CHAPITRE 22

GROUPE SYMÉTRIQUE

Rappel 0.1

Soit E un ensemble. L'ensemble des permutations de E, *i.e.* les bijections de E dans E, forme un groupe pour la composition, appelé *groupe symétrique de* E.

Pour tout $n \in \mathbb{N}^*$, on note S_n le groupe symétrique de $[\![1, n]\!]$. Pour $\sigma, \tau \in S_n$, on note $\sigma\tau$ à la place de $\sigma \circ \tau$ s'il n'y a pas d'ambigüité.

1. Motivation

On considère un jeu de N cartes distinctes que l'on veut mélanger. On procède pour cela à un *battage par insertion* : on prend la première carte (celle du dessus) du paquet, et on la place aléatoirement dans le paquet de façon équiprobable ; on reproduit ce schéma T fois. Peut-on obtenir un jeu bien mélangé de cette façon ?

On peut modéliser le mélange par un élément de S_N : on numérote de 1 à N les cartes dans l'ordre initial du jeu ; après un mélange, ces cartes sont dans un autre ordre. On note alors pour toute carte i, $\sigma(i)$ la position dans le paquet de la carte i. L'application σ est bien une bijection de $[\![1, N]\!]$ dans lui-même.

On dira que le jeu est *bien mélangé* si après T insertions, toutes les permutations sont équiprobables. On travaille donc dans un espace probabilisé (Ω, P_T) où $\Omega = S_N$ et pour tout $\sigma \in S_N$, $P_T(\sigma)$ est la probabilité qu'après T insertions, le paquet se trouve dans la configuration décrite par σ.

On peut modéliser la succession d'insertions par une *chaîne de Markov* :

— on note pour tout $t \in \mathbb{N}$ et $\sigma \in S_N$, X_t^σ l´événement "après t insertions, le paquet est dans la configuration donnée par σ"

— pour toutes permutations σ, σ', $P(X_{t+1}^{\sigma'} | X_t^\sigma) = \dfrac{1}{N}$ s'il existe une insertion de la carte en position 1 dans le paquet qui amène ce paquet dans la configuration σ', et 0 sinon.

La première étape consiste donc à décrire en termes de permutations l'action d'insérer la carte du dessus du paquet.

Notation 1.1

On peut représenter une permutation $\sigma \in S_N$ par

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & N \\ \sigma(1) & \sigma(2) & \cdots & \sigma(N) \end{pmatrix}$$

On considère que le paquet est dans la configuration σ, et qu'après insertion de carte du dessus du paquet en position k, le paquet est en position σ'. Alors

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & \cdots & k & k+1 & \cdots & N \\ k & 1 & 2 & \cdots & k-1 & k+1 & \cdots & N \end{pmatrix} \sigma$$

Pour tout k, on pose $\gamma_k = \begin{pmatrix} 1 & 2 & 3 & \cdots & k & k+1 & \cdots & N \\ k & 1 & 2 & \cdots & k-1 & k+1 & \cdots & N \end{pmatrix}$.

On se pose donc maintenant deux questions :

(1) Toute permutation peut-elle s'écrire comme un produit de γ_k, $k \in [\![1, N]\!]$?

(2) Existe-t-il un entier T tel que $A^T = \dfrac{1}{N!}(1)_{1 \leq i,j \leq N!}$ où A est la matrice de transition de la chaîne de Markov ?

Exemple 1.2

On va traiter l'exemple de $N = 3$ ($N!$ croît très rapidement !).
Le groupe S_3 est constitué de 6 permutations :

$$\sigma_0 = \mathrm{id}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

On remarque que $\gamma_1 = \mathrm{id} = \sigma_0$, $\gamma_2 = \sigma_1$ et $\gamma_3 = \sigma_5$. On a donc
— $\sigma_0 = \gamma_1$
— $\sigma_1 = \gamma_2$
— $\sigma_2 = \gamma_2\gamma_3$
— $\sigma_3 = \gamma_3\gamma_2$
— $\sigma_4 = \gamma_3^2$
— $\sigma_5 = \gamma_3$
Ainsi, toutes les permutations sont atteintes après 2 insertions au plus.
La matrice de transition A est :

$$A = (P(X_{t+1}^{\sigma_i} | X_t^{\sigma_j}))_{1 \leq i,j \leq 6} = \frac{1}{3} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Le calcul des puissances de A ne permet pas de trouver T, mais on constate que (A^t) converge la matrice dont toutes les colonnes sont égales à $\frac{1}{N!} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$. Par exemple, $A^5 = \begin{pmatrix} \frac{41}{243} & \frac{41}{243} & \frac{40}{243} & \frac{40}{243} & \frac{40}{243} & \frac{41}{243} \\ \frac{41}{243} & \frac{41}{243} & \frac{41}{243} & \frac{40}{243} & \frac{40}{243} & \frac{40}{243} \\ \frac{40}{243} & \frac{40}{243} & \frac{41}{243} & \frac{41}{243} & \frac{41}{243} & \frac{40}{243} \\ \frac{40}{243} & \frac{41}{243} & \frac{40}{243} & \frac{41}{243} & \frac{40}{243} & \frac{41}{243} \\ \frac{41}{243} & \frac{40}{243} & \frac{41}{243} & \frac{40}{243} & \frac{41}{243} & \frac{40}{243} \\ \frac{40}{243} & \frac{40}{243} & \frac{40}{243} & \frac{41}{243} & \frac{41}{243} & \frac{41}{243} \end{pmatrix}$.

Définition 1.3

L'*ordre* d'une permutation σ est le plus petit entier r strictement positif tel que $\sigma^r = \mathrm{id}$.

2. Décompositions remarquables d'une permutation

Définition 2.1

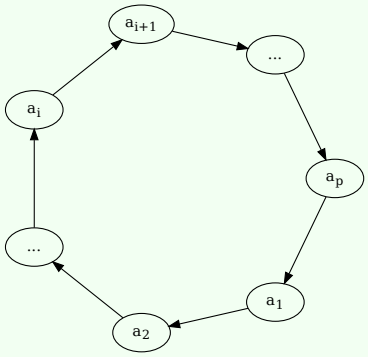
Le *support* d'une permutation $\sigma \in S_n$ est l'ensemble $\{i \in S_n \mid \sigma(i) \neq i\}$.

Définition 2.2

Soit $a_1, \cdots, a_p$ des entiers distincts de $[\![1, n]\!]$ et $\sigma \in S_n$ la permutation définie par :

$$\begin{cases} \forall x \notin \{a_i \mid 1 \leq i \leq p\},\ \sigma(x) = x \\ \forall i \in [\![1, p-1]\!],\ \sigma(a_i) = a_{i+1} \\ \sigma(a_p) = a_1. \end{cases}$$

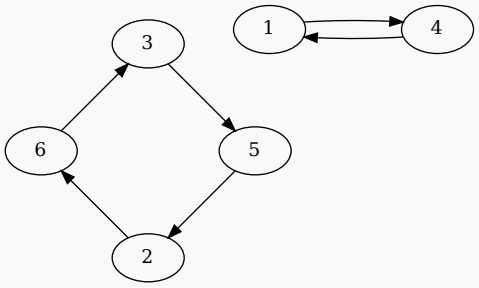
On dit que σ est un *p-cycle* et on note $\sigma = (a_1\ a_2\ \cdots\ a_p)$.



Exemple 2.3

(1) La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ est le 4-cycle $(1\quad 2\quad 4\quad 3)$.

(2) La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 5 & 1 & 2 & 3 & 7 & 8 \end{pmatrix}$ n'est pas un cycle, mais on peut le décomposer en un produit de cycles :



$\sigma = (1\quad 4)(2\quad 6\quad 3\quad 5)$.

Proposition 2.4

L'ordre d'un cycle est le cardinal de son support.

Proposition 2.5

Deux cycles à supports disjoints commutent.

Proposition 2.6

Soient $\gamma = (a_1\quad a_2\quad \cdots\quad a_p)$ un p-cycle et $\sigma \in S_n$. Alors

$$\sigma\gamma\sigma^{-1} = (\sigma(a_1)\quad \sigma(a_2)\quad \cdots\quad \sigma(a_p)).$$

Réciproquement, deux p-cycles quelconques sont conjugués.

Définition 2.7

Soit σ une permutation de S_n et $a \in [\![1, n]\!]$. L'orbite de a par σ est $\{\sigma^k(a) \mid k \in \mathbb{N}\}$.

Théorème 2.8

Toute permutation se décompose de façon unique comme produit de cycles à supports disjoints.

Corollaire 2.9

L'ordre d'une permutation est le PPCM des ordres des cycles qui la composent.

Définition 2.10

On appelle *transposition* tout cycle d'ordre 2.

Proposition 2.11

Tout cycle peut de décomposer comme produit de transpositions (mais cette décomposition n'est pas unique.)

Corollaire 2.12

Toute permutation peut se décomposer comme un produit de transpositions.

On cherchait dans la Section 1 s'il est possible d'écrire toute permutation comme produit des cycles γ_k.

(1) Montrer que toute transposition peut s'écrire comme produit de transpositions *simples* : une transposition simple de S_n est de la forme $(i\ i+1)$ avec $i < n$ ou $(n\ 1)$.

(2) Montrer que pour toute transposition simple τ, il existe $k \in \mathbb{N}$ tel que $\tau = \gamma^k(1\ 2)\gamma^{-k}$ où $\gamma = (1 \quad 2 \quad \cdots \quad n)$.

(3) En déduire que toute permutation peut s'écrire comme produit de γ_2 et γ_n.

3. Signature d'une permutation

Remarque 3.1

Il y a en général plusieurs façons de décomposer une permutation en produit de transpositions, et le nombre de transpositions qui intervient est lui aussi variable, mais on va voir que ce n'est pas le cas de sa parité.

Définition 3.2

Soit $\sigma \in S_n$. On appelle *inversion* de σ tout couple $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.
La *signature* de σ est $(-1)^i$ où i est le nombre d'inversions de σ. On note ce nombre $\varepsilon(\sigma)$.

Proposition 3.3

L'application $\varepsilon : (S_n, \circ) \to (\{-1, 1\}, \times)$ est un morphisme de groupes.

Corollaire 3.4

Quelle que soit la décomposition d'une permutation en produit de transpositions, celle-ci fait intervenir un nombre pair de transpositions si $\varepsilon(\sigma) = 1$ et un nombre impair de transpositions si $\varepsilon(\sigma) = -1$.

Définition 3.5

On dit qu'une permutation est *paire* si sa signature vaut 1, et *impaire* si elle vaut -1.

Proposition 3.6

L'ensemble des permutations paires est un sous-groupe de S_n.

Remarque 3.7

L'ensemble des permutations impaires n'est pas un sous-groupe de S_n : le produit de deux transpositions impaires est paire.

1. Marche aléatoire sur le groupe symétrique

Soit $N \in \mathbb{N}^*$. Le problème de battage de cartes comme énoncé en Section 1 est un exemple de marche aléatoire sur le groupe symétrique S_N : on démarre en la permutation id, et à chaque étape on peut atteindre une permutation donnée avec une certaine probabilité qui dépend uniquement de la permutation courante.

Ceci correspond donc à une chaîne de Markov dont les états sont les éléments de S_N.

Définition 1.1

On dit qu'une chaîne de Markov est *irréductible* si pour tous états x et y, la probabilité d'atteindre au moins une fois y en partant de x est strictement positive.

On dit qu'elle est *apériodique* si pour tout état x, la probabilité de rester en x au tour suivant est non nulle.

On dit que π est une *loi invariante* si π est un vecteur de probabilité et $T\pi = \pi$ où T est la matrice de transition de la chaîne de Markov.

Le *Théorème ergodique* affirme qu'une chaîne de Markov irréductible et apériodique possédant une loi invariante converge vers celle-ci en loi.

1.1. Battage de cartes. Nous allons montrer que la chaîne de Markov correspondant au battage de cartes est irréductible, apériodique et que la probabilité uniforme est invariante.

Comme toute permutation peut s'écrire comme produit des γ_k, le chaîne est bien irréductible. De plus, pour toute permutation σ, la probabilité de rester en σ vaut $\frac{1}{N}$, donc la chaîne est apériodique.

On pose $\pi = \frac{1}{N!}\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}$. Montrons que π est invariante. On obtient $T\pi$ en ajoutant toutes les colonnes de T et en multipliant par $\frac{1}{N!}$. Or, la chaîne de Markov est réversible, donc la transposée de T est la matrice de transition de la chaîne de Markov traversée dans l'autre sens. Or, la somme des lignes d'une matrice de transition vaut $(1 \quad 1 \quad \cdots \quad 1)$ donc π est bien invariante.

D'après le théorème ergodique, si on bat le jeu de cartes par insertion une infinité de fois, le paquet finit par être bien mélangé.

1.2. Décoder un texte crypté par substitution. Consulter http ://probability.ca/jeff/ftpdir/decipherart.pdf