Développement: Caractères et marches aléatoires dans les groupes abéliens.

Arthur Maritch-Roy

Dans ce développement, on s'intéresse à la transformée de Fourier discrète qui, comme dans le cas continu, permet de simplifier des calculs de lois de sommes de variables aléatoires indépendantes. Pour introduire la transformée de Fourier sur un groupe, on doit introduire ses caractères et son groupe dual (de la même manière que la transformée de Fourier d'une fonction L^1 définit un élément de son dual).

Dans toute la suite G désignera un groupe abélien fini de cardinal supérieur à 2.

Définition 1. Un *caractère* de G est un morphisme de G vers $(\mathbb{C}^*, \times)$. Le groupe formé des caractères de G est un groupe pour la multiplication est noté $\widehat{G}$ est appelé *groupe dual* de G. Puisque G est fini, les caractères sont en fait à valeurs dans les racines de l'unité, et en particulier sont donc de module 1.

Exemple 1. Les caractères de $\mathbb{Z}/N\mathbb{Z}$ sont les $\overline{x} \mapsto \mathrm{e}^{\frac{2ikx\pi}{N}}$ pour $\overline{k} \in \mathbb{Z}/N\mathbb{Z}$. On remarque que $\widehat{\mathbb{Z}/N\mathbb{Z}} \simeq \mathbb{Z}/N\mathbb{Z}$.

Remarque 1. Tout groupe abélien fini est isomorphe à son dual et canoniquement isomorphe à son bidual par $g \mapsto (\chi \mapsto \chi(g))$ par le théorème de structure des groupes abéliens finis.

Définition 2. Soit H un groupe abélien fini, on peut définir un produit scalaire sur $\mathbb{C}^H$ par la formule :

$$\langle f_1, f_2 \rangle_H = \frac{1}{|H|} \sum_{h \in H} \overline{f_1(h)} f_2(h).$$

Définition 3. Soit $f \in \mathbb{C}^G$. On définit $\widehat{f} \in \mathbb{C}^{\widehat{G}}$ par la formule :

$$\widehat{f}(\chi) := \sum_{g \in G} \overline{\chi(g)} f(g) = |G| \langle \chi, f \rangle_G.$$

Proposition 1. Les caractères forment une base orthonormée de $\mathbb{C}^G$.

Démonstration. Soient χ et ψ deux caractères de G. Alors remarquons que

$$\langle \chi, \psi \rangle_G = \langle \chi\overline{\psi}, 1 \rangle_G = \langle \chi\psi^{-1}, 1 \rangle_G.$$

Ainsi, pour montrer que la base est orthonormée, il suffit de montrer que $\langle \varphi, 1 \rangle_G = \delta_{\varphi,1}$ pour tout caractère φ. Soit donc un tel caractère, et $h \in H$ différent de 1.

$$\langle \varphi, 1 \rangle_G = \frac{1}{|G|} \sum_{g \in G} \varphi(g) = \frac{1}{|G|} \sum_{g \in G} \varphi(gh) = \varphi(h) \frac{1}{|G|} \sum_{g \in G} \varphi(g),$$

Si $\varphi(h)$ est différent de 1 pour un h, *i.e.* si $\varphi \neq 1$, on obtient $\frac{1}{|G|} \sum_{g \in G} \chi(g) = 0$ d'où le résultat. □

Proposition 2. (Égalité de Bessel-Parseval)
Pour toute fonction $f \in \mathbb{C}^G$, puisque la famille $\widehat{G}$ est une base orthonormée, on a

$$\sum_{g\in G} |f(g)|^2 = |G| \sum_{g\in G} |\langle \chi, f\rangle|^2 = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} |\widehat{f}(\chi)|^2.$$

Proposition 3. (Inversion de Fourier)
Soit $f \in \mathbb{C}^G$. Alors pour tout $g \in G$:

$$f(g) = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(g)\widehat{f}(\chi)$$

Démonstration. Il suffit de décomposer f dans la base orthonormée $\widehat{G}$:

$$f = \sum_{\chi\in\widehat{G}} \langle \chi, f\rangle_G \, \chi = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi.$$

$\square$

Remarque 2. On aurait pu aussi directement écrire :

$$\frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(g)\widehat{f}(\chi) = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \sum_{h\in G} \chi(g)\overline{\chi(h)}f(h) = \frac{1}{|G|} \sum_{h\in H} \left(f(h) \sum_{\chi\in\widehat{G}} \overline{\chi(h)}\chi(g) \right).$$

Ainsi, par isomorphisme canonique avec le bidual, on a $\sum_{\chi\in\widehat{G}} \overline{\chi(h)}\chi(g) = |G|\delta_{g,h}$, d'où le résultat. Toujours avec cet isomorphisme canonique avec le bidual, on peut écrire $f(g) = \langle g^{-1}, \widehat{f}\rangle_{\widehat{G}} = \frac{1}{|\widehat{G}|}\widehat{\widehat{f}}(g^{-1}) = \frac{1}{|G|}\widehat{\widehat{f}}(g^{-1})$.

Définition 4. On peut définir un produit de convolution (associatif, commutatif et distributif par rapport à $+$) sur $\mathbb{C}^H$ pour H un groupe abélien fini par la formule suivante :

$$(f_1 * f_2)(h) := \sum_{k\in G} f_1(k) f_2(hk^{-1}).$$

Proposition 4. Soient f_1 et f_2 deux fonctions de $\mathbb{C}^G$. Alors $\widehat{f_1 * f_2} = \widehat{f_1}\widehat{f_2}$.

Démonstration. Soit $\chi \in \widehat{G}$:

$$\begin{aligned}
\widehat{f_1 * f_2}(\chi) &= \sum_{g\in G} \overline{\chi(g)} (f_1 * f_2)(g) \\
&= \sum_{g\in G} \sum_{h\in G} \overline{\chi(g)} f_1(h) f_2(gh^{-1}) \\
&= \sum_{g\in G} \sum_{h\in G} \overline{\chi(gh^{-1})\chi(h)} \, f_1(h) f_2(gh^{-1}) \\
&= \sum_{g'\in G} \overline{\chi(g')} f_2(g') \sum_{h\in G} \overline{\chi(h)} f_1(h) \\
&= \widehat{f_1}(\chi)\widehat{f_2}(\chi).
\end{aligned}$$

où l'on a posé $g' = gh^{-1}$ qui réalise une bijection sur G. $\square$

On a maintenant tout ce qu'il nous faut pour faire des probabilités. On considère une particule sur $\mathbb{Z}/N\mathbb{Z} = (\overline{0}, \dots, \overline{N-1})$, initialement en $\overline{0}$. À chaque étape, la particule se déplace d'un cran vers la droite ou vers la gauche ou stationne de manière équiprobable. On peut modéliser cela par une chaîne de Markov dont la loi initiale est $\delta_{\overline{0}}$ et dont la loi de transition est $\mu = \frac{1}{3}(\delta_{-\overline{1}}+\delta_{\overline{0}}+\delta_{\overline{1}})$. La loi de X_n la position de la particule au rang n a pour loi

$$\mu_n = \mu_0 * \mu^{*n} = \mu^{*n}.$$

Théorème 5. La chaîne de Markov en question converge vers la loi uniforme notée μ_∞ et on a une approximation de la vitesse de convergence en variation totale :

$$\|\mu_n - \mu_\infty\|_{\mathrm{VT}} \leq \sqrt{N}\mathrm{e}^{-\frac{\pi^2 n}{N^2}}.$$

Démonstration. Tout l'intérêt de la transformée de Fourier discrète est de pouvoir passer cette équation dans le monde de Fourier :

$$\widehat{\mu_n} = \widehat{\mu}^n.$$

Calculons alors $\widehat{\mu}$. On utilise pour cela l'isomorphisme entre $\mathbb{Z}/N\mathbb{Z}$ et son dual :

$$\widehat{\mu}(\overline{k}) = \sum_{l=0}^{N-1} \mathrm{e}^{\frac{2\mathrm{i}kl\pi}{N}}\mu(\overline{l}) = \frac{1}{3}\left(1+\mathrm{e}^{-\frac{2\mathrm{i}k\pi}{N}}+\mathrm{e}^{\frac{2\mathrm{i}k\pi}{N}}\right) = \frac{1}{3}\left(1+2\cos\left(\frac{2k\pi}{N}\right)\right).$$

Ainsi, par inversion de Fourier, pour $\overline{l} \in \mathbb{Z}/n\mathbb{Z}$:

$$\mu_n(\overline{l}) = \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{e}^{\frac{2\mathrm{i}k\pi}{N}}\left(\frac{1}{3}\left(1+2\cos\left(\frac{2k\pi}{N}\right)\right)\right)^n.$$

Or $\frac{1}{3}|1+2\cos(\frac{2k\pi}{n})| = 1$ si et seulement si $k=0$ donc quand n tend vers l'infini : $\mu_n(\overline{l}) \sim \frac{1}{N}$. Ainsi la chaîne de Markov converge en loi vers la mesure uniforme $\mu_\infty = \frac{1}{N}\sum_{k=0}^{N-1}\delta_{\overline{k}}$ dont la transformée de Fourier est $\delta_{\overline{0}}$. Par Parseval, on a donc

$$\|\mu_n - \mu_\infty\|_2^2 = \frac{1}{N}\|\widehat{\mu_n} - \widehat{\mu_\infty}\|_2^2 = \frac{1}{N}\sum_{k=0}^{n-1}\left|\left(\frac{1}{3}\left(1+2\cos\left(\frac{2k\pi}{N}\right)\right)\right)^n - \delta_0(k)\right|^2.$$

Les termes en $k=0$ se simplifient et on a donc :

$$\|\mu_n - \mu_\infty\|_2^2 = \frac{1}{N}\sum_{k=1}^{N-1}\left(\frac{1}{3}\left(1+2\cos\left(\frac{2k\pi}{N}\right)\right)\right)^{2n}.$$

Le terme est maximal pour $k=1$ donc

$$\|\mu_n - \mu_\infty\|_2 \leq \left(\frac{1+2\cos(\frac{2\pi}{N})}{3}\right)^n.$$

Par Cauchy-Schwarz, on a alors

$$\|\mu_n - \mu_\infty\|_{\mathrm{VT}} \leq \sqrt{N}\left(\frac{1+2\cos(\frac{2\pi}{N})}{3}\right)^n.$$

Pour $x \in]0, \frac{\pi}{2}[$, on peut montrer que $\frac{1+2\cos(x)}{3} \leq 1 - \frac{x^2}{4} \leq \mathrm{e}^{-\frac{x^2}{4}}$. Ainsi, pour $N > 4$, on a la majoration suivante :

$$\|\mu_n - \mu_\infty\|_{\mathrm{VT}} \leq \sqrt{N}\mathrm{e}^{-\frac{\pi^2 n}{N^2}}.$$

□

Référence. Cours de chaînes de Markov de Pierre-Loïc Méliot, accessible ici.