1. Marches aléatoires sur $\mathfrak{S}(N)$ et représentations des groupes finis

① Permutations et marches aléatoires

notations : $[\![1, N]\!] = \{1, 2, 3, \dots, N\}$

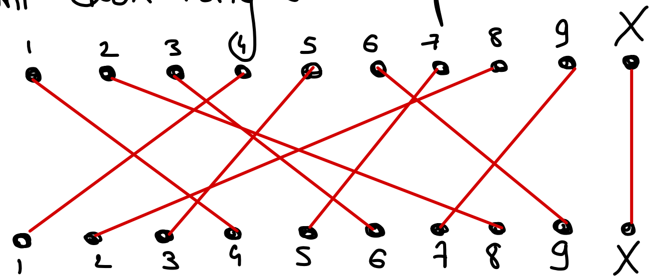
$\mathfrak{S}(N) = \{ \text{bijections } \sigma : [\![1, N]\!] \longrightarrow [\![1, N]\!] \} = \{ \text{permutations de taille } N \}$

On peut représenter une permutation de multiples façons :

- comme un mot de taille N.

$$\sigma = 4\,8\,6\,1\,3\,9\,5\,2\,7\,X$$

- par un diagramme reliant deux rangées de points



- comme un produit de cycles disjoints :

$$\sigma = (1, 4)(2, 8)(3, 6, 9, 7, 5)(X)$$

L'ensemble $\mathfrak{S}(N)$ a pour cardinal $N! = 1 \times 2 \times \dots \times N$.

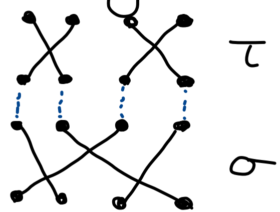
<u>exemple</u> : $\mathfrak{S}(3) = \left\{ \underset{\mathrm{id}}{123} \,;\, \underset{(2,3)}{132} \,;\, \underset{(1,2)}{213} \,;\, \underset{(1,2,3)}{231} \,;\, \underset{(1,3,2)}{312} \,;\, \underset{(1,3)}{321} \right\}$

C'est un groupe pour la composition : $\sigma\tau = \sigma \circ \tau$

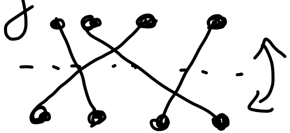
σ^{-1} = inverse de la bijection σ

Au niveau des diagrammes :

$\sigma\tau =$



; σ^{-1} : renverser le diagramme de σ



On se donne une mesure de probabilité μ sur $\mathfrak{S}(N)$

<u>Définition</u> La marche aléatoire de générateur μ sur $\mathfrak{S}(N)$ est

la suite de permutations aléatoires $(\sigma_n)_{n\in\mathbb{N}}$ définie par la relation de récurrence :

$\sigma_0 = id_{[\![1,N]\!]}$, $\sigma_n = \sigma_{n-1}\circ\tau_n$, où les τ_n sont iiD de loi μ.

<u>exemple</u> : On considère <u>un</u> paquet de cartes initialement ordonnées et numérotées de 1 à N. À chaque instant $n \geq 1$, on tire au hasard i_n et j_n uniformément dans $[\![1,N]\!]$, et on échange la i_n-ième carte du paquet avec la j_n-ième (si $i_n \neq j_n$).

$$\begin{array}{ccc}
\sigma_{n-1}(1) & & \sigma_{n-1}(1) \\
\vdots & & \vdots \\
\sigma_{n-1}(i_n) & & \sigma_{n-1}(j_n) \\
\vdots & \longrightarrow & \vdots \\
\sigma_{n-1}(j_n) & & \sigma_{n-1}(i_n) \\
\vdots & & \vdots \\
\sigma_{n-1}(N) & & \sigma_{n-1}(N) \\
\text{temps } n-1 & & \text{temps } n
\end{array}
\quad = \sigma_n$$

C'est la marche aléatoire sur $\mathfrak{S}(N)$ avec :

$$\mathbb{P}[\tau_n = (i,j)] = \frac{2}{N^2} \quad \forall i<j$$

$$\mathbb{P}[\tau_n = id_{[\![1,N]\!]}] = \frac{1}{N}.$$

Proposition : Notons μ_n la loi de σ_n, $(\sigma_n)_{n\in\mathbb{N}}$ MA de générateur μ.

1. $(\sigma_n)_{n\in\mathbb{N}}$ est une chaîne de Markov sur $\mathfrak{S}(N)$.
2. Supposons $\mu(id) > 0$, et μ supportée par un ensemble S qui engendre $\mathfrak{S}(N)$: $\mathfrak{S}(N) = \bigcup_{n\geq 1} S^n$.

Alors, $\mu_n \xrightarrow[n\to+\infty]{}$ loi uniforme $\frac{1}{N!}$ (chaîne ergodique).

Preuve : 1. $\mathbb{P}[\sigma_1 = \rho_1, \sigma_2 = \rho_2, \dots \sigma_n = \rho_n]$

$$= \mathbb{P}[\tau_1 = \rho_1, \tau_2 = \rho_1^{-1}\rho_2, \dots \tau_n = \rho_{n-1}^{-1}\rho_n]$$

$$= \mu(\rho_1)\,\mu(\rho_1^{-1}\rho_2)\dots\mu(\rho_{n-1}^{-1}\rho_n)$$

$\longrightarrow$ chaîne de Markov avec matrice de transition $P(\sigma,\rho) = \mu(\sigma^{-1}\rho)$.

2. Sous ces hypothèses, la chaîne est irréductible apériodique.

$\longrightarrow$ convergence vers l'unique mesure μ_∞ invariante.

Vérifions que la loi uniforme $\pi(\sigma) = \frac{1}{N!}$ est invariante.

$$(\pi P)(\sigma) = \sum_{\rho \in \mathfrak{S}(N)} \pi(\rho)\, \mu(\rho^{-1}\sigma) = \frac{1}{N!} \sum_{\rho \in \mathfrak{S}(N)} \mu(\rho^{-1}\sigma) = \frac{1}{N!} \times 1 = \pi(\sigma). \quad \square.$$

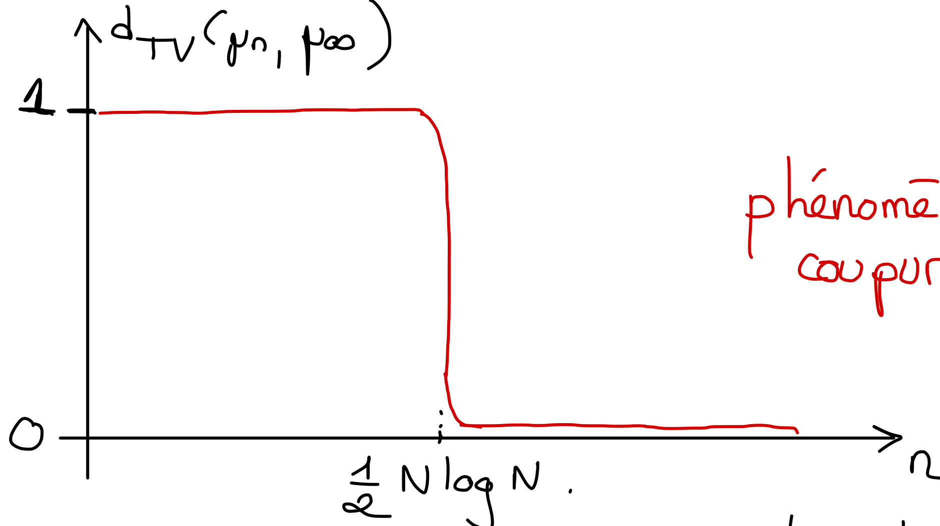
<u>Question</u> : peut-on calculer la distance entre μ_n et μ_∞ ?

par exemple, la distance en variation totale

$$d_{TV}(\mu_n, \mu_\infty) = \sup_{A \subset \mathfrak{S}(N)} \left| \mu_n(A) - \mu_\infty(A) \right|$$

$$= \sup_{A \subset \mathfrak{S}(N)} \left| \mu_n(A) - \frac{|A|}{N!} \right| .$$

<u>spoiler</u> :



phénomène de coupure.

On va développer des techniques générales pour démontrer ce genre de résultats.

Il est utile d'introduire l'algèbre du groupe symétrique. Soit G un groupe fini (ensemble avec produit associatif, neutre e_G et inverses), de cardinal $|G| = \text{card}\, G$.

Définition L'algèbre de G est l'espace vectoriel $\mathbb{C}[G] = \mathbb{C}G$ des combinaisons linéaires formelles $\sum_{g \in G} c_g\, g$, les $c_g \in \mathbb{C}$.

C'est un espace de dimension $\dim \mathbb{C}G = |G|$.

Le produit

$$\sum_{h \in G} c_g\, g \times \sum_{h \in G} d_h\, h = \sum_{h,g} \underbrace{c_g d_h}_{\text{produit de nombres complexes.}} \cdot \underbrace{(gh)}_{\text{produit dans } G}$$

fait de $\mathbb{C}G$ une algèbre (en général non commutative, unitaire : $1 = e_G$).

exemple $G = \mathfrak{S}(2)$, $x = \mathrm{id} - (1,2) \in \mathbb{C}\mathfrak{S}(2)$

$$x^2 = (\mathrm{id} - (1,2))(\mathrm{id} - (1,2)) = \mathrm{id} - (1,2) - (1,2) + \mathrm{id}$$

$$= 2\,\mathrm{id} - 2 \cdot (1,2) = 2x.$$

Lien avec les marches aléatoires : si $(\sigma_n)_{n\in\mathbb{N}}$ a générateur μ, on peut voir $\mu = \sum_{\sigma\in\mathfrak{S}(N)} \mu(\sigma).\sigma$ comme un élément de $\mathbb{C}\mathfrak{S}(N)$.

De même pour la loi marginale μ_n de σ_n :

$$\mu_n = \sum_{\sigma\in\mathfrak{S}(N)} \mu_n(\sigma)\sigma = \sum_{\sigma\in\mathfrak{S}(N)} \mathbb{P}[\sigma_n = \sigma].\sigma.$$

Alors : $\boxed{\mu_n = \mu^n}$ dans $\mathbb{C}\mathfrak{S}(N)$.

En effet, c'est clair au rang $n = 1$, et si c'est vrai au rang n, alors au rang $n+1$:

$$\mu_{n+1} = \sum_{\sigma\in\mathfrak{S}(N)} \mathbb{P}[\sigma_{n+1} = \sigma].\sigma$$

$$= \sum_{\rho, \sigma \in \mathfrak{S}(N)} \mathbb{P}[\sigma_n = \rho] \, \mathbb{P}[\sigma_{n+1} = \sigma \mid \sigma_n = \rho] \, \sigma$$

$$= \sum_{\rho, \sigma \in \mathfrak{S}(N)} \mu_n(\rho) \, \mu(\rho^{-1}\sigma) \, \sigma \qquad \hookrightarrow = \rho \cdot \rho^{-1}\sigma$$

$$= \sum_{\rho, \tau \in \mathfrak{S}(N)} \mu_n(\rho) \, \mu(\tau) \, . \, \rho\tau$$

$$= \left(\sum_{\rho} \mu_n(\rho) . \rho \right) \left(\sum_{\tau} \mu(\tau) . \tau \right) = \mu_n \times \mu .$$

$$= \mu^{n+1} \qquad \square$$

<u>exemple</u> : Le générateur de la MA associé aux produits de transpositions aléatoires est :

$$\mu = \frac{1}{N} \, id_{[\![1,N]\!]} + \frac{2}{N^2} \sum_{1 \le i < j \le N} (i, j)$$

autres générateurs intéressants :

- $\mu = \frac{1}{N}\,\mathrm{id} + \frac{1}{N}\sum_{i=2}^{N} (1, i)$

  $\Leftrightarrow$ échanger une carte choisie au hasard dans $[\![1, N]\!]$ avec la carte du haut du paquet.

- $\mu = \frac{1}{N}\,\mathrm{id} + \frac{1}{N}\sum_{i=2}^{N} (i-1, i)$

  $\Leftrightarrow$ échanger deux cartes adjacentes au hasard

- $\mu = \frac{1}{N}\,\mathrm{id} + \frac{1}{N}\sum_{i=2}^{N} (i, i-1, i-2, \dots 1)$

  $\Leftrightarrow$ placer la carte du haut au hasard à la $i \in [\![1, N]\!]$ ième position.

idée : on veut calculer μ^n pour $\mu \in \mathbb{C}G$ arbitraire.

$\mathbb{C}G$ est une algèbre complexe de dimension finie.

Si l'on avait une algèbre de matrices $\mathrm{Mat}(N, \mathbb{C})$, pour calculer M^n, on diagonaliserait M.

$\mathbb{C}G$ est-elle une algèbre de matrices ?

spoiler : presque. C'est une somme directe $\bigoplus \mathrm{End}(V^\lambda)$

(isomorphe à)

On verra par exemple que

$$\mathbb{C}\mathfrak{S}(3) \underset{\text{iso}}{\simeq} M(1, \mathbb{C}) \oplus M(1, \mathbb{C}) \oplus M(2, \mathbb{C})$$

avec un isomorphisme canonique.

2. Représentations d'un groupe fini

G = groupe fini

Définition Une représentation de G (linéaire, complexe) est la donnée d'une paire (V, ρ) avec :

- V espace vectoriel complexe de dimension $\dim V$ finie.
- ρ morphisme de groupes $G \longrightarrow \underbrace{GL(V)}_{\text{applications linéaires inversibles}}$

$$\rho(e_G) = \mathrm{id}_V \; ; \; \rho(gh) = \rho(g) \circ \rho(h).$$

Si $g \in G$ et $v \in V$, on note souvent $\rho(g)(v) = g \cdot v$.

Plus généralement, pour $x = \sum_{g \in G} c_g \cdot g$ et $v \in V$, on peut considérer

$$x \cdot v = \sum_{g \in G} c_g \cdot g \cdot v.$$ Alors, $(xy) \cdot v = x \cdot (y \cdot v)$.

produit dans $\mathbb{C}G$

<u>remarque</u> (si vous connaissez le langage des modules)

Une représentation (ρ, V) de G est donc équivalente à une structure de $\mathbb{C}G$-module sur l'espace vectoriel V.

<u>constructions</u> :

1) Un morphisme (resp., un isomorphisme) entre deux représentations (V_1, ρ_1) et (V_2, ρ_2) de G est une application linéaire (resp., une application linéaire inversible) $\phi : V_1 \to V_2$ telle que

$$g \cdot_2 \phi(v) = \phi(g \cdot_1 v) \quad \forall g \in G, \ \forall v \in V_1.$$

$\iff$ commutativité de

$$\begin{tikzcd} V_1 \arrow[r, "\phi"] \arrow[d, "\rho_1(g)"'] & V_2 \arrow[d, "\rho_2(g)"] \\ V_1 \arrow[r, "\phi"] & V_2 \end{tikzcd}$$

On classifiera bientôt les représentations de $G = \mathfrak{S}(N)$ à isomorphisme près.

2) Une sous-représentation W d'une représentation V de G est un sous-espace vectoriel $W \subset V$ tel que $g \cdot W = W$ $\forall g \in G$.

Une représentation V est dite irréductible si ces seules sous-représentations sont : $\left| \begin{array}{l} W = V \\ W = \{0\} \end{array} \right.$. (et si $\dim(V) \geq 1$)

<u>exemple</u> Le groupe $\mathfrak{S}(N)$ agit sur $\mathbb{C}^N$ par :

$$\sigma \cdot (x_1, \dots, x_N) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(N)})$$

On a bien $(\sigma \circ e) \cdot x = \sigma \cdot (e \cdot x)$.

On a donc une représentation de $\mathfrak{S}(N)$ de dimension N.

Une sous-représentation est donnée par l'hyperplan

$$W = \{ x \in \mathbb{C}^N \mid x_1 + x_2 + \dots + x_N = 0 \}.$$

$\dim V = N$, $\dim W = N-1$.

La représentation $V = \mathbb{C}^N$ n'est donc pas irréductible.

On verra que la sous-représentation W est irréductible.

3) Étant données des représentations $V_1, V_2, \dots, V_r$ de G, on peut former leur somme directe.

$$V_1 \oplus V_2 \oplus \dots \oplus V_r,$$

qui est une représentation de G pour

$$g \cdot (v_1 + v_2 + \dots + v_r) = g \cdot_1 v_1 + g \cdot_2 v_2 + \dots + g \cdot_r v_r.$$

Théorème (Maschke) Toute représentation V de G est une somme directe de représentations irréductibles.

Lemme si (V, ρ) est une représentation de G, $\exists$ un produit scalaire hermitien sur V telle que les applications $\rho(g)$ soient des isométries pour $\langle . | . \rangle$, $\forall g \in G$.

Preuve. On part d'un produit scalaire $(. | .)$ sur V et on forme

$$\langle v_1 | v_2 \rangle = \sum_{h \in G} (h \cdot v_1 | h \cdot v_2).$$

Alors, $$\langle g \cdot v_1 | g \cdot v_2 \rangle = \sum_{h \in G} (hg \cdot v_1 | hg \cdot v_2)$$
$$= \sum_{h' \in G} (h' \cdot v_1 | h' \cdot v_2) = \langle v_1 | v_2 \rangle. \quad \square.$$

Preuve du théorème de Maschke : On fixe $<\cdot|\cdot>$. Si V n'est pas irréductible, soit W sous-représentation non triviale. L'orthogonal $W^\perp = \{v \in V \mid <v|w> = 0 \ \forall w \in W\}$ est aussi une sous-représentation : si $v \in W^\perp$, alors

$$<g \cdot v | \underbrace{w}_{\in W}> = <v | \underbrace{g^{-1} \cdot w}_{\in W}> = 0 \ \forall w \in W \Rightarrow g \cdot v \in W^\perp.$$

On peut donc décomposer $V = W \oplus W^\perp$ (sous-représentations)

On conclut avec une récurrence sur $\dim V$. $\square$

→ unicité à isomorphisme près des composantes irréductibles d'une représentation $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$?

→ combien y-a-t'il de types de représentations irréductibles non isomorphes ?

Étant données deux représentations V, W de G, on pose

$$\hom_G(V, W) = \{ \text{morphismes de représentations } \phi : V \to W \}$$

C'est un espace vectoriel complexe.

Lemme (Schur) Si V et W sont irréductibles, alors

$$\dim(\hom_G(V, W)) = \begin{cases} 1 & \text{si } V \underset{\text{isomorphe}}{\simeq} W, \\ 0 & \text{sinon.} \end{cases}$$

Preuve. Si ϕ est un morphisme, on voit facilement que $\ker(\phi) \subset V$ sont $\mathrm{im}(\phi) \subset W$ des sous-représentations. Par conséquent :

- soit $\phi = 0$

- soit $\ker(\phi) = 0$ et $\operatorname{im}(\phi) = W \iff \phi$ est un isomorphisme de représentations.

Supposons $V \underset{\text{isom}}{\sim} W$. Si ϕ et $\psi \neq 0 \in \hom_G(V, W)$, alors $\psi^{-1} \circ \phi \in \hom_G(V, V)$ admet une valeur propre complexe $\lambda \in \mathbb{C}$. Dans ce cas,

$(\psi^{-1} \circ \phi - \lambda \, id_V) \in \hom_G(V, V)$ n'est pas un isomorphisme

$\implies \psi^{-1} \circ \phi - \lambda \, id_V = 0 \iff \phi = \lambda \psi$.

Donc, tous les isomorphismes de $\hom_G(V, W)$ sont proportionnels entre eux.

$\square$

Soit V une représentation de G. On scinde V en irréductibles et on réunit les composantes irréductibles par type d'isomorphisme :

$$V \underset{(\text{isom})}{=} \bigoplus_{\lambda \in \hat{G}} m_\lambda V^\lambda, \qquad m_\lambda \geq 0 \text{ entier}$$

$$m_\lambda V^\lambda = \underbrace{V^\lambda \oplus V^\lambda \oplus \cdots \oplus V^\lambda}_{m_\lambda \text{ fois}}.$$

dual de G = $\hat{G}$ = $\left\{ \text{classes d'isomorphisme de représentations irréductibles } \underbrace{(V^\lambda, \rho^\lambda)}_{\lambda} \text{ de } G \right\}$

Proposition : La multiplicité $m_\lambda = m_\lambda(V)$ est entièrement déterminée par V.

$\Longleftrightarrow$ unicité de la décomposition.

Preuve: $\dim \hom_G(V, V^\lambda) = \dim \hom_G\left(\bigoplus_{\mu \in \hat{G}} m_\mu(V) V^\mu, V^\lambda\right)$

$$= \sum_{\mu \in \hat{G}} m_\mu(V) \dim \hom_G(V^\mu, V^\lambda)$$

$$= m_\lambda(V). \qquad \square$$

Théorème: L'ensemble $\hat{G}$ est fini. Chaque $\lambda \in \hat{G}$ apparait comme composante de la représentation régulière de G avec multiplicité $\dim \lambda = \dim V^\lambda$.

$V = \mathbb{C}G$; action: $g \cdot \sum_{h \in G} c_h h = \sum_{h \in G} c_h (gh)$.

Preuve. Soit W une représentation arbitraire de G.

On considère l'application linéaire :

$$\Psi : \begin{array}{rcl} \hom_G(\mathbb{C}G, W) & \longrightarrow & W \\ \phi & \longmapsto & \phi(e_G). \end{array}$$

Ψ est un isomorphisme linéaire. En effet, si $\Psi(\phi) = 0$, alors $\phi(e_G) = 0$, d'où :

$$\phi\left(\sum c_g g\right) = \sum_{g \in G} c_g \, \phi(g \cdot e_G) \quad \text{(linéarité)}$$

$$= \sum_{g \in G} c_g \, g \cdot \phi(e_G) \quad \text{(ϕ morphisme de représentations)}$$

$$= 0 \implies \phi = 0 \implies \ker(\Psi) = \{0\}.$$

Par ailleurs, si $w \in W$, alors l'application linéaire

$$\phi : \mathbb{C}G \longrightarrow W \qquad \text{est dans } \hom_G(\mathbb{C}G, W)$$

$$\sum_{g \in G} c_g\, g \longmapsto \sum c_g\, (g \bullet w)$$

et vérifie $\Psi(\phi) = \phi(e_G) = e_G \bullet w = w$

$$\Longrightarrow \operatorname{im}(\Psi) = W.$$

Donc $\forall W$ représentation de G,

$$\dim(W) = \dim \hom_G(\mathbb{C}G, W).$$

En particulier, $\forall \lambda \in \hat{G}$,

$$m_\lambda(\mathbb{C}G) = \dim \hom_G(\mathbb{C}G, V^\lambda) = \dim V^\lambda = \dim \lambda \geq 1$$

Chaque irréductible est donc une composante de $\mathbb{C}G$. $\square$

<u>résumé</u> : $\{$représentations de G groupe fini$\}$

$$= \left\{ \sum_{\lambda \in \hat{G}} m_\lambda V^\lambda \text{ avec les } m_\lambda \in \mathbb{N} \right\}$$

où les V^λ sont les classes d'isomorphisme de composantes irréductibles de $\mathbb{C}G$.

<u>remarque</u> : D'après ce qui précède,

$$\mathbb{C}G = \bigoplus_{\lambda \in \hat{G}} (\dim \lambda)\, V^\lambda .$$

$\underset{\text{dimensions}}{\Longrightarrow}$ $$|G| = \sum_{\lambda \in \hat{G}} (\dim \lambda)^2$$ formule de Plancherel.

En particulier, $\mathbb{P}[\lambda] = \dfrac{(\dim \lambda)^2}{|G|}$ est une probabilité sur $\hat{G}$.

<u>exemple</u> : représentations de $\mathfrak{S}(3)$.

→ On a, pour tout groupe fini G, la représentation triviale de dimension 1

$V_{triviale} = \mathbb{C}$; $g \cdot x = x \quad \forall g \in G$.

→ Le groupe $\mathfrak{S}(N)$ agit aussi sur $\mathbb{C}$ par la représentation signature

$V_{signature} = \mathbb{C}$; $\sigma \cdot x = \varepsilon(\sigma)\, x$

$$\varepsilon(\sigma) = (-1)^{\#\text{ inversions de } \sigma} = (-1)^{N - \#\text{ cycles de } \sigma}.$$

→ Finalement $\mathfrak{S}(3)$ agit sur l'hyperplan $W = \{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 + x_2 + x_3 = 0\}$ par permutation des coordonnées (représentation géométrique)

$$6 = 1^2 + 1^2 + 2^2 \implies \widehat{\mathfrak{S}(3)} = (V_{triviale}, V_{signature}, V_{géométrique}).$$