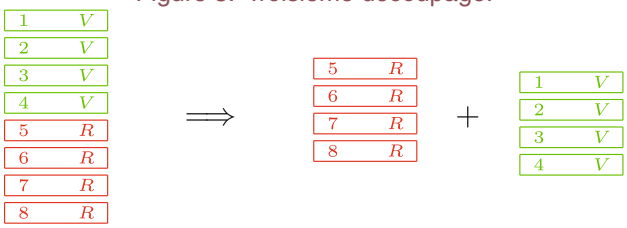


Figure 4. Quatrième découpage.

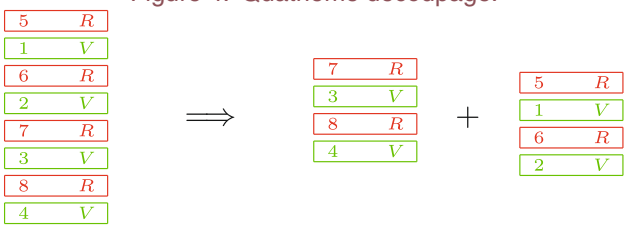


Figure 5. Cinquième découpage.

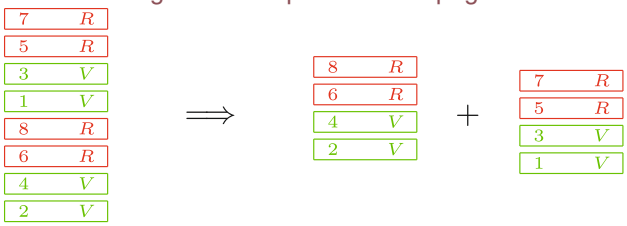


Figure 6. Sixième découpage.

et magicien Elmsley en 1957 [8]. On trouvera également une large description historique du problème dans la section intitulée « Some history of perfect shuffle » de [7].

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 [21, 22] pour un recensement de ces divers mélanges ainsi que d'autres variantes.

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 [8] ? 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 précédé 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 [6]).

Reprenons les questions posées par mon élève. La réponse à la première question (retour à l'état initial) 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 (calcul du nombre minimal de mélanges) est également affirmative ; c'est un calcul de période et une formule implicite est disponible, voir par exemple les livres de Conway et Guy [3], p. 163–165, de Herstein et Kaplansky [10], Chapitre 3.4, ou d'Uspensky et Heaslet [20], p. 244–245. Néanmoins, une formule explicite ne semble pas accessible excepté pour les cas particuliers où n est une puissance de 2 à ± 1 près. La troisième question (retour au regroupement initial dans le désordre) 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 $\{0, 1, 2, \ldots, 2n-1\}$ ou $\{1, 2, 3, \ldots, 2n\}$. L'un des deux ensembles sera d'une utilisation plus commode que

l'autre selon le cas étudié. Les permutations associées à $\{0, 1, 2, \ldots, 2n-1\}$ 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 ± 1 près. Toute cette analyse permet d'accéder au calcul des périodes de chacun des mélanges décrits ici. Dans un deuxième article [12], j'examinerai d'autres exemples de mélanges parfaits : les mélanges de Monge qui sont des in/out-shuffles déformés par une symétrie (voir par exemple [3, 21, 22]). On pourra trouver une version préliminaire rassemblant les deux articles sur le site arXiv [11].

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

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 [7, 9]). L'étude approfondie de certaines permutations mises en jeu a été entreprise indépendamment de ce contexte par Lévy [13–15]. Ce type de problème connaît également des applications, notamment en informatique (calcul parallèle, réseaux [2, 18, 19]), en cryptographie (codage d'informations [5]) ainsi qu'en imagerie numérique. Concernant ce dernier domaine, le mélange spécifique « out-shuffle » apparaît naturellement dans une opération de déformation connue sous le nom de « transformation du boulanger discrète » (voir [4] pour plus de détails). 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 la sous-section III.4, nous examinons brièvement le cas d'un jeu contenant un nombre impair de cartes que l'on divise en deux, ainsi que celui d'un paquet de cartes que l'on divise en un nombre supérieur à deux.
– Dans la section IV, 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 ± 1 près, ce qui permet de fournir une réponse explicite aux questions posées.
– Dans la section V, nous décrivons enfin un procédé simple pour déplacer une carte donnée vers une position prédéfinie dans le cas où n est une puissance de 2.

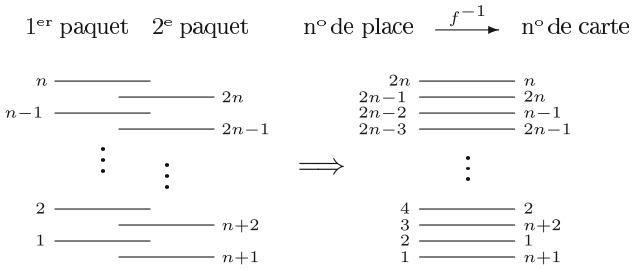


Figure 7. In-shuffle, permutation f^{-1}.

II Modélisation

Le jeu de cartes numérotées de bas en haut dans l'ordre $1, 2, 3, \ldots, 2n$ est coupé en son milieu et donne les deux paquets de cartes numérotées $1, 2, \ldots, n$ pour le premier et $n+1, n+2, \ldots, 2n$ 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^{os} $n+1, 1, n+2, 2, n+3, 3, \ldots, 2n-1, n-1, 2n, n$ (figure 7).

Cela se traduit par une correspondance entre numéros d'ordre avant et après mélange : à l'issue du mélange, la première carte du nouveau tas porte le n° $n+1$, la deuxième le n° 1, la troisième le n° $n+2$,

la quatrième le n° 2, etc. De manière générale, la j^{e} carte porte le n° $j/2$ lorsque j est pair et le n° $(n + (j + 1)/2)$ lorsque j est impair.

Inversement, une carte portant un numéro i entre 1 et n (qui correspond aussi à son numéro de classement initial) occupe à l'issue du mélange la place n° $2i$, et une carte portant un numéro i entre $n + 1$ et $2n$ occupe la place n° $(2i - 2n - 1)$. Par exemple, la carte n° 1 occupe la place n° 2, la carte n° 2 occupe la place n° 4, ..., puis la carte n° n occupe la place n° $2n$, la carte n° $(n + 1)$ occupe la place n° 1, la carte n° $(n + 2)$ occupe la place n° 3, etc.

Cette correspondance définit une permutation f des entiers $1, 2, 3, \ldots, 2n$ qui à la carte de numéro initial i associe son numéro de classement final $f(i)$ donné par

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

Réciproquement, le numéro $f^{-1}(j)$ est celui de la carte se situant à la j^{e} position à l'issue du mélange. Cette permutation réciproque – décrite sur la figure 7 – s'écrit

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

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

$$f(i) \equiv 2i \pmod{(2n + 1)}$$

qui sera utile pour calculer la période de f.

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

$$\mathfrak{f}(i) = \begin{cases} 2i + 1 & \text{si } 0 \leqslant i \leqslant n - 1, \\ 2i - 2n & \text{si } n \leqslant i \leqslant 2n - 1. \end{cases}$$

Les permutations f et $\mathfrak{f}$ 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$^{\text{os}}$ $1, n + 1, 2, n + 2, 3, n + 3, \ldots, n - 1, 2n - 1, n, 2n$ (figure 8).

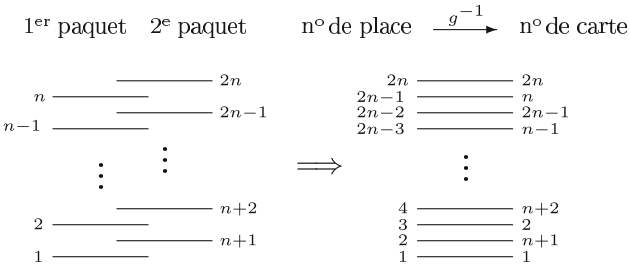


Figure 8. Out-shuffle, permutation g^{-1}.

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

$$g(i) = \begin{cases} 2i - 1 & \text{si } 1 \leqslant i \leqslant n, \\ 2i - 2n & \text{si } n + 1 \leqslant i \leqslant 2n, \end{cases}$$

de réciproque

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

On observe que $g(1) = 1$ et $g(2n) = 2n$, *i.e.* les cartes n$^{\text{os}}$ 1 et $2n$ restent immobiles tout au cours de la manipulation. Il convient alors de noter que cette particularité affecte en profondeur la nature du mélange (et des résultats) par rapport à l'in-shuffle des $2n$ cartes.

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

$$\mathfrak{g}(i) = \begin{cases} 2i & \text{si } 0 \leqslant i \leqslant n - 1, \\ 2i + 1 - 2n & \text{si } n \leqslant i \leqslant 2n - 1. \end{cases}$$

Notons en particulier la congruence

$$\mathfrak{g}(i) \equiv 2i \pmod{(2n - 1)}.$$

La restriction de $\mathfrak{g}$ à l'ensemble $\{1, \ldots, 2n - 2\}$ 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.

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

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

Plus précisément, la quantité $f^k(i)$ désigne la position occupée au bout de k mélanges par la carte portant initialement le numéro i.

Ainsi l'intégralité de l'expérience (supposée illimitée...) est modélisée par l'ensemble des itérations successives de f suivant : $\{\mathrm{id}, f, f^2, f^3, \ldots\} = \{f^k,\ k \in \mathbb{N}\}$. C'est un sous-ensemble de l'ensemble fini $\mathcal{S}_{2n}$ des permutations de $\{1, 2, \ldots, 2n\}$, 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 $r = l - k$, $f^r = \mathrm{id}$. 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 $\{\mathrm{id}, f, f^2, \ldots, f^{r-1}\}$. Le nombre r est une période de l'application $k \in \mathbb{Z} \longmapsto f^k \in \mathcal{S}_{2n}$. Remarquons que la permutation $\mathfrak{f}$ qui est définie par $\mathfrak{f}(i) = f(i+1)-1$ vérifie $\mathfrak{f}^k(i) = f^k(i+1)-1$. Ainsi, l'équation d'inconnue r, $f^r = \mathrm{id}$, est équivalente à $\mathfrak{f}^r = \mathrm{id}$. Cela signifie que les permutations f et $\mathfrak{f}$ (et aussi f^{-1} et $\mathfrak{f}^{-1}$) 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 pourrons travailler indifféremment avec f ou $\mathfrak{f}$ selon le cas. Le calcul de cette période – le plus petit $r \geqslant 1$ tel que $f^r = \mathrm{id}$ – est précisément l'objet de la deuxième question posée dans l'introduction. Une méthode de calcul est proposée dans les théorèmes 1 et 4 ci-dessous, on peut la trouver par exemple dans les divers livres [3, 10, 20] ainsi que dans les articles [8, 16].

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 correspondant à un ordre de jetons (s'ils étaient discernables) différent. Cela revient à déterminer pour la permutation f le plus petit entier $r' \geqslant 1$, s'il existe, tel que $f^{r'} \neq \mathrm{id}$ et

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

et

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

Il est facile de voir que l'entier r', s'il existe, divise la période 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 $r \geqslant 1$ vérifiant $2^r \equiv 1\ [\mathrm{mod}\ (2n+1)]$. 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 :

$$f(i) \equiv 2i\ [\mathrm{mod}\ (2n+1)].$$

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

$$f^k(i) \equiv 2^k i\ [\mathrm{mod}\ (2n+1)].$$

La période de f est donc le plus petit entier $r \geqslant 1$ vérifiant $2^r \equiv 1\ [\mathrm{mod}\ (2n+1)]$. Notons qu'un tel entier existe effectivement. En effet, en adaptant le raisonnement précédent et en rappelant la notation $a \mod n$ qui désigne le reste de la division euclidienne de a par n, l'ensemble $\{2^k \mathrm{mod}\ (2n+1),\ k \in \mathbb{N}\}$ est fini, il existe au moins deux entiers distincts k et l tels que $k < l$ et $2^k \equiv 2^l\ [\mathrm{mod}\ (2n+1)]$. 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 $2^{l-k} \equiv 1\ [\mathrm{mod}\ (2n+1)]$ avec $l - k \geqslant 1$. □

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

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

L'orbite de 1 est en particulier

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

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

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

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

Proposition 2.

– *Pour tout $i \in \{1, 2, \ldots, n\}$, le cardinal de l'orbite de i est un diviseur de celui de l'orbite de 1 :* $\mathrm{card}\,\mathcal{O}(i)$ *divise* $\mathrm{card}\,\mathcal{O}(1)$.

– *Dans le cas particulier où i est un nombre premier avec $2n+1$, ces orbites ont même cardinal :* $\operatorname{card} \mathcal{O}(i) = \operatorname{card} \mathcal{O}(1)$.

– *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 $2n+1$: $d_i = \operatorname{pgcd}(i, 2n+1)$ et posons $r_i = \operatorname{card} \mathcal{O}(i)$ (on a en particulier $r_1 = r$). Le cardinal r_i est le plus petit entier strictement positif tel que $2^k i \equiv i \ [\mathrm{mod}\ (2n+1)]$. Cette dernière égalité est équivalente à l'assertion « $(2n+1)$ divise $i(2^k-1)$ », ou encore « $(2n+1)/d_i$ divise $(i/d_i)(2^k-1)$ ». 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^k-1. On voit ainsi que $r_i = \min\{k \in \mathbb{N}^* : 2^k \equiv 1 \ [\mathrm{mod}\ m_i]\}$.

Prouvons que r_i divise r. Comme m_i divise $2n+1$, on a l'implication

$$x \equiv y \ [\mathrm{mod}\ (2n+1)] \Longrightarrow x \equiv y \ [\mathrm{mod}\ m_i].$$

On peut alors définir de manière cohérente, entre les groupes multiplicatifs

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

et

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

un morphisme

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

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

– Lorsque i est premier avec $2n+1$, i est inversible modulo $(2n+1)$ et l'application de multiplication par i

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

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 $i \in \{1, 2, \ldots, 2n\}$ est premier avec $2n+1$ et donc $r_i = r$. La réunion des différentes orbites coïncidant avec $\{1, 2, \ldots, 2n\}$, il y a alors $2n/r$ orbites distinctes. □

Exemple (cas d'un jeu de 52 cartes). 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 : $\mathcal{O}(1) = \{1, 2, 3, \ldots, 52\}$ et l'in-shuffle est de période 52.

Exemple (cas d'un jeu de 54 cartes). 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 :

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

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 $(p \geqslant 1)$ est $2p$.*

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

Démonstration. Écrivons l'orbite de 1.

– Si $n = 2^{p-1}$, alors $2n+1 = 2^p + 1$. On voit que $2^p \equiv -1 \ [\mathrm{mod}\ (2n+1)]$, puis, en élevant au carré, que $2^{2p} \equiv 1 \ [\mathrm{mod}\ (2n+1)]$. D'après le théorème 1, on tire que $2p$ est une période de l'in-shuffle. On a ensuite, pour tout $k \in \{p, p+1, \ldots, 2p\}$, $2^k \equiv 2^p - 2^{k-p} + 1 \ [\mathrm{mod}\ (2n+1)]$ avec l'encadrement $1 \leqslant 2^p - 2^{k-p} + 1 \leqslant 2n$. L'orbite de 1 est dans ce cas

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

On constate que $\operatorname{card} \mathcal{O}(1) = 2p$ 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 $2^p \equiv 1 \ [\mathrm{mod}\ (2n+1)]$. Cette fois, l'orbite de 1 est donnée par

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

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

Exemple (cas d'un jeu de 32 cartes). 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 $f(1) = 2$, $f^2(1) = 4$, $f^3(1) = 8$, $f^4(1) = 16$, $f^5(1) = 32$, $f^6(1) = 31$, $f^7(1) = 29$, $f^8(1) = 25$, $f^9(1) = 17$, $f^{10}(1) = 1$. Plus généralement, on trouve quatre orbites distinctes :

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

On vérifie que les cardinaux de $O(3)$, $O(5)$, $O(11)$, valant respectivement 10, 10, 2, divisent le cardinal de $O(1)$ 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 $s \geqslant 1$ vérifiant $2^s \equiv 1 \ [\mathrm{mod}\ (2n-1)]$. En d'autres termes, s est l'ordre de 2 modulo $(2n-1)$.*

Démonstration. Rappelons la congruence vérifiée par la permutation $\mathfrak{g}$ associée à l'out-shuffle : $\mathfrak{g}(i) \equiv 2i \ [\mathrm{mod}\ (2n-1)]$ qui donne pour tout $k \in \mathbb{N}$:

$$\mathfrak{g}^k(i) \equiv 2^k i \ [\mathrm{mod}\ (2n-1)].$$

La période de $\mathfrak{g}$ et donc de g est alors le plus petit entier $s \geqslant 1$ vérifiant $2^s \equiv 1 \ [\mathrm{mod}\ (2n-1)]$. □

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^{e} carte ($i \in \{0, 1, 2, \ldots, 2n-1\}$) est décrite par l'orbite de i sous l'action de $\mathfrak{g}$:

$$\begin{aligned} \mathfrak{O}(i) &= \{\mathfrak{g}^k(i),\ k \in \mathbb{Z}\} \\ &= \{i, \mathfrak{g}(i), \mathfrak{g}^2(i), \ldots, \mathfrak{g}^{s-1}(i)\} \\ &= \{2^k i \bmod (2n-1),\ 0 \leqslant k \leqslant s-1\}. \end{aligned}$$

L'orbite de 1 est en particulier

$$\mathfrak{O}(1) = \{2^k \bmod (2n-1),\ 0 \leqslant k \leqslant s-1\}.$$

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 neuf orbites suivantes :

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

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 :

$$\mathfrak{O}(0) = \{0\},\ \mathfrak{O}(1) = \{1, 2, 3, \ldots, 52\},\ \mathfrak{O}(53) = \{53\}.$$

La période dans ce cas est $s = 52$.

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

Corollaire 5.

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

– *La période de l'out-shuffle d'un jeu de $2^p + 2$ cartes ($p \geqslant 1$) 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° 1 est décrite selon le cycle $\mathfrak{g}(1) = 2$, $\mathfrak{g}^2(1) = 4$, $\mathfrak{g}^3(1) = 8$, $\mathfrak{g}^4(1) = 16$, $\mathfrak{g}^5(1) = 1$. Plus généralement, on trouve huit orbites distinctes :

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

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 Quelques valeurs numériques

Nous donnons ci-dessous les périodes des in-shuffles pour des jeux de $2n$ cartes avec $2n \leqslant 64$.

$2n$	2	4	6	8	10	12	14	16
Période	2	4	3	6	10	12	4	8

$2n$	18	20	22	24	26	28	30	32
Période	18	6	11	20	18	28	5	10

$2n$	34	36	38	40	42	44	46	48
Période	12	36	12	20	14	12	23	21

$2n$	50	52	54	56	58	60	62	64
Période	8	52	20	18	58	60	6	12

III.4 Quelques prolongements

Nous considérons succinctement ici deux prolongements de notre analyse dont on trouvera les détails dans [11].

III.4.1 Cas d'un jeu contenant un nombre impair de cartes

Examinons le cas d'un jeu de $2n+1$ cartes, cas étudié dans [16]. 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 $(n+1)^{\text{e}}$. En d'autres termes, après coupage, le premier paquet contient n cartes et le deuxième en contient $n+1$, ou inversement. On intercale alors le paquet de n cartes dans celui de $n+1$. On observe aisément que la première ou la dernière carte, selon le coupage effectué, reste immobile et qu'en la retirant du jeu, cette manipulation est identique à l'in-shuffle du jeu des $2n$ cartes restantes. En conclusion, on a le résultat suivant.

Théorème 6. *La période du mélange parfait de $2n+1$ cartes est l'ordre de 2 modulo $(2n+1)$.*

III.4.2 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 $1, 2, \ldots, n$, le deuxième a un jeu de cartes numérotées de bas en haut $n+1, n+2, \ldots, 2n$, etc., le k^{e} a un jeu de cartes numérotées de bas en haut $(k-1)n+1$, $(k-2)n+2, \ldots, kn$.

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. Les cartes prélevées sont placées successivement les unes au-dessous des autres. Dans le cas d'un in-shuffle, on prélève les cartes du premier au dernier joueur et dans le cas d'un out-shuffle, le prélèvement s'effectue du dernier au premier joueur. 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 [17].

L'in-shuffle et l'out-shuffle généralisés peuvent mathématiquement être décrits par les permutations f des entiers $1, 2, \ldots, kn$ et $\mathfrak{g}$ des entiers $0, 1, 2, \ldots, kn-1$ caractérisées par les congruences

$$f(i) \equiv ki \ [\mathrm{mod}\ (kn+1)],$$
$$\mathfrak{g}(i) \equiv ki \ [\mathrm{mod}\ (kn-1)].$$

Une analyse analogue à celle décrite en début de section conduit à la formulation suivante des périodes de f et $\mathfrak{g}$.

Théorème 7.

– *La période de f est l'ordre de k modulo $(kn+1)$, c'est-à-dire le premier entier $r \geqslant 1$ tel que $k^r \equiv 1$ [mod $(kn+1)$].*

– *La période de $\mathfrak{g}$ est l'ordre de k modulo $(kn-1)$, c'est-à-dire le premier entier $s \geqslant 1$ tel que $k^s \equiv 1$ [mod $(kn-1)$].*

Corollaire 8. *Si n est de la forme k^{p-1} pour un $p \geqslant 1$, alors la période de f est $2p$ et celle de $\mathfrak{g}$ est p.*

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 $\mathfrak{f}$. Introduisons l'écriture binaire d'un numéro de carte $i \in \{0, 1, \dots, 2n-1\}$:

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

où les $i_0, i_1, \dots, i_{p-1}$ sont des bits 0 ou 1. On a en particulier $n = \overline{\underbrace{10-0}_{p-1}}$ et $2n-1 = \overline{\underbrace{1-1}_{p}}$. Dans ces conditions, l'image de i par la permutation $\mathfrak{f}$ se calcule comme suit. Si $i \leqslant n-1$, alors $i_{p-1} = 0$ et

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

De même, si $i \geqslant n$, alors $i_{p-1} = 1$ et

$$\mathfrak{f}(i) = 2i - 2n = \overline{i_{p-2} \dots i_0 0}.$$

On peut finalement écrire $\mathfrak{f}(i)$ sous la forme

$$\mathfrak{f}(i) = \begin{cases} \overline{i_{p-2} \dots i_0 1} & \text{si } i_{p-1} = 0, \\ \overline{i_{p-2} \dots i_0 0} & \text{si } i_{p-1} = 1, \end{cases}$$

soit encore

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

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

$$\mathfrak{f}(i) = \overline{i_{p-2} \dots i_0 (1 - i_{p-1})},$$
$$\mathfrak{f}^2(i) = \overline{i_{p-3} \dots i_0 (1 - i_{p-1})(1 - i_{p-2})}$$

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

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

Pour $k = p$, on obtient

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

que l'on peut réécrire

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

Ainsi $\mathfrak{f}^p$ 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 $p \leqslant k \leqslant 2p$,

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

pour aboutir finalement à

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

On retrouve bien le fait que, dans le cas où $n = 2^{p-1}$, le nombre $2p$ est une période de $\mathfrak{f}$ (et aussi de 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 $i \in \{1, 2 \dots, 2n\}$: $i = \overline{i_{p-1} \dots i_0}$. Dans ces conditions, l'image de i par la permutation f s'écrit

$$f(i) = \begin{cases} \overline{i_{p-2} \dots i_0 0} & \text{si } i_{p-1} = 0, \\ \overline{i_{p-2} \dots i_0 1} & \text{si } i_{p-1} = 1, \end{cases}$$

soit encore

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

Dans ce cas, la permutation f correspond à une simple permutation circulaire des chiffres de la décomposition binaire de la variable : $(i_0, i_1, \dots, i_{p-1}) \longmapsto (i_{p-1}, i_0, i_1, \dots, i_{p-2})$. On obtient immédiatement, pour $0 \leqslant k \leqslant p$,

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

Finalement pour $k = p$:

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

Ce procédé est signalé dans [1, 7]. On retrouve le fait que, dans le cas où $n = 2^{p-1} - 1$, p est une période de f.

V 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 succession 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 ($p \geqslant 1$) et renvoyons le lecteur à [6] où une procédure algorithmique est proposée dans le cas général. Les cartes sont numérotées de bas en haut $0, 1, 2, \dots, 2^p - 1$.

V.1 Procédure générale

Rappelons que les déplacements de la carte n° i, où $i = \overline{i_{p-1} \dots i_0}$, par un in- et un out-shuffles sont respectivement représentés par

$$\mathfrak{f}(i) = \overline{i_{p-2} \dots i_0 (1 - i_{p-1})}, \quad \mathfrak{g}(i) = \overline{i_{p-2} \dots i_0 i_{p-1}}.$$

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

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

Déterminons explicitement l'écriture binaire du numéro j. On a

$$\mathfrak{f}^{k_1}(i) = \overline{i_{p-k_1-1}\dots i_0(1-i_{p-1})\dots(1-i_{p-k_1})}$$

puis

$$(\mathfrak{g}^{k_2}\circ\mathfrak{f}^{k_1})(i) = \overline{i_{p-k_1-k_2-1}\dots i_0}\ \overline{(1-i_{p-1})\dots(1-i_{p-k_1})i_{p-k_1-1}\dots i_{p-k_1-k_2}}$$

puis

$$\begin{aligned}(\mathfrak{f}^{k_3}\circ\mathfrak{g}^{k_2}\circ\mathfrak{f}^{k_1})(i) &= \overline{i_{p-k_1-k_2-k_3-1}\dots i_0}\\ &\quad\overline{(1-i_{p-1})\dots(1-i_{p-k_1})}\\ &\quad\overline{i_{p-k_1-1}\dots i_{p-k_1-k_2}}\\ &\quad\overline{(1-i_{p-k_1-k_2-1})\dots(1-i_{p-k_1-k_2-k_3})}.\end{aligned}$$

De proche en proche, on arrive à

$$\begin{aligned}(\mathfrak{f}^{k_{m-1}}\circ\mathfrak{g}^{k_{m-2}}\circ\dots\circ\mathfrak{g}^{k_2}\circ\mathfrak{f}^{k_1})(i) &= \overline{i_{p-k_1-\dots-k_{m-1}-1}\dots i_0}\\ &\quad\overline{(1-i_{p-1})\dots(1-i_{p-k_1})i_{p-k_1-1}\dots i_{p-k_1-k_2}}\\ &\quad\overline{\dots}\\ &\quad\overline{(1-i_{p-k_1-\dots-k_{m-2}-1})\dots(1-i_{p-k_1-\dots-k_{m-1}})}\\ &= \overline{i_{k_m-1}\dots i_0(1-i_{p-1})\dots(1-i_{p-k_1})}\\ &\quad\overline{i_{p-k_1-1}\dots i_{p-k_1-k_2}}\\ &\quad\overline{\dots}\\ &\quad\overline{(1-i_{k_m+k_{m-1}-1})\dots(1-i_{k_m})}\end{aligned}$$

et enfin à

$$\begin{aligned}(\mathfrak{g}^{k_m}\circ\mathfrak{f}^{k_{m-1}}\circ\dots\circ\mathfrak{g}^{k_2}\circ\mathfrak{f}^{k_1})(i) &= \overline{\underbrace{(1-i_{p-1})\dots(1-i_{p-k_1})}_{k_1}\underbrace{i_{p-k_1-1}\dots i_{p-k_1-k_2}}_{k_2}}\\ &\quad\overline{\dots}\\ &\quad\overline{\underbrace{(1-i_{k_m+k_{m-1}-1})\dots(1-i_{k_m})}_{k_{m-1}}\underbrace{i_{k_m-1}\dots i_0}_{k_m}}.\end{aligned}$$

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

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

Ce calcul permet d'élaborer un algorithme pour déplacer une carte de numéro donné i vers une position de numéro donné j ($j \neq i$). 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 situés à chaque même place et l'on fait apparaître dans j des blocs de bits successifs identiques à ceux de i et des blocs de bits successifs complémentaires à ceux de i. On décompose ainsi j en « blocs de coïncidence » et « blocs de complémentarité » avec ceux de i. Plus précisément, en introduisant la suite des longueurs de ces blocs

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

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

$$\begin{aligned}j = &\overline{\underbrace{(1-i_{p-1})\dots(1-i_{p-\lambda_m})}_{\lambda_m}}\\ &\overline{\underbrace{i_{p-\lambda_m-1}\dots i_{p-\lambda_m-\lambda_{m-1}}}_{\lambda_{m-1}}}\\ &\overline{\dots}\\ &\overline{\underbrace{(1-i_{\lambda_1+\lambda_2-1})\dots(1-i_{\lambda_1})}_{\lambda_2}}\\ &\overline{\underbrace{i_{\lambda_1-1}\dots i_0}_{\lambda_1}}.\end{aligned}$$

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

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

Cela indique que λ_m in-, λ_{m-1} out-, …, λ_2 in- et λ_1 out-shuffles mènent la carte n° i à la position n° j. En d'autres termes, le procédé recherché se schématise selon la succession suivante (de gauche à droite) :

$$\underbrace{I-I}_{\lambda_m}\underbrace{O-O}_{\lambda_{m-1}}\dots\underbrace{I-I}_{\lambda_2}\underbrace{O-O}_{\lambda_1}.$$

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° i à la place n° j déplace également la carte n° j à la position n° i.

Exemple. Examinons le cas d'un jeu de 32 cartes numérotées $0, 1, 2, \ldots, 31$. 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 : $\mathfrak{f}(7) = 15$, $\mathfrak{g}(15) = 30$, $\mathfrak{f}(30) = 28$, $\mathfrak{g}(28) = 25$, $\mathfrak{g}(25) = 19$, qui donne

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

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 : $\mathfrak{g}(19) = 7$... 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 [6], 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.

V.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. Introduisons la décomposition binaire de i par blocs

$$i = \overbrace{\underbrace{1-1}_{l_m}\underbrace{0-0}_{l_{m-1}}}\ldots\overbrace{\underbrace{1-1}_{l_2}\underbrace{0-0}_{l_1}},$$

où les $l_1, \ldots, l_m$ 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. Les calculs précédents nous enseignent que

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

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 $\mathfrak{g}(0) = 0$ (un out-shuffle n'affecte pas la carte n° 0), on peut retirer la manipulation redondante $\mathfrak{g}^{l_{m-1}}$ ci-dessus pour obtenir

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

Ainsi, en effectuant successivement l_m in-, l_{m-1} out-, $\ldots$, 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 [8]. D'un point de vue pratique, comme cela est mentionné dans [6–8], 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 $l_m = 0$:

$$\underbrace{I-I}_{l_m}\underbrace{O-O}_{l_{m-1}}\ldots\underbrace{I-I}_{l_2}\underbrace{O-O}_{l_1}.$$

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 $i \in \{0, 1, \ldots, n-1\}$, $\mathfrak{f}(i) = 2i + 1$ et $\mathfrak{g}(i) = 2i$. Soit alors un $i \in \{0, 1, \ldots, n-1\}$ d'écriture binaire $i = \overline{i_{p-1} \ldots i_0}$. Pour un tel i, on a

$$\mathfrak{f}(i) = \overline{i_{p-2} \ldots i_0 1}, \quad \mathfrak{g}(i) = \overline{i_{p-2} \ldots i_0 0}.$$

Plus généralement, si $\overline{i_{p-2} \ldots i_0 \underbrace{1-1}_{k}} \leqslant 2n - 1$, (cette condition montrant que

$$\overline{i_{p-2} \ldots i_0 \underbrace{1-1}_{k-1}} \leqslant n - 1$$

et que l'utilisation de l'expression de $\mathfrak{f}$ ci-dessus est licite), alors

$$\mathfrak{f}^k(i) = \overline{i_{p-2} \ldots i_0 \underbrace{1-1}_{k}}.$$

De même, si $\overline{i_{p-2} \ldots i_0 \underbrace{0-0}_{k}} \leqslant 2n - 1$, alors

$$\mathfrak{g}^k(i) = \overline{i_{p-2} \ldots i_0 \underbrace{0-0}_{k}}.$$

Ainsi, pour l_m tel que $\overline{\underbrace{1-1}_{l_m}} \leqslant 2n-1$, on a

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

puis, pour l_{m-1} tel que $\overline{\underbrace{1-1}_{l_m}\underbrace{0-0}_{l_{m-1}}} \leqslant 2n-1$, on a

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

De manière générale, si les nombres $l_1, \ldots, l_m$ vérifient la condition

$$\overline{\underbrace{1-1}_{l_m}\underbrace{0-0}_{l_{m-1}}\ldots\underbrace{1-1}_{l_2}\underbrace{0-0}_{l_1}} \leqslant 2n-1,$$

alors

$$(\mathfrak{g}^{l_1} \circ \cdots \circ \mathfrak{f}^{l_m})(0) = \overline{\underbrace{1-1}_{l_m}\underbrace{0-0}_{l_{m-1}}\ldots\underbrace{1-1}_{l_2}\underbrace{0-0}_{l_1}}.$$

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

V.3 Autres déplacements

De manière analogue, le lecteur pourra vérifier les procédures suivantes. Donnons-nous un numéro i décomposé comme auparavant selon

$$i = \overline{\underbrace{1-1}_{l_m}\underbrace{0-0}_{l_{m-1}}\ldots\underbrace{1-1}_{l_2}\underbrace{0-0}_{l_1}}$$

avec $l_1, l_m \geqslant 0$ et $l_2, \ldots, l_{m-1} \geqslant 1$.

– Pour déplacer la carte du dessus du paquet vers la position n° i, on suivra le schéma

$$\underbrace{I-I}_{l_{m-1}}\underbrace{O-O}_{l_{m-2}}\ldots\underbrace{O-O}_{l_2}\underbrace{I-I}_{l_1}.$$

– Pour déplacer la carte de numéro i vers le dessous du paquet, on suivra le schéma

$$\underbrace{I-I}_{l_m}\underbrace{O-O}_{l_{m-1}}\ldots\underbrace{O-O}_{l_3}\underbrace{I-I}_{l_2}.$$

– Pour déplacer la carte de numéro i vers le dessus du paquet, on suivra le schéma suivant, en omettant le dernier bloc de O lorsque $l_1 = 0$:

$$\underbrace{O-O}_{l_m}\underbrace{I-I}_{l_{m-1}}\ldots\underbrace{O-O}_{l_2}\underbrace{I-I}_{l_1}.$$

Remerciements. J'adresse mes sincères remerciements à deux de mes élèves, Matthieu Bacconnier et Anthony Tschirhard (INSA de Lyon, 51e promotion), le premier pour son aide relative aux calculs numériques présentés dans la section III.3, 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 ainsi qu'à Roger Mansuy et un référé anonyme pour leurs nombreuses suggestions qui m'ont permis d'améliorer la présentation de cet article.

Références

[1] P. Biane, « Combien de fois faut-il battre un jeu de cartes ? », *Gaz. Math.* **91** (2002) 4–10.

[2] P.-Y. Chen, D.-H. Lawrie, P.-C. Yew and D.-A. Podera, « Interconnection networks using shuffles », *Computer* **December** (1981) 55–64.

[3] J.-H. Conway and R.-K. Guy, *The book of numbers*, Springer-Verlag, 1996.

[4] J.-P. Delahaye et P. Mathieu, « Images brouillées, images retrouvées », *Pour la Science* **242** (1997) 102–106.

[5] J.-P. Delahaye, « L'ag♣nt s♣cr♣t jou♣ aux cart♣s », *Pour la Science* **284** (2001) 100–104.

[6] P. Diaconis and R. Graham, « The solutions to Elmsley's Problem », *Math Horizons* **14** (2007) 22–27.

[7] P. Diaconis, R.L. Graham and W.M. Kantor, « The mathematics of perfect shuffles », *Adv. Appl. Math.* **4** (1983) 175–191.

[8] A. Elmsley, « Mathematics of the weave shuffle », *The Pentagram* **11** (1957) 70–71, 78–79, 85.

[9] S.-W. Golomb, « Permutations by cutting and shuffling », *SIAM Rev.* **3** (1961) 293–297.

[10] I.-N. Herstein and I. Kaplansky, *Matters Mathematical*, Harper & Row, 1974.

[11] A. Lachal, « Quelques mélanges parfaits de cartes ». Disponible sur arXiv : http://arxiv.org/abs/0910.0524 [math.HO] (2009).

[12] A. Lachal, « Mélanges parfaits de cartes (II) – Mélanges de Monge », *Quadrature* (à paraître).

[13] P. Lévy, « Étude d'une classe de permutations », *C. R. Acad. Sci.* **227** (1948) 422–423, 578–579.

[14] P. Lévy, « Sur deux classes de permutations », *C. R. Acad. Sci.* **228** (1949) 1089–1090.

[15] P. Lévy, « Sur quelques classes de permutations », *Compositio Math.* **8** (1950) 1–48.

[16] S.-B. Morris, « The basic mathematics of the Faro shuffle », *Pi Mu Epsilon J.* **6** (1973) 85–92.

[17] S.-B. Morris and R.-E. Hartwig, « The generalized Faro shuffle », *Discrete Math.* **15** (1976) 333–346.

[18] J.-T. Schwartz, « Ultracomputers », *ACM Trans. Program. Language Systems* **2** (1980) 484–521.

[19] H.-S. Stone, « Parallel processing with the perfect shuffle », *IEEE Trans. Comput.* **2** (1971) 153–161.

[20] J.-V. Uspensky and M.-A. Heaslet, *Elementary number theory*, McGraw Hill, 1939.

[21] Shuffle, Wolfram Mathworld.
http://mathworld.wolfram.com/Shuffle.html
http://mathworld.wolfram.com/RiffleShuffle.html
http://mathworld.wolfram.com/In-Shuffle.html
http://mathworld.wolfram.com/Out-Shuffle.html
http://mathworld.wolfram.com/MongesShuffle.html

[22] Shuffling, Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Shuffling.

* * * * * * *

QUADRATURE

Appel à auteurs

Quadrature, magazine de mathématiques pures et appliquées, **s'adresse aux enseignants, étudiants, ingénieurs, amateurs de mathématiques**.

La plupart des articles requièrent un bon niveau de terminale scientifique ou une première année de premier cycle. Les auteurs sont des mathématiciens, des enseignants et des étudiants...

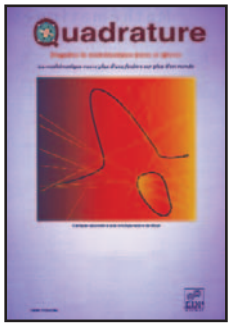
Quadrature est éclectique : certains articles présentent des mathématiques toutes récentes, tandis que d'autres donnent un nouveau point de vue sur des sujets traditionnels ou encore ressuscitent des questions de géométrie ancienne. On trouve également dans le magazine un **forum**, des **nouvelles**, des **notes de lecture**, des **articles d'histoire des mathématiques** et des **articles de réflexion en relation avec l'actualité**. Enfin, un large « coin des problèmes » permet aux lecteurs de poser des questions, qu'ils en connaissent la réponse ou pas.

Quadrature est ouvert, en particulier aux jeunes. Le magazine publie régulièrement des TPE (travaux personnels encadrés) de terminale et premier cycle d'université.

Vous souhaitez contribuer activement à la revue. Venez enrichir nos différentes rubriques et proposez-nous :

- ✔ articles de revue,
- ✔ brèves scientifiques,
- ✔ forum des lecteurs,
- ✔ manifestations,
- ✔ reportages,
- ✔ images mathématiques,
- ✔ analyses d'ouvrages et de logiciels,
- ✔ sites internet spécialisés en mathématiques,
- ✔ nouvelles, fantaisies mathématiques...

N'hésitez pas à prendre contact avec notre bureau de rédaction :



Quadrature
EDP Sciences
PA de Courtabœuf
17 avenue du Hoggar
BP 112
91944 Les Ulis Cedex A
Tél. : 01 69 18 75 75 • Fax : 01 69 07 45 17
E-mail : **quadrature@edpsciences.org**

Quadrature

Magazine de mathématiques pures et épicées

Quadrature, magazine de mathématiques pures et appliquées, **s'adresse aux enseignants, étudiants, ingénieurs, amateurs de mathématiques**.

La plupart des articles requièrent un bon niveau de terminale scientifique ou une première année de premier cycle. Les auteurs sont des mathématiciens, mais aussi des enseignants motivés et des étudiants.

Quadrature est éclectique : certains articles présentent des mathématiques toutes récentes, tandis que d'autres donnent un nouveau point de vue sur des sujets traditionnels ou encore ressuscitent des questions de géométrie ancienne ! On trouve également dans le magazine un **forum**, des **nouvelles**, des **notes de lecture**, des **articles d'histoire des mathématiques** et des **articles de réflexion en relation avec l'actualité**. Enfin, un large "coin des problèmes" permet aux lecteurs de poser des questions, qu'ils en connaissent la réponse ou pas.

Quadrature est ouvert, en particulier aux jeunes. Le magazine publie régulièrement des TPE (travaux personnels encadrés) de terminale et premier cycle d'université.

Nouveau

Abonnez-vous en ligne

www.quadrature-journal.org

BULLETIN D'ABONNEMENT

Quadrature

❒ Mme ❒ Mlle ❒ M.

Nom . . . . . .

Prénom . . . . . .

Profession . . . . . .

Institution . . . . . .

. . . . . .

Adresse . . . . . .

. . . . . .

. . . . . .

Code Postal . . . . . .

Ville . . . . . .

Pays . . . . . .

e-mail . . . . . .

Veuillez enregistrer mon abonnement :

❒ Pour **1 an** (4 numéros) :
- ❒ **Europe** (TVA 2,1 % incluse) . . . . . .33 €
- ❒ **Reste du monde** (Hors Taxe) . . . . . .38 €

❒ Pour **2 ans** (8 numéros) :
- ❒ **Europe** (TVA 2,1 % incluse) . . . . . .59 €
- ❒ **Reste du monde** (Hors Taxe) . . . . . .69 €

Paiement :

❒ Envoyez-moi une facture proforma
❒ Chèque joint (à l'ordre d'EDP Sciences)
❒ Carte de Crédit :
❒ Visa ❒ Eurocard ❒ American Express
Carte No . . . . . .
Date de validité . . . . . .

Date/Signature

Veuillez retourner ce coupon à :

EDP Sciences - Service Abonnement
17, avenue du Hoggar • B.P. 112 • PA de Courtabœuf • F-91944 Les Ulis Cedex A • France
Tél : 33 (0)1 69 18 75 75 • Fax : 33 (0)1 69 86 06 78 - E-mail : subscribers@edpsciences.org