

Rapport de l'équipe $\mathbb{KRD}$

$\mathbb{K}$arré d'or

Problème 8 : Graine de deck

Résumé

Dans ce problème, nous avons d'abord essayé de comprendre le phénomène en jouant avec de vrais cartes pour conjecturer et nous avons ensuite tenté de généraliser. Pour connaître le mélange, la méthode que nous avons employée est de réduire le nombre de place possible pour chaque carte au cours de parties successives. Nous avons répondu aux questions 1, 2, 3, 4 et 5. La 6, elle, n'est résolu qu'à moitié avec seulement le a).

Notations

Pour l'étude du présent problème, nous avons fait le choix d'utiliser la notion de permutation, figurant au programme de MPSI et de MP2I. Pour une introduction complète à cette notion, nous conseillons la lecture du polycopié intitulé « Groupe symétrique » de la classe MPSI du lycée Carnot, disponible ici en accès libre sous licence CC-BY-ND-SA.

Alternativement, nous proposons ici une synthèse des notions que nous avons fait le choix d'utiliser, faisant abstraction des considérations relatives à la structure de groupe de $\mathfrak{S}_n$.

Nous appellerons *permutation* de l'ensemble $[\![1\,;n]\!]$ toute fonction σ de $[\![1\,;n]\!]$ dans lui-même telle qu'à chaque $i \in [\![1\,;n]\!]$, σ associe un unique entier $\sigma(i)$ de l'ensemble $[\![1\,;n]\!]$. Nous notons :

Notation	Signification
$[\![1\,;n]\!]$	l'ensemble $\{1\,;\ldots\,;n\}$
$\mathfrak{S}_n$	l'ensemble des permutations de $[\![1\,;n]\!]$
$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$	la permutation associant $\sigma(i)$ à i pour tout $i \in [\![1\,;n]\!]$
$\sigma = (a_1, \ldots, a_n)$	la permutation transformant a_i en a_{i+1} pour tout $1 \leqslant i < n$ et a_n en a_1, dite *cyclique*
Supp σ	l'ensemble $\{a_1\,;\ldots\,;a_n\}$, si σ est un cycle, appelé support de σ
$\sigma\tau$	la permutation $\sigma \circ \tau$, avec $(\sigma, \tau) \in \mathfrak{S}_n^2$

Une *transposition* est un cycle de la forme (i, j) avec $i \neq j$.

Notion

Permutation σ : La notion de permutation permet de formaliser l'idée de mélange, ici de cartes. On peut l'écrire de la façon de l'énoncé : les positions initiales sur la ligne du haut, les positions finales leur correspondant en dessous ; ou bien en regroupant au sein d'une même parenthèse les modifications cycliques. Dans l'exemple ci-dessous, les deux écritures modélisent le même mélange.

$\begin{pmatrix} 123456 \\ 153246 \end{pmatrix}$	$\sigma = (245)(1)(3)(6)$
Le 1 reste en 1, le 2 passe en 5, le 3 reste en 3, le 4 prend la place du 5, le 5 celle du 2 et le 6 ne change pas de position.	Le 2 prend la place du 4, le 4 se retrouve en 5 et le 5 va en 2. 1, 3 et 6 ne changent pas de position.

Il existe différents types de permutations :
L'identité est la permutation qui "ne fait rien", c'est-à-dire que chaque carte est à la même place avant et après mélange. Ainsi pour n termes, on note : $\sigma = (1)(2)(3)\ldots(n)$
La permutation circulaire complète est une réorganisation qui fait se déplacer les cartes de 1 cran, sans en changer l'ordre entre elles. Par exemple $\sigma = (1, 2, 3, 4, \ldots, n-1, n)$ est la permutation par laquelle 1 devient 2, 2 devient 3, etc jusqu'à $n-1$ devient n et n devient 1.

Présentation

On peut résumer la situation de la manière suivante :

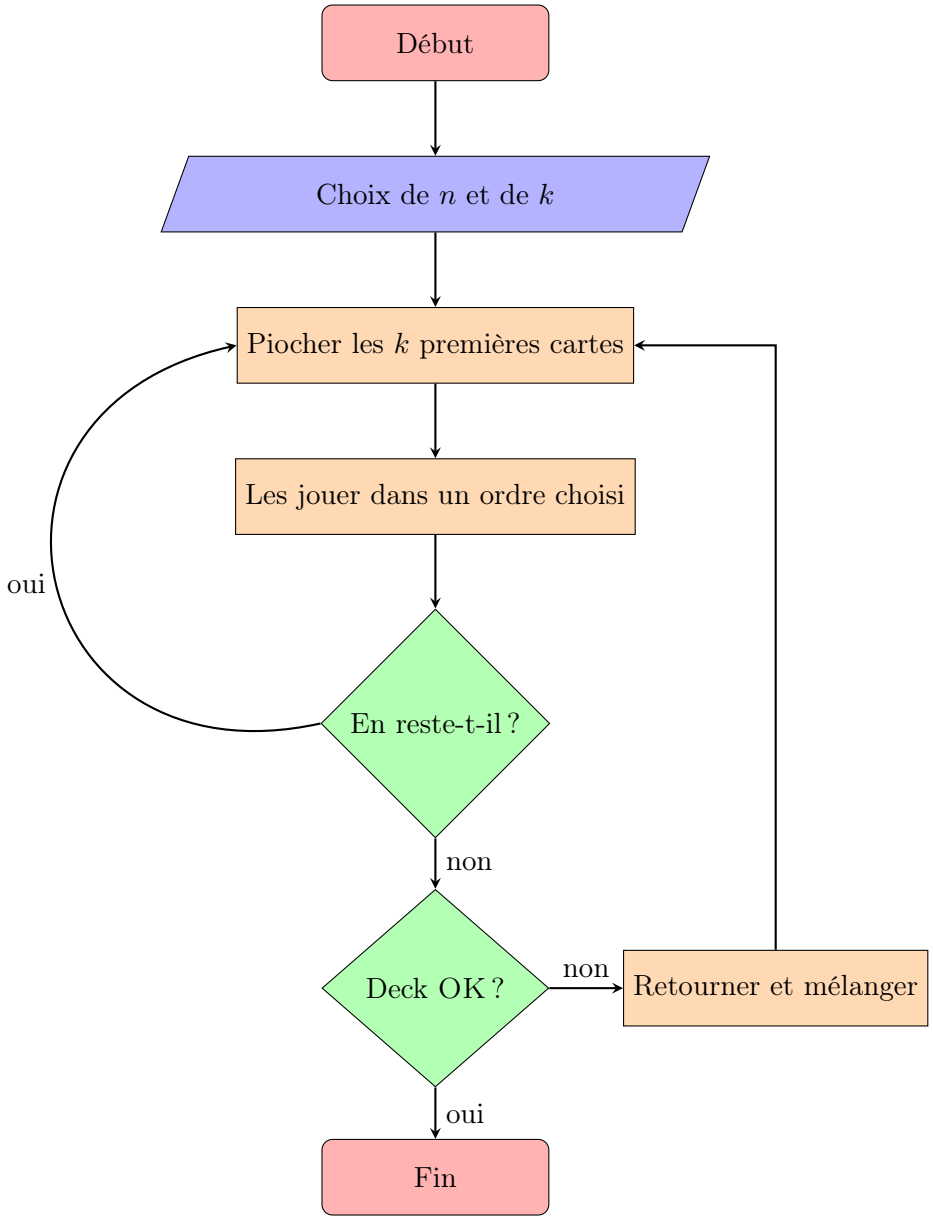

FIGURE 1 – Organigramme représentant la situation

1 Question 1

a) Pour $n = k$ et que toutes les cartes sont différentes, Nicolas connaît l'ordre initial, il peut par exemple jouer les cartes dans l'ordre de la pioche, et la place des cartes et la place finale de chaque carte, il connaît donc en un tour la permutation σ.

b) Pour $n = k$ et un deck de deux cartes différentes, notées A et B, avec A présente une unique fois et B toutes les autres, c'est-à-dire $n - 1$ fois, Nicolas connaît l'ordre avant de jouer (il peut choisir l'ordre car il a le deck entier en main). Il a pour unique solution de tester la place prise par la carte A, il ne peut distinguer ce que deviennent les cartes B qui

sont toutes identiques. Il convient donc de tester chaque position de A, une à chaque tour, soit il connaît σ en n parties. Cependant, on peut déduire la dernière position à partir des autres. Il a besoin de $n-1$ parties pour trouver σ.

c) $k = n$ avec n pair A en $n/2$ fois et B en $n/2$ fois.
A chaque partie jouée, on élimine la moitié des positions possibles pour chaque carte. Chaque partie peut réduire de moitié le nombre de places potentiellement prises par une carte. Donc si $a = \lceil \log_2(n) \rceil$, i.e. $2^{a-1} < n \leqslant 2^a$, on a besoin d'au moins a parties. Avec un tel a, on peut effectivement parvenir à trouver σ en a parties en regroupant les A et les B selon l'algorithme suivant : on numérote les places de 0 à $n-1$, donc avec $n-1 < 2^a$, puis à la p^{e} partie on met les A aux places ayant un 1 comme p^{e} chiffre dans leur écriture en binaire. De la sorte la succession de A et de B au cours des parties est uniquement déterminée par la place et on peut donc reconstituer σ. Exemple : pour $n = 4$, on choisit $BABA$ puis $BBAA$ et si on veut savoir $\sigma(1)$, on étudie la place numérotée 0 et donc son image est la position commune aux cartes B. Pour $n = 8$ on prend $BABABABA$, puis $BBAABBAA$ puis $BBBBAAAA$. Avec $n = 6$ on retire deux places complémentaires, i.e. ayant des écritures complémentaires, par exemple $1 = \overline{001}$ et $6 = \overline{110}$, ce qui donne $BBABAA$, $BAABBA$ et $BBBAAA$. Pour $n = 10$ on part de la situation pour $n = 16$ et on retire trois paires de places complémentaires, afin d'assurer qu'on a autant de A et que de B.

d) L'alternance parfaite entre A et B, et le fait que l'on joue les cartes deux par deux, impliquent que les cartes peuvent être jouées soit AB soit BA. Il est possible de combiner ces deux formes dans une même partie. Partons du deck $ABABAB\ldots$ Comme précédemment, on divise le deck en 2. On inverse l'ordre de la première moitié. On a alors $BABA\ldots BA$. Puis on divise la première moitié de deck en 2 parties (donc on obtient deux quarts de deck). On peut à nouveau inverser l'ordre des cartes dans le premier quart du deck (la première moitié de la première moitié). On répète cet algorithme jusqu'à obtenir une situation dans laquelle chaque carte ne peut occuper qu'une seule place. Il est en effet possible de répéter l'algorithme puisque le nombre de cartes est pair. On retombe bien sur $\lceil \log_2(n) \rceil$ comme dans la question c). Par exemple pour $n = 8$: $ABABABAB$, $BABAABAB$, $ABBABAAB$. Aussi, on supprime les paires répétitives si besoin. Par exemple pour $n = 6$, en supprimant la dernière paire : $ABABAB$, $BABAAB$, $ABBABA$. En conclusion, il faut que le nombre de parties soit le nombre d'itération de l'algorithme.

e) C'est une généralisation de la question c. On distingue plusieurs cas :
   - Si $a = 1$, il est impossible de trouver σ, car toutes les cartes étant identiques, il n'y a aucune différenciation des mélanges
   - Si $a = 2$, voir la question c.
   - Si a est un entier naturel quelconque divisant n. Cela revient à faire la décomposition en base a. On écrit $a^{m-1} < n \leqslant a^m$ et on numérote les cartes de 0 à $n-1$, donc avec m chiffres en base a, tous compris entre 0 et $a-1$. Chaque partie consiste à jouer les cartes dans l'ordre indiqué par les chiffres en base a, la p^{e} partie correspondant au p^{e} chiffre de l'écriture. Par exemple avec $n = 9$ et $a = 3$, on a deux parties : $AAABBBCCC$ puis $ABCABCABC$. Si $n = 6$ on supprime trois cartes obtenues par permutation circulaire des chiffres, e.g. $\overline{02} = 2$, $\overline{10} = 3$ et $\overline{21} = 7$, en permutant 0 en 1, 1 en 2 et 2 en 3. On retire donc les cartes en positions 3, 4 et 8, ce qui donne : $AABBCC$ puis $ABBCAC$.

2 Question 2 :

Si $k = n$ et deux cartes différentes, on peut trouver le mélange.

Si $k = \frac{n}{p}$ avec $p \in \mathbb{N}$, il faut au moins deux cartes différentes dans chaque partie. En effet, si σ est l'identité. On peut considérer chaque partie comme un jeu or, évidemment, s'il n'y a que des cartes identiques dans un jeu on ne peut par connaître le mélange.

3 Question 3 :

Si $k = n$ tout est faisable car on peut disposer les cartes comme on veut.

Si $k \neq n$ et l'on considère que l'objectif de l'ordre initial est obtenu sans même jouer, rien n'est réalisable hormis le positionnement de base, à l'ordre des cartes d'une partie P prêt. En effet, le mélange peut boucler au sein de chaque partie empêchant donc tout transfert de cartes.

Si $k \neq n$ et l'on considère que l'objectif de l'ordre initial n'est pas obtenu sans même jouer, il faut prouver que l'on peut l'obtenir après un nombre n de mélanges. Si tous les paquets sont identiques, il semble que peut importe σ on peut obtenir l'ordre initial après un certain nombre de mélanges. Il faut donc en plus que $\mathscr{O}$ soit composé de $\frac{n}{k}$ parties identiques.

Si $k \neq n$, $\mathscr{O}$ n'est pas composé de $\frac{n}{k}$ parties identiques et l'on considère que l'objectif de l'ordre initial est obtenu sans même jouer, il semble que aucun objectif ne soit réalisable car avec σ l'identité on ne peut que faire l'ordre initial et si $\mathscr{O}$ n'est pas composé de $\frac{n}{k}$ parties identiques, on n'est pas sûr avec les autres mélanges que l'ordre initial soit forcément réalisable. Il semble donc que rien n'est faisable.

4 Question 4 :

Comme évoqué précédemment, le mélange qui limite le plus dans les deux cas est celui qui boucle au sein de chaque partie. On a donc $\sigma = (1;2)(3;4)\dots(n-3;n-2)(n-1;n)$, par exemple avec 4 cartes on peut avoir $\sigma = (1,2)(3,4)$. Cependant, pour les autres σ, on peut remarquer qu' à partir du moment où deux cartes issu de deux parties différentes arrivent dans la même partie, alors on a peut faire plus d'objectif, il faut donc que les parties soient échangées entre elles. Il y a donc tous les mélanges qui ne font que inter-changer les parties. En effet, on peut jouer les cartes dans l'ordre que l'on veut au sein d'une même partie et ainsi appliquer la transformation $(2i-1, 2i)$. Soit G l'ensemble de ses transformations, il faut que pour chaque élément g de l'ensemble σ et $\sigma \circ g$ donnent le même résultat, en termes de paquets. Or le résultat de $\sigma \circ g$ est aussi celui de $g^{-1} \circ \sigma \circ g$. On remarque que $g^{-1} = g$. Il faut donc que l'image $(2i-1, 2i)$ soit invariante par l'échange de $2i-1$ et $2i$.

5 Question 5 :

À contrario, le mélange qui rend le plus de choses possibles est celui qui permet de changer les cartes entre chaque partie, et qui ne renvoie pas une partie sur une autre, c'est-à-dire un mélange qui scinde les parties. La permutation circulaire complète marche donc. En fait si on regarde le jeu à l'arrivée, il est dans l'ordre $(\sigma^{-1}(1), \sigma^{-1}(2), \dots)$. Comme $(\sigma \circ g)^{-1} = g^{-1} \circ \sigma^{-1} = g \circ \sigma^{-1}$, le but est donc de savoir si les antécédents de (1,2) sont dans la même partie ou pas. C'est possible pour la permutation circulaire (1, 2, . . . , n), donc le maximum est atteint. Notons tout de même qu'il existe de multiples permutations totale qui permettent la même chose.

6 Question 6 :

On peut poser que si on connaît le mélange alors on saura si l'objectif est réalisable.

a) Il suffit d'une seule partie car comme toute les cartes sont différentes, il peut connaître le mélange en une seule fois.