Géométrie intégrale et racines de polynômes aléatoires

Thomas Letendre

Mini-cours de Rentrée de la FMJH
31 aout et 1 septembre 2022

Résumé

Dans ce mini-cours on s'intéressera à des problèmes de géométrie intégrale, aussi appelée théorie des probabilités géométriques. Notre premier objectif sera de démontrer la formule de Crofton, qui permet de calculer la longueur d'une courbe paramétrée dans l'espace euclidien comme le nombre moyen de points d'intersection entre cette courbe et un hyperplan affine choisi uniformément au hasard. Ce sera l'occasion de parler rapidement de mesures invariantes et de géométrie affine. Dans un second temps, nous utiliserons une variante de la formule de Crofton pour calculer le nombre moyen de racines réelles d'un polynôme aléatoire à coefficients gaussiens.

1 Introduction : l'aiguille de Buffon

Buffon est un scientifique français du $18^{\text{ème}}$ siècle, principalement naturaliste mais aussi philosophe, mathématicien... En 1777, il s'intéresse à la question suivante. Si on lance une aiguille au hasard sur un sol en parquet, quelle est la probabilité que l'aiguille intersecte la frontière entre deux lattes ?

1.1 Modélisation

Mathématiquement, les frontières entre les différentes lattes sont un ensemble F, formé de droites parallèles et séparées par une même distance D. Disons $F = \mathbb{R} \oplus D\mathbb{Z}$.
L'aiguille est un segment A (orienté du chas vers la pointe) de longueur ℓ. On considère $\ell < D$ de sorte que A rencontre au plus l'une des droites de F.
La position de l'aiguille A est décrite par :

- la position $(x, y) \in \mathbb{R}^2$ de son centre de gravité (le milieu du segment),
- l'angle $\theta \in]-\pi, \pi]$ entre la direction de A et le demi-axe horizontal positif.

Quitte à translater par un élément de $\mathbb{R} \oplus D\mathbb{Z}$, on peut supposer que $x = 0$ et $y \in]-\frac{D}{2}, \frac{D}{2}]$. La translation laisse F invariant et préserve le fait que A intersecte F ou non.
L'intersection éventuelle de A et F dépend uniquement de $(y, \theta) \in]-\frac{D}{2}, \frac{D}{2}] \times]-\pi, \pi]$. On va décrire un lancé aléatoire de A en supposant que y et θ sont deux variables aléatoires indépendantes uniformes, i.e. (y, θ) est distribuée selon la mesure de Lebesgue normalisée $\frac{1}{2\pi D}\, \mathrm{d}y \otimes \mathrm{d}\theta$.

1.2 Probabilité d'intersection

La projection du segment A sur l'axe vertical est l'intervalle $I = \left[y - \frac{\ell}{2}|\sin\theta|, y + \frac{\ell}{2}|\sin\theta|\right]$.
On a $\ell < D$ et $|y| \leqslant \frac{D}{2}$, donc $|y| + \frac{\ell}{2}|\sin\theta| < D$ et

$$A \cap F \neq \emptyset \iff A \cap (\mathbb{R} \times \{0\}) \neq \emptyset \iff 0 \in I \iff |y| \leqslant \frac{\ell}{2}|\sin\theta|.$$

On a donc

$$\mathbb{P}[A \cap F \neq \emptyset] = \mathbb{P}\left[|y| \leqslant \frac{\ell}{2}|\sin\theta|\right] = \frac{1}{2\pi D}\int_{-\pi}^{\pi}\int_{-\frac{\ell}{2}|\sin\theta|}^{\frac{\ell}{2}|\sin\theta|} \mathrm{d}y\,\mathrm{d}\theta = \frac{\ell}{\pi D}\int_0^{\pi}\sin\theta\,\mathrm{d}\theta = \frac{2\ell}{\pi D}.$$

En fait,

$$\#(A\cap F) = \begin{cases} 0 & \text{si } |y| > \frac{\ell}{2}|\sin\theta|, \\ 1 & \text{si } |y| \leqslant \frac{\ell}{2}|\sin\theta| \text{ et } \theta \neq 0, \\ +\infty & \text{si } y = 0 = \theta. \end{cases}$$

Le dernier cas étant de mesure nulle : $\mathbb{E}[\#(A\cap F)] = \mathbb{P}[A\cap F\neq\emptyset] = \frac{2\ell}{\pi D}$.
Cette dernière formule est le prototype des résultats de géométrie intégrale. Elle exprime une quantité géométrique déterministe, le quotient $\frac{\ell}{D}$, comme la moyenne d'une certaine variable aléatoire dont la valeur est très facile à observer (déterminer $\#(A\cap F)$ pour un tirage donné ne nécessite pas de calcul, déterminer une longueur si).

1.3 Application : calcul numérique de π

Supposons $\ell = \frac{D}{2}$. On note $X = \#(A\cap F)$ qui est une variable aléatoire dans $\{0,1\}$ d'espérance $\frac{1}{\pi}$.
Soit $(X_k)_{k\geqslant 1}$ une suite de variables aléatoires indépendantes de même loi que X.
Par la loi des grands nombres, presque surement : $\frac{1}{n}\sum_{k=0}^{n} X_k \xrightarrow[n\to+\infty]{} \mathbb{E}[X] = \frac{1}{\pi}$. Cela fournit une méthode expérimental de calcul de π. Cependant, par le théorème central limite :

$$\sqrt{n}\left(\frac{1}{n}\sum_{k=0}^{n} X_k - \mathbb{E}[X]\right) \xrightarrow[n\to+\infty]{\text{loi}} \mathcal{N}(0,1).$$

Moralement l'erreur $\frac{1}{n}\sum_{k=0}^{n} X_k - \mathbb{E}[X]$ est donc d'ordre $\frac{1}{\sqrt{n}}$. C'est très très mauvais : il faut de l'ordre de 10^{2k} lancés pour obtenir un résultat précis à 10^{-k} près.

1.4 Teaser : la formule de Crofton

Le premier objectif de ce mini-cours est de montrer le résultat de géométrie intégrale suivant, attribuée à Crofton (mathématicien irlandais du 19ème siècle).
Soient C une courbe paramétrée suffisamment régulière de longueur ℓ et H une droite du plan tirée uniformément au hasard, alors $\mathbb{E}[\#(C\cap H)] = \frac{2}{\pi}\ell$.
Plus généralement, on va montrer un résultat similaire dans $\mathbb{R}^n$ avec H un hyperplan affine uniforme. Pour cela, on va devoir définir une notion naturelle de mesure uniforme sur l'ensemble des hyperplans, c'est-à-dire invariante sous l'action d'un certain groupe de transformations.

2 Géométrie affine

On va maintenant décrire l'ensemble des hyperplans de $\mathbb{R}^n$ ainsi que l'action du groupe des isométries de $\mathbb{R}^n$ sur cet ensemble. Pour des raisons techniques, on va considérer des hyperplans orientés et des isométries directes. Dans la suite, $\mathbb{R}^n$ est supposé orienté par sa base canonique, muni de son produit scalaire euclidien $\langle\cdot\,,\cdot\rangle$ et de la norme associée $\|\cdot\|$. Le cas qui nous intéresse est $n\geqslant 2$.

2.1 Hyperplans affines

Définition 2.1 (hyperplan affine orienté)**.** Un *hyperplan affine* de $\mathbb{R}^n$ est un sous-ensemble de la forme $H = a + \overrightarrow{H}$, où $a \in \mathbb{R}^n$ et $\overrightarrow{H}$ est un hyperplan vectoriel, appelé la *direction* de H. On dit que H est *orienté* si $\overrightarrow{H}$ l'est.

Remarque. $\overrightarrow{H} = \{y - x \mid x, y \in H\}$ est uniquement défini par H, mais pas a.

Soit θ un vecteur unitaire normal à $\overrightarrow{H}$. Il définit une orientation ω_θ sur $\overrightarrow{H}$ par : $(e_2, \dots, e_n)$ est une base orthonormée directe (B.O.N.D.) de $\overrightarrow{H}$ si et seulement si $(\theta, e_2, \dots, e_n)$ est une B.O.N.D. de $\mathbb{R}^n$. Le vecteur $-\theta$ définit l'orientation opposée $\omega_{-\theta}$. Le choix d'une orientation de $\overrightarrow{H}$ est donc le choix de l'un des deux vecteurs de $\mathbb{S}^{n-1} \cap \overrightarrow{H}$.

Définition 2.2 (grassmannienne)**.** On note $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ l'ensemble, appelé *grassmannienne*, des hyperplans affines orientés de $\mathbb{R}^n$.

Soit $(H, \omega) \in \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$, où $H = a + \overrightarrow{H}$ et ω est l'orientation de $\overrightarrow{H}$. Il existe un unique $\theta \in \mathbb{S}^{n-1}$ tel que $\overrightarrow{H} = \theta^\perp$ et $\omega = \omega_\theta$. Ensuite, pour tout $x \in \mathbb{R}^n$ on a :

$$x \in H \iff x - a \in \overrightarrow{H} \iff \langle x - a\,, \theta \rangle = 0 \iff \langle x\,, \theta \rangle = \langle a\,, \theta \rangle.$$

En notant $\alpha = \langle a\,, \theta \rangle \in \mathbb{R}$, on a donc $H = \{x \in \mathbb{R}^n \mid \langle x\,, \theta \rangle = \alpha\}$.
Pour tout $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$, on note $H(\alpha, \theta) = \{x \in \mathbb{R}^n \mid \langle x\,, \theta \rangle = \alpha\} = \alpha\theta + \theta^\perp$. On vient de montrer que pour tout $(H, \omega) \in \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$, il existe un unique $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$ tel que $H = H(\alpha, \theta)$ et $\omega = \omega_\theta$. En d'autres termes, $(\alpha, \theta) \mapsto (H(\alpha, \theta), \omega_\theta)$ est une bijection de $\mathbb{R} \times \mathbb{S}^{n-1}$ vers $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$. Dans la suite on identifie $\mathbb{R} \times \mathbb{S}^{n-1} \simeq \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ via cette bijection. En particulier, cela munit $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ d'une topologie sympathique et naturelle.

Remarque. Plus généralement, on peut définir la grassmannienne (i.e. l'ensemble) des sous-espaces de codimension $k \in \{0, \dots, n\}$ de $\mathbb{R}^n$ (affines ou vectoriels, orientés ou non). Ces ensembles s'identifient naturellement à des quotients de $\mathbb{R}^k \times O_n(\mathbb{R})$.

2.2 Applications affines

On commence donc par s'intéresser aux applications affines dont les isométries sont un cas particulier.

Définition 2.3 (application affine)**.** Une application $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ est dite *affine* si elle préserve les barycentre, c'est-à-dire : $\forall x, y \in \mathbb{R}^n$, $\forall t \in \mathbb{R}$, $\varphi\big(tx + (1-t)y\big) = t\varphi(x) + (1-t)\varphi(y)$.

Exemples. Les translations $\tau_v : x \mapsto x + v$ pour $v \in \mathbb{R}^n$. Les applications linéaires $L \in M_n(\mathbb{R})$.

Lemme 2.4. *Soient φ et ψ des applications affines alors $\psi \circ \varphi$ est affine. Si de plus φ est bijective alors φ^{-1} est affine.*

Exercice. Prouver ce lemme.

En particulier, les bijections affines de $\mathbb{R}^n$ forment un groupe pour la composition, noté $\mathrm{Aff}(\mathbb{R}^n)$. Il contient comme sous-groupe $GL_n(\mathbb{R})$ et $\mathbb{R}^n$, identifié au sous-groupe des translations via $\tau : v \mapsto \tau_v$.

Lemme 2.5. *Soit φ une application affine, il existe un unique $(v, L) \in \mathbb{R}^n \times M_n(\mathbb{R})$ tel que $\varphi = \tau_v \circ L$. On appelle L la* partie linéaire *de φ, notée $\overrightarrow{\varphi}$.*

Exemples. Si $v \in \mathbb{R}^n$ alors $\overrightarrow{\tau_v} = \mathrm{Id}$. Si $L \in M_n(\mathbb{R})$ alors $\overrightarrow{L} = L$.

Démonstration. Par analyse-synthèse, si $\varphi = \tau_v \circ L$, alors $\varphi(0) = \tau_v(0) = v$ et $L = \tau_{-v} \circ \varphi$. Cela prouve l'unicité et donne les seuls candidats pour l'existence.
Soit φ affine, posons $v = \varphi(0)$ et $L = \tau_{-v} \circ \varphi$. Il suffit de vérifier qu'une application affine fixant 0, telle que L, est linéaire. Soient $x, y \in \mathbb{R}^n$ et $\lambda \in \mathbb{R}$,

$$\begin{aligned} L(x+\lambda y) &= L\left((1+\lambda)\frac{x+\lambda y}{1+\lambda} - \lambda 0\right) = (1+\lambda)L\left(\frac{x+\lambda y}{1+\lambda}\right) - \lambda L(0) \\ &= (1+\lambda)\left(\frac{1}{1+\lambda}L(x) + \frac{\lambda}{1+\lambda}L(y)\right) = L(x) + \lambda L(y). \end{aligned}$$ □

En particulier, une application affine φ est bijective si et seulement si sa partie linéaire $\vec{\varphi}$ l'est. On a donc montré que $(v, L) \mapsto \tau_v \circ L$ est bijective de $\mathbb{R}^n \times GL_n(\mathbb{R})$ vers $\mathrm{Aff}(\mathbb{R}^n)$. Attention ce n'est pas un isomorphisme pour la structure produit sur $\mathbb{R}^n \times GL_n(\mathbb{R})$. Cependant on a le résultat suivant.

Lemme 2.6. *Il existe une unique structure de groupe sur $\mathbb{R}^n \times GL_n(\mathbb{R})$ telle que $(v, L) \mapsto \tau_v \circ L$ soit un isomorphisme. Elle est décrite par : $(w, M) \cdot (v, L) = (w + Mv, ML)$.*

Exercice. Le vérifier. En déduire que $\varphi \mapsto \vec{\varphi}$ est un morphisme de groupe surjectif de $\mathrm{Aff}(\mathbb{R}^n)$ vers $GL_n(\mathbb{R})$ dont le noyau est le sous-groupe des translations.

L'ensemble $\mathbb{R}^n \times GL_n(\mathbb{R})$ muni de la structure de groupe donné par le lemme 2.6 est appelé *produit semi-direct* de $\mathbb{R}^n$ par $GL_n(\mathbb{R})$, noté $\mathbb{R}^n \rtimes GL_n(\mathbb{R})$. On a donc $\mathbb{R}^n \rtimes GL_n(\mathbb{R}) \simeq \mathrm{Aff}(\mathbb{R}^n)$.

2.3 Isométries

Définition 2.7 (isométrie)**.** Une isométrie de $\mathbb{R}^n$ est une application $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ qui préserve la distance : $\forall x, y \in \mathbb{R}^n$, $\|\varphi(y) - \varphi(x)\| = \|y - x\|$.

Exemples. Les translations τ_v avec $v \in \mathbb{R}^n$. Les isométries vectorielles $\Omega \in O_n(\mathbb{R})$.

Proposition 2.8. *Soit φ une isométrie de $\mathbb{R}^n$, alors φ est affine et $\vec{\varphi} \in O_n(\mathbb{R})$.*

En particulier, toute isométrie de $\mathbb{R}^n$ est bijective et les isométries forment un sous-groupe de $\mathrm{Aff}(\mathbb{R}^n)$. Sous l'isomorphisme $\mathbb{R}^n \rtimes GL_n(\mathbb{R}) \simeq \mathrm{Aff}(\mathbb{R}^n)$, ce sous-groupe est :

$$\{\varphi \in \mathrm{Aff}(\mathbb{R}^n) \mid \vec{\varphi} \in O_n(\mathbb{R})\} = \{\tau_v \circ \Omega \mid v \in \mathbb{R}^n, \Omega \in O_n(\mathbb{R})\} \simeq \mathbb{R}^n \rtimes O_n(\mathbb{R}).$$

Définition 2.9 (isométries directes)**.** On note $\mathrm{Isom}^+(\mathbb{R}^n)$ le sous-groupe de $\mathrm{Aff}(\mathbb{R}^n)$ formé des isométries directes :

$$\mathrm{Isom}^+(\mathbb{R}^n) = \{\varphi \in \mathrm{Aff}(\mathbb{R}^n) \mid \vec{\varphi} \in SO_n(\mathbb{R})\} = \{\tau_v \circ \Omega \mid v \in \mathbb{R}^n, \Omega \in SO_n(\mathbb{R})\} \simeq \mathbb{R}^n \rtimes SO_n(\mathbb{R}).$$

Démonstration de la proposition 2.8. Soit φ une isométrie. Si on suppose φ affine alors $\varphi = \tau_{\varphi(0)} \circ \vec{\varphi}$ et $\vec{\varphi} = \tau_{-\varphi(0)} \circ \varphi$ est linéaire et préserve $\|\cdot\|$. Il s'agit donc de montrer que φ est affine.
Étape 1 : φ préserve l'alignement. Soient x, y et $z \in \mathbb{R}^n$ alignés dans cet ordre. On a :

$$\|z - x\| = \|\varphi(z) - \varphi(x)\| \leqslant \|\varphi(z) - \varphi(y)\| + \|\varphi(y) - \varphi(x)\| = \|z - y\| + \|y - z\| = \|z - x\|,$$

en utilisant la condition d'alignement. Donc $\|\varphi(z) - \varphi(x)\| = \|\varphi(z) - \varphi(y)\| + \|\varphi(y) - \varphi(x)\|$. Comme $\|\cdot\|$ est la norme euclidienne, cela signifie que $\varphi(x), \varphi(y)$ et $\varphi(z)$ sont alignés dans cet ordre. Formellement cela se ramène au cas d'égalité dans l'inégalité de Cauchy-Schwarz.
Étape 2 : φ préserve les barycentres. Soient $x, y \in \mathbb{R}^n$ et $t \in \mathbb{R}$, on note $g = tx + (1-t)y$. On peut supposer que $x \neq y$. Supposons aussi que $t \leqslant 0$, les cas $t \in [0, 1]$ et $t \geqslant 1$ étant similaires.
Alors x, y et g sont alignés dans cet ordre, donc $\varphi(x), \varphi(y)$ et $\varphi(g)$ sont alignés dans cet ordre. Il existe donc $s \leqslant 0$ tel que $\varphi(g) = s\varphi(x) + (1-s)\varphi(y)$. Il s'agit de montrer que $s = t$.
On a $g - y = t(x - y)$. Comme $t \leqslant 0$, on a $t = -|t| = -\frac{\|g-y\|}{\|x-y\|}$. De même, $s = -\frac{\|\varphi(g)-\varphi(y)\|}{\|\varphi(x)-\varphi(y)\|}$. Comme φ est isométrique, on en déduit que $s = t$. Donc φ préserve les barycentres, i.e. est affine. □

2.4 Actions des isométries sur la grassmannienne

Soit $H = a+\vec{H}$ un hyperplan affine et $\varphi = \tau_v \circ L \in \mathrm{Aff}(\mathbb{R}^n)$. Alors $\varphi(H) = v+L(a+\vec{H}) = v+La+L\vec{H}$. Donc $\varphi(H)$ est un hyperplan affine de direction $\vec{\varphi}(\vec{H})$. De plus, on définit une orientation sur $\vec{\varphi}(\vec{H})$ en demandant que l'image $(\vec{\varphi}e_2, \dots, \vec{\varphi}e_n)$ d'une base directe $(e_2, \dots, e_n)$ de $\vec{H}$ soit directe.
Donc φ induit une application de $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ dans lui-même, encore notée φ. On se convaincra que cela définit un morphisme de groupe $\mathrm{Aff}(\mathbb{R}^n) \to \mathrm{Bij}(\mathcal{G}\mathrm{r}^+(\mathbb{R}^n))$, i.e. une action $\mathrm{Aff}(\mathbb{R}^n) \curvearrowright \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$.

Exercice. Se convaincre.

On veut maintenant décrire l'action induite $\mathbb{R}^n \rtimes SO_n(\mathbb{R}) \simeq \mathrm{Isom}^+(\mathbb{R}^n) \curvearrowright \mathcal{G}\mathrm{r}^+(\mathbb{R}^n) \simeq \mathbb{R} \times \mathbb{S}^{n-1}$. Soit $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$ correspondant à $(H(\alpha,\theta), \omega_\theta) \in \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$. Soient $(v, \Omega) \in \mathbb{R}^n \rtimes SO_n(\mathbb{R})$ et $\varphi = \tau_v \circ \Omega$:

$$\varphi(H(\alpha,\theta)) = v + \Omega\Big(\alpha\theta + \theta^\perp\Big) = v + \alpha\Omega\theta + \Omega(\theta^\perp).$$

On a $\Omega(\theta^\perp) = (\Omega\theta)^\perp$ car Ω préserve l'orthogonalité. Par ailleurs, comme $\|\Omega\theta\| = \|\theta\| = 1$, on peut écrire $v = \langle v\,, \Omega\theta\rangle\Omega\theta + v^\perp$, où $v^\perp \in (\Omega\theta)^\perp$. Donc

$$\varphi(H(\alpha,\theta)) = (\alpha + \langle v\,, \Omega\theta\rangle)\Omega\theta + (\Omega\theta)^\perp = H\big(\alpha + \langle v\,, \Omega\theta\rangle, \Omega\theta\big).$$

Soit $(e_2, \dots, e_n)$ une B.O.N.D. de $\theta^\perp$ pour ω_θ. Alors $(\theta, e_2, \dots, e_n)$ est une B.O.N.D. de $\mathbb{R}^n$, et donc $(\Omega\theta, \Omega e_2, \dots, \Omega e_n)$ aussi. Donc $(\Omega e_2, \dots, \Omega e_n)$ est une B.O.N.D. de $(\Omega\theta)^\perp$ pour $\omega_{\Omega\theta}$. Cela prouve que l'orientation sur $(\Omega\theta)^\perp$ image de ω_θ par φ est $\omega_{\Omega\theta}$.
Ainsi, $\varphi(H(\alpha,\theta),\omega_\theta) = \big(H\big(\alpha + \langle v\,, \Omega\theta\rangle, \Omega\theta\big), \omega_{\Omega\theta}\big)$, qui correspond à $(\alpha + \langle v\,, \Omega\theta\rangle, \Omega\theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$. L'action $\mathbb{R}^n \rtimes SO_n(\mathbb{R}) \curvearrowright \mathbb{R} \times \mathbb{S}^{n-1}$ est donc décrite par :

$$\forall (v,\Omega) \in \mathbb{R}^n \rtimes SO_n(\mathbb{R}), \forall (\alpha,\theta) \in \mathbb{R} \times \mathbb{S}^{n-1}, \qquad (v,\Omega)\cdot(\alpha,\theta) = (\alpha + \langle v\,, \Omega\theta\rangle, \Omega\theta). \tag{1}$$

3 Mesures invariantes

Notre prochain objectif est de définir une mesure sur $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ qui soit invariante par isométries.

3.1 Rappels de théorie de la mesure

Définition 3.1 (mesure image)**.** Soient $\varphi : E \to F$ mesurable entre espaces mesurés et μ une mesure sur E. La *mesure image* $\varphi_*\mu$ de μ par φ est la mesure sur F définie par : $\varphi_*\mu(A) = \mu\big(\varphi^{-1}(A)\big)$ pour tout $A \subset F$ mesurable.

C'est l'unique mesure telle que $f \in L^1(F, \varphi_*\mu) \iff f \circ \varphi \in L^1(E,\mu)$ et, pour tout $f \in L^1(F,\varphi_*\mu)$, $\int_F f \,\mathrm{d}\varphi_*\mu = \int_E (f\circ\varphi)\,\mathrm{d}\mu$.
Exercice. Vérifier que c'est le cas.

Définition 3.2 (mesure invariante)**.** Une mesure μ est dite *invariante* par $\varphi : E \to E$ si $\varphi_*\mu = \mu$. Soit G ensemble de fonctions mesurables, μ est dite *G-invariante* si elle est invariante par tout $\varphi \in G$.

Exemple. La mesure de Lebesgue est invariante par les isométries de $\mathbb{R}^n$.

Dans la suite, les mesures sur des espaces topologiques seront toujours supposées être boréliennes.

Théorème 3.3. *La mesure de Lebesgue sur $\mathbb{R}^n$ est l'unique mesure finie sur les compacts et invariante par translation, à constante multiplicative près.*

Exercice. Prouver ce théorème. On pourra commencer par montrer que si μ est invariante par translation alors il existe $a \geqslant 0$ telle que pour tout cube C de côté 2^k ($k \in \mathbb{Z}$) on a $\mu(C) = a\,\mathrm{Leb}(C)$.

3.2 Gaussiennes et loi uniforme sur la sphère

On travaille toujours dans $\mathbb{R}^n$ muni de son produit scalaire euclidien $\langle \cdot\,, \cdot \rangle$ et de la norme $\|\cdot\|$ associée. On note $\mathcal{S}_{\mathrm{n}}^+(\mathbb{R})$ l'ensemble des matrices symétriques définies positives de taille n.

Définition 3.4 (gaussienne centrée)**.** Soit $\Lambda \in \mathcal{S}_{\mathrm{n}}^+(\mathbb{R})$, la loi *gaussienne centrée* de variance Λ est la mesure de probabilité $\mathcal{N}(0,\Lambda)$ sur $\mathbb{R}^n$ admettant la densité $x \mapsto \frac{1}{\sqrt{(2\pi)^n \det(\Lambda)}} \exp\bigl(-\frac{1}{2}\langle \Lambda^{-1}x\,, x\rangle\bigr)$ par rapport à la mesure de Lebesgue. La loi $\mathcal{N}(0,\mathrm{Id})$ est appelée *gaussienne standard*.

Lemme 3.5. *Soient $X \sim \mathcal{N}(0,\Lambda)$ et $L \in GL_n(\mathbb{R})$ alors on a $LX \sim \mathcal{N}\bigl(0, L\Lambda\,{}^tL\bigr)$, c'est-à-dire $L_*\mathcal{N}(0,\Lambda) = \mathcal{N}\bigl(0, L\Lambda\,{}^tL\bigr)$. En particulier, $\mathcal{N}(0,\mathrm{Id})$ est $O_n(\mathbb{R})$-invariante.*

Exercice. Prouver ce lemme.
Si $X \sim \mathcal{N}(0,\mathrm{Id})$, alors $\theta = \frac{X}{\|X\|}$ est une variable aléatoire dans $\mathbb{S}^{n-1}$ définie presque surement.

Définition 3.6 (mesure uniforme sur $\mathbb{S}^{n-1}$)**.** On appelle *mesure uniforme* sur $\mathbb{S}^{n-1}$ la loi $\mathrm{d}\theta$ de θ. Si $p : \mathbb{R}^n \setminus \{0\} \to \mathbb{S}^{n-1}$ est la projection radiale, $d\theta = p_*\mathcal{N}(0,\mathrm{Id})$.

Lemme 3.7. $\mathrm{d}\theta$ *est $O_n(\mathbb{R})$-invariante sur $\mathbb{S}^{n-1}$.*

Démonstration. Soit $\Omega \in O_n(\mathbb{R})$, pour tout $x \neq 0$, on a $\Omega(p(x)) = \Omega\frac{x}{\|x\|} = \frac{\Omega x}{\|x\|} = \frac{\Omega x}{\|\Omega x\|} = p(\Omega(x))$. Donc $p \circ \Omega = \Omega \circ p$. On en déduit que :

$$\Omega_*\,\mathrm{d}\theta = \Omega_* p_* \mathcal{N}(0,\mathrm{Id}) = (\Omega\circ p)_*\mathcal{N}(0,\mathrm{Id}) = p_*\Omega_*\mathcal{N}(0,\mathrm{Id}) = p_*\mathcal{N}(0,\mathrm{Id}) = \mathrm{d}\theta. \qquad \square$$

Théorème 3.8. *Si $n \geqslant 2$, alors $\mathrm{d}\theta$ est l'unique mesure de probabilité $SO_n(\mathbb{R})$-invariante sur $\mathbb{S}^{n-1}$.*

On admet ce résultat. C'est un cas particulier d'un résultat très général évoqué à la section 3.4.

Exercice.
1. Montrer qu'une mesure de probabilité $SO_n(\mathbb{R})$-invariante sur $\mathbb{S}^{n-1}$ est sans atome.
2. Si $\mu = \rho\,\mathrm{d}\theta$ est $SO_n(\mathbb{R})$-invariante et ρ est continue, montrer que ρ est constante.

3.3 Mesure uniforme sur la grassmannienne

Définition 3.9 (mesure uniforme)**.** On appelle *mesure uniforme* sur $\mathcal{G}\mathrm{r}^+(\mathbb{R}^{\mathrm{n}}) \simeq \mathbb{R}\times\mathbb{S}^{n-1}$ la mesure $\mathrm{d}\mu = \mathrm{d}\alpha \otimes \mathrm{d}\theta$, où $\mathrm{d}\alpha$ est la mesure de Lebesgue sur $\mathbb{R}$ et $\mathrm{d}\theta$ est la mesure uniforme sur $\mathbb{S}^{n-1}$.

Lemme 3.10. *La mesure $\mathrm{d}\mu$ est $\mathrm{Isom}^+(\mathbb{R}^{\mathrm{n}})$-invariante.*

Démonstration. Soient $(v,\Omega) \in \mathbb{R}^n \rtimes SO_n(\mathbb{R})$ et $\varphi = \tau_v \circ \Omega \in \mathrm{Isom}^+(\mathbb{R}^{\mathrm{n}})$. On rappelle que l'action de (v,Ω) sur $\mathcal{G}\mathrm{r}^+(\mathbb{R}^{\mathrm{n}})$ est décrite par l'équation (1). Pour toute fonction mesurable positive f sur $\mathbb{R}\times\mathbb{S}^{n-1} \simeq \mathcal{G}\mathrm{r}^+(\mathbb{R}^{\mathrm{n}})$ on calcule :

$$\begin{aligned}
\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^{\mathrm{n}})} f\circ\varphi\,\mathrm{d}\mu &= \int_{\mathbb{R}\times\mathbb{S}^{n-1}} f\bigl(\varphi\cdot(\alpha,\theta)\bigr)\,\mathrm{d}\alpha\,\mathrm{d}\theta \qquad = \int_{\mathbb{S}^{n-1}}\left(\int_{\mathbb{R}} f(\alpha+\langle v\,,\Omega\theta\rangle,\Omega\theta)\,\mathrm{d}\alpha\right)\mathrm{d}\theta \\
&= \int_{\mathbb{S}^{n-1}}\left(\int_{\mathbb{R}} f(\alpha,\Omega\theta)\,\mathrm{d}\alpha\right)\mathrm{d}\theta \qquad \text{(invariance par translation de } \mathrm{d}\alpha) \\
&= \int_{\mathbb{R}}\left(\int_{\mathbb{S}^{n-1}} f(\alpha,\Omega\theta)\,\mathrm{d}\theta\right)\mathrm{d}\alpha \\
&= \int_{\mathbb{R}}\left(\int_{\mathbb{S}^{n-1}} f(\alpha,\theta)\,\mathrm{d}\theta\right)\mathrm{d}\alpha \qquad \text{(invariance par rotation de } \mathrm{d}\theta) \\
&= \int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^{\mathrm{n}})} f\,\mathrm{d}\mu.
\end{aligned}$$

Si f est l'indicatrice du borélien A, on obtient bien $\varphi_*\mu(A) = \mu(\varphi^{-1}(A)) = \mu(A)$. Donc $\varphi_*\mu = \mu$. $\square$

Théorème 3.11 (admis)**.** *La mesure* $\mathrm{d}\mu$ *est l'unique mesure sur* $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ *finie sur les compacts et* $\mathrm{Isom}^+(\mathbb{R}^n)$*-invariante, à constante multiplicative près.*

3.4 Mesures de Haar

L'unicité de la mesure de Lebesgue sur $\mathbb{R}^n$ et des mesures uniformes sur $\mathbb{S}^{n-1}$ et $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ sont des cas particuliers d'un résultat général qu'on présente pour la culture dans cette section.

Définition 3.12 (action de groupe continue)**.** Une action $G \curvearrowright X$ est dite *continue* si :
- G et X sont des espaces topologiques localement compacts ;
- les opérations du groupe $(g,h) \mapsto gh$ et $g \mapsto g^{-1}$ sont continues ;
- l'application $(g,x) \mapsto g \cdot x$ est continue de $G \times X$ dans X.

Exemples.
- L'action $\mathbb{R}^n \curvearrowright \mathbb{R}^n$ par translation.
- L'action naturelle de $\mathrm{Aff}(\mathbb{R}^n)$ et ses sous-groupes sur $\mathbb{R}^n$.
- L'action $SO_n(\mathbb{R}) \curvearrowright \mathbb{S}^{n-1}$ par rotation.
- Notre action préférée $\mathrm{Isom}^+(\mathbb{R}^n) \curvearrowright \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$ décrite à la section 2.4.

Définition 3.13 (mesure de Haar)**.** Une *mesure de Haar* pour une action $G \curvearrowright X$ continue et transitive est une mesure borélienne non nulle sur X qui est G-invariante et finie sur les compacts.

On connait une condition nécessaire et suffisante, appelé *critère de Weil*, pour que $G \curvearrowright X$ admette une mesure de Haar. Son énoncé précis sort du cadre de ce cours. Il est satisfait dans les cas suivants :

1. Il existe $x \in X$ dont le stabilisateur est compact (en particulier si G est compact).
2. $G \curvearrowright G$ est l'action par translation à gauche ou à droite.

De plus, si $G \curvearrowright X$ admet une mesure de Haar elle est unique à une constante multiplicative près.

Remarque.
- Le point 1, pour l'action $O_n(\mathbb{R}) \curvearrowright \mathbb{S}^{n-1}$ remontre l'existence de $\mathrm{d}\theta$.
- Le point 2 remontre l'existence de la mesure de Lebesgue, un indice que ce résultat est dur.
- Comme l'action est transitive, les stabilisateurs sont tous conjugués, donc homéomorphes. Dans le point 1, il est donc équivalent de demander que le stabilisateur de tout point soit compact.
- Ce résultat est satisfaisant théoriquement mais il ne dit pas comment construire la mesure invariante, ce qui est gênant pour la manipuler. Dans les cas concrets on construit souvent une mesure invariante à la main, comme dans les sections précédentes.

4 Formule de Crofton euclidienne

Dans cette section on prouve la formule de Crofton dans $\mathbb{R}^n$.

Théorème 4.1 (Formule de Crofton)**.** *Soit* $I \subset \mathbb{R}$ *un intervalle. Soit* $\gamma : I \to \mathbb{R}^n$ *une courbe paramétrée de classe* $\mathcal{C}^1$ *et régulière, i.e.* $\forall t \in I,\ \gamma'(t) \neq 0$*. Notons* $\ell = \int_I \|\gamma'(t)\|\,\mathrm{d}t \in [0,+\infty]$ *la longueur de* $\gamma(I)$*. On a :*

$$\int_{(H,\omega)\in\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)} \#(\gamma(I)\cap H)\,\mathrm{d}\mu(H,\omega) = C_n\ell, \qquad \text{où} \quad C_n = \frac{\Gamma\left(\frac{n}{2}\right)}{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{n+1}{2}\right)}.$$

Remarque.
- Attention ce n'est pas une espérance car μ est de masse infinie. Si $\gamma(I) \subset B(0,M)$ pour un certain $M > 0$ (par exemple si ℓ est finie), alors on peut se restreindre à intégrer sur $\{(H,\omega) \in \mathcal{G}\mathrm{r}^+(\mathbb{R}^n) \mid H \cap B(0,M) \neq \emptyset\} \simeq [-M,M] \times \mathbb{S}^{n-1}$, qui est de mesure finie. Quitte à normaliser on a alors bien une mesure de probabilité.
- Chaque hyperplan est compté exactement deux fois, une fois avec chaque orientation.
- $\#(\gamma(I)\cap H)$ est un abus de notation pour $\#\gamma^{-1}(H)$, ce qui est différent si la courbe n'est pas simple : un point double sera compté deux fois. Ce ne sera pas un problème dans la suite.

4.1 Cas d'un segment

On commence par prouver le théorème lorsque $\gamma(I)$ est un segment. Par invariance sous $\mathrm{Isom}^+(\mathbb{R}^n)$, on peut se ramener à $\gamma : t \mapsto te_1$ de $[-\frac{\ell}{2}, \frac{\ell}{2}]$ dans $\mathbb{R}^n$, où e_1 est le premier vecteur de base de $\mathbb{R}^n$.
Soient $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$, la projection orthogonale de $\gamma(I) = \big[-\frac{\ell}{2}, \frac{\ell}{2}\big]e_1$ sur la droite $\mathbb{R}\theta$ est le segment $\big[-\frac{\ell}{2}|\langle e_1\,,\theta\rangle|, \frac{\ell}{2}|\langle e_1\,,\theta\rangle|\big]\theta$.
L'hyperplan $H(\alpha,\theta) = \alpha\theta + \theta^\perp$ intersecte $\gamma(I)$ si et seulement si $\alpha \in \big[-\frac{\ell}{2}|\langle e_1\,,\theta\rangle|, \frac{\ell}{2}|\langle e_1\,,\theta\rangle|\big]$. Comme dans le cas des aiguilles de Buffon on a donc :

$$\#(\gamma(I) \cap H(\alpha,\theta)) = \begin{cases} 0 & \text{si } |\alpha| > \frac{\ell}{2}|\langle e_1\,,\theta\rangle|, \\ 1 & \text{si } |\alpha| \leqslant \frac{\ell}{2}|\langle e_1\,,\theta\rangle|, \text{ et } \langle e_1\,,\theta\rangle \neq 0, \\ +\infty & \text{si } \alpha = 0 = \langle e_1\,,\theta\rangle. \end{cases}$$

Comme $\mu\big(\{0\} \times (\{0\} \times \mathbb{S}^{n-2})\big) = 0$, on a :

$$\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)} \#(\gamma(I)\cap H)\,\mathrm{d}\mu = \mu\big(\{(H,\omega) \mid \gamma(I)\cap H \neq \emptyset\}\big) = \int_{\mathbb{S}^{n-1}} \int_{-\frac{\ell}{2}|\langle e_1\,,\theta\rangle|}^{\frac{\ell}{2}|\langle e_1\,,\theta\rangle|} \mathrm{d}\alpha\,\mathrm{d}\theta = \ell \int_{\mathbb{S}^{n-1}} |\langle \theta\,, e_1\rangle|\,\mathrm{d}\theta.$$

Le résultat en prouvé en posant $C_n = \int_{\mathbb{S}^{n-1}} |\langle \theta\,, e_1\rangle|\,\mathrm{d}\theta$. Il reste à calculer cette constante. Notons $\mathrm{d}\sigma_{k-1}$ la mesure de volume sur $\mathbb{S}^{k-1} \subset \mathbb{R}^k$. En passant en coordonnées sphériques, on a :

$$\begin{aligned} C_n &= \int_{\mathbb{S}^{n-1}} |\langle \theta\,, e_1\rangle|\,\mathrm{d}\theta = \frac{1}{\mathrm{Vol}(\mathbb{S}^{n-1})} \int_{\mathbb{S}^{n-1}} |\langle \eta\,, e_1\rangle|\,\mathrm{d}\sigma_{k-1}(\eta) \\ &= \frac{1}{\mathrm{Vol}(\mathbb{S}^{n-1})} \int_{\beta=0}^{\pi} \int_{\{0\}\times\mathbb{S}^{n-2}} |\cos(\beta)||\sin(\beta)|^{n-2}\,\mathrm{d}\sigma_{k-2}(\eta)\,\mathrm{d}\beta \\ &= 2\frac{\mathrm{Vol}(\mathbb{S}^{n-2})}{\mathrm{Vol}(\mathbb{S}^{n-1})} \int_0^{\frac{\pi}{2}} \cos(\beta)\sin(\beta)^{n-2}\,\mathrm{d}\beta = \frac{2}{n-1}\frac{\mathrm{Vol}(\mathbb{S}^{n-2})}{\mathrm{Vol}(\mathbb{S}^{n-1})}. \end{aligned}$$

On conclut en utilisant $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ et la formule suivante pour le volume $(n-1)$-dimensionnel de la sphère $\mathbb{S}^{n-1}$: $\mathrm{Vol}(\mathbb{S}^{n-1}) = \frac{2\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}$.

4.2 Cas où l'intervalle I est compact

C'est l'étape difficile. Si I est compact alors $\ell < +\infty$, et on peut supposer que $I = [0, \ell]$ et que γ est un paramétrage par longueur d'arc : $\forall t \in I, \|\gamma'(t)\| = 1$.
On procède en approchant $\gamma(I)$ par des lignes brisées. Soient $k \in \mathbb{N}$ et $i \in \{1, \ldots, 2^k\}$, on note $S_{k,i} = \big[\gamma\big(\frac{i-1}{2^k}\ell\big), \gamma\big(\frac{i}{2^k}\ell\big)\big]$ et $C_k = \bigcup_{1\leqslant i\leqslant 2^k} S_{k,i}$, la ligne brisée qui interpole $\gamma(I)$ aux points de paramètres $\big(\frac{i\ell}{2^k}\big)_{0\leqslant i\leqslant 2^k}$. On note $\ell_{k,i}$ la longueur de $S_{k,i}$ et $\ell_k = \sum_{i=1}^{2^k} \ell_{k,i}$ celle de C_k.
On va déduire le résultat des trois lemmes suivants.

Lemme 4.2. *On a* $\ell_k \xrightarrow[k\to+\infty]{} \ell$.

Lemme 4.3. *Soit H un hyperplan affine de $\mathbb{R}^n$ tel que :*

1. *H ne contient aucun des noeuds $\gamma\big(\frac{i\ell}{2^k}\big)$, où $k \in \mathbb{N}$ et $0 \leqslant i \leqslant 2^k$;*
2. *H n'est pas tangent à $\gamma(I)$: $\forall t \in I$, si $\gamma(t) \in H$ alors $\gamma'(t) \notin \overrightarrow{H}$.*

Alors $(\#(C_k \cap H))_{k\geqslant 0}$ est une suite croissante qui converge vers $\#(\gamma(I) \cap H) < +\infty$.

Lemme 4.4. *Pour presque tout $(H,\omega) \in \mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$, les conditions 1 et 2 du lemme 4.3 sont satisfaites.*

Si on suppose ces lemmes établis, le lemme de croissance monotone assure que :

$$\begin{aligned}\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^\mathrm{n})} \#(\gamma(I)\cap H)\,\mathrm{d}\mu &= \int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^\mathrm{n})} \lim_{k\to+\infty} \#(C_k\cap H)\,\mathrm{d}\mu = \lim_{k\to+\infty}\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^\mathrm{n})} \#(C_k\cap H)\,\mathrm{d}\mu \\ &= \lim_{k\to+\infty}\sum_{i=1}^{2^k}\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^\mathrm{n})} \#(S_{k,i}\cap H)\,\mathrm{d}\mu = \lim_{k\to+\infty}\sum_{i=1}^{2^k} C_n\ell_{k,i} = \lim_{k\to+\infty} C_n\ell_k \\ &= C_n\ell.\end{aligned}$$

Il faut maintenant prouver les lemmes.

Démonstration du lemme 4.2. Comme γ' est continue sur $[0,\ell]$, elle y est uniformément continue. Soit $\varepsilon>0$ et soit $\eta>0$ tel que $|t-s|\leqslant\eta$ implique $\|\gamma'(t)-\gamma'(s)\|\leqslant\varepsilon$.
Pour tout $k\geqslant 0$ assez grand pour que $\frac{\ell}{2^k}\leqslant\eta$ et tout $i\in\{1,\dots,2^k\}$,

$$\begin{aligned}\left\|\gamma\left(\frac{i}{2^k}\ell\right)-\gamma\left(\frac{i-1}{2^k}\ell\right)-\frac{\ell}{2^k}\gamma'\left(\frac{i}{2^k}\ell\right)\right\| &= \left\|\int_{\frac{i-1}{2^k}\ell}^{\frac{i}{2^k}\ell}\gamma'(t)-\gamma'\left(\frac{i}{2^k}\ell\right)\mathrm{d}t\right\| \\ &\leqslant \int_{\frac{i-1}{2^k}\ell}^{\frac{i}{2^k}\ell}\left\|\gamma'(t)-\gamma'\left(\frac{i}{2^k}\ell\right)\right\|\mathrm{d}t\leqslant\frac{\ell}{2^k}\varepsilon.\end{aligned}$$

Donc

$$\begin{aligned}\left|l_{k,i}-\frac{\ell}{2^k}\right| &= \left|\|\gamma\left(\frac{i}{2^k}\ell\right)-\gamma\left(\frac{i-1}{2^k}\ell\right)\|-\frac{\ell}{2^k}\|\gamma'\left(\frac{i}{2^k}\ell\right)\|\right| \leqslant \left\|\gamma\left(\frac{i}{2^k}\ell\right)-\gamma\left(\frac{i-1}{2^k}\ell\right)-\frac{\ell}{2^k}\gamma'\left(\frac{i}{2^k}\ell\right)\right\| \\ &\leqslant \frac{\ell}{2^k}\varepsilon\end{aligned}$$

et donc

$$|\ell_k-l| = \left|\sum_{i=1}^{2^k}\left(l_{k,i}-\frac{\ell}{2^k}\right)\right| \leqslant \sum_{i=1}^{2^k}\left|l_{k,i}-\frac{\ell}{2^k}\right| \leqslant \ell\varepsilon. \qquad \square$$

Démonstration du lemme 4.3. Soit $k\geqslant 0$ et $1\leqslant i\leqslant 2^k$. Par l'hypothèse 1, les extrémités de $S_{k,i}$ ne sont pas dans H. Donc $\#(S_{k,i}\cap H)\in\{0,1\}$.
Croissance. Si les extrémités de $S_{k,i}$ sont dans la même composante connexe de $\mathbb{R}^n\setminus H$, alors $\#(S_{k,i}\cap H)=0$ par convexité. Donc $\#(S_{k,i}\cap H)\leqslant\#(S_{k+1,2i-1}\cap H)+\#(S_{k+1,2i}\cap H)$.
Par contraposée, si $\#(S_{k,i}\cap H)=1$, alors $\gamma\left(\frac{i-1}{2^k}\ell\right)$ et $\gamma\left(\frac{i}{2^k}\ell\right)$ ne sont pas dans la même composante de $\mathbb{R}^n\setminus H$. Par théorème des valeurs intermédiaires, tout chemin continu reliant ces points intersecte H, en particulier $S_{k+1,2i-1}\cup S_{k+1,2i}$. Donc $\#(S_{k+1,2i-1}\cap H)+\#(S_{k+1,2i}\cap H)\geqslant 1=\#(S_{k,i}\cap H)$.
Finalement on obtient :

$$\#(C_k\cap H)=\sum_{i=1}^{2^k}\#(S_{k,i}\cap H)\leqslant\sum_{i=1}^{2^k}\#(S_{k+1,2i-1}\cap H)+\#(S_{k+1,2i}\cap H)=\#(C_{k+1}\cap H).$$

Donc la suite $(\#(C_k\cap H))_{k\geqslant 1}$ est croissante.
Finitude. On fait une preuve par l'absurde. Si $\gamma^{-1}(H)\subset[0,\ell]$ est infini, il admet un point d'accumulation par compacité. Il existe donc $t\in[0,\ell]$ et une suite $(t_j)_{j\geqslant 0}$ de points de $\gamma^{-1}(H)\setminus\{t\}$ tels que $t_j\xrightarrow[j\to+\infty]{} t$. Comme H est fermé, $\gamma(t)\in H$. Par ailleurs $\frac{\gamma(t)-\gamma(t_j)}{t-t_j}\in\vec{H}$ pour tout j. En passant à la limite, $\gamma'(t)\in\vec{H}$, ce qui contredit l'hypothèse 2. Donc $\gamma^{-1}(H)$ est fini.

Stationnarité. On note $0 < t_1 < \cdots < t_m < \ell$ les éléments de $\gamma^{-1}(H)$. Pour tout j, $\gamma(t_j) \in H$. Donc, par l'hypothèse 2, $\gamma'(t_j) \notin \overrightarrow{H}$ i.e. la courbe traverse H. Pour tout $k \geqslant 0$ assez grand, chaque intervalle $\left[\frac{i-1}{2^k}\ell, \frac{i}{2^k}\ell\right]$ contient au plus l'un des t_j. De plus, $\#(S_{k,i} \cap H) = 1$ si et seulement si c'est le cas. Donc, pour tout k assez grand,

$$\#(C_k \cap H) = \sum_{i=1}^{2^k} \#(S_{k,i} \cap H) = m = \#(\gamma(I) \cap H). \qquad \square$$

La preuve du lemme 4.4 utilise le lemme suivant, qui est un cas très particulier du théorème de Sard.

Lemme 4.5. *Soit $f : [0, \ell] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^1$, alors* $\mathrm{Leb}(\{f(t) \mid f'(t) = 0\}) = 0$.

Démonstration. Soit $\varepsilon > 0$, alors $\{t \in [0, \ell] \mid |f'(t)| < \varepsilon\} = (f')^{-1}(]-\varepsilon, \varepsilon[)$ est ouvert. Il s'écrit donc comme l'union disjointe $\bigsqcup_{i\in I} U_i$ de ses composantes connexes, qui sont des intervalles ouverts.
Soient $x, y \in U_i$, par le théorème des accroissements finis, $|f(y) - f(x)| \leqslant \varepsilon|y - x|$. Donc l'intervalle $f(U_i)$ est de longueur $\mathrm{Leb}(f(U_i)) \leqslant \varepsilon \,\mathrm{Leb}(U_i)$. Ensuite,

$$\big\{f(t) \mid f'(t) = 0\big\} \subset \big\{f(t) \mid |f'(t)| < \varepsilon\big\} = f\left(\bigsqcup_{i\in I} U_i\right) = \bigcup_{i\in I} f(U_i).$$

Donc $\mathrm{Leb}(\{f(t) \mid f'(t) = 0\}) \leqslant \sum_{i\in I} \mathrm{Leb}(f(U_i)) \leqslant \varepsilon \sum_{i\in I} \mathrm{Leb}(U_i) \leqslant \varepsilon\ell$, pour tout $\varepsilon > 0$. $\square$

Démonstration du lemme 4.4. Il suffit de montrer que chacune des conditions 1 et 2 est satisfaite μ-presque partout sur $\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)$.
Condition 1. Soit $k \geqslant 0$ et $0 \leqslant i \leqslant 2^k$, pour tout $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$ on a :

$$\gamma\left(\frac{i\ell}{2^k}\right) \in H(\alpha, \theta) = \alpha\theta + \theta^\perp \iff \left\langle \gamma\left(\frac{i\ell}{2^k}\right), \theta \right\rangle = \alpha.$$

Donc $\mu\big(\big\{(\alpha, \theta) \;\big|\; \gamma\big(\frac{i\ell}{2^k}\big) \in H(\alpha, \theta)\big\}\big) = \int_{\mathbb{S}^{n-1}} \mathrm{Leb}\big(\big\{\big\langle \gamma\big(\frac{i\ell}{2^k}\big), \theta\big\rangle\big\}\big)\,\mathrm{d}\theta = 0$. Comme on considère un nombre dénombrable de couples (k, i),

$$\mu\left(\left\{(\alpha, \theta) \;\middle|\; \exists (k, i), \gamma\left(\frac{i\ell}{2^k}\right) \in H(\alpha, \theta)\right\}\right) = 0.$$

Condition 2. Pour $\theta \in \mathbb{S}^{n-1}$, on note $f_\theta : t \mapsto \langle \gamma(t), \theta\rangle$ de I dans $\mathbb{R}$. Cette fonction est $\mathcal{C}^1$ et $f'_\theta : t \mapsto \langle \gamma'(t), \theta\rangle$. Soient $(\alpha, \theta) \in \mathbb{R} \times \mathbb{S}^{n-1}$ et $t \in I$, on a :

$$H \text{ est tangent à } \gamma(I) \text{ en } \gamma(t) \iff \begin{cases} \gamma(t) \in H(\alpha, \theta), \\ \gamma'(t) \in \overrightarrow{H(\alpha, \theta)}, \end{cases} \iff \begin{cases} \langle \gamma(t), \theta\rangle = \alpha, \\ \langle \gamma'(t), \theta\rangle = 0, \end{cases} \iff \begin{cases} f_\theta(t), = \alpha \\ f'_\theta(t) = 0. \end{cases}$$

Donc, par le lemme 4.5,

$$\begin{aligned} \mu\big(\{(\alpha, \theta) \;\big|\; H(\alpha, \theta) \text{ tangent à } \gamma(I)\}\big) &= \mu\big(\big\{(\alpha, \theta) \;\big|\; \exists t \in I \text{ tel que } \alpha = f_\theta(t) \text{ et } f'_\theta(t) = 0\big\}\big) \\ &= \mu\left(\left\{(\alpha, \theta) \;\middle|\; \alpha \in \big\{f_\theta(t) \;\big|\; f'_\theta(t) = 0\big\}\right\}\right) \\ &= \int_{\mathbb{S}^{n-1}} \mathrm{Leb}\big(\big\{f_\theta(t) \;\big|\; f'_\theta(t) = 0\big\}\big)\,\mathrm{d}\theta = 0. \end{aligned} \qquad \square$$

4.3 Cas général

Si on ne suppose pas que I est compact, il existe une suite croissante (K_j) d'intervalles compacts tels que $I = \bigcup_{j\geqslant 0} K_j$. On peut toujours supposer que γ est un paramétrage par longueur d'arc.
Pour tout hyperplan H fixé, la suite $\left(\#(\gamma(K_j)\cap H)\right)_{j\geqslant 0}$ est croissante et converge vers $\#(\gamma(I)\cap H)$. Par convergence monotone et le cas précédent, on obtient :

$$\begin{aligned}\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)} \#(\gamma(I)\cap H)\,\mathrm{d}\mu &= \int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)} \lim_{j\to+\infty} \#(\gamma(K_j)\cap H)\,\mathrm{d}\mu = \lim_{j\to+\infty}\int_{\mathcal{G}\mathrm{r}^+(\mathbb{R}^n)} \#(\gamma(K_j)\cap H)\,\mathrm{d}\mu \\ &= C_n \lim_{j\to+\infty} \mathrm{Leb}(K_j) = C_n\ell.\end{aligned}$$

5 Formule de Crofton sphérique

Dans cette section, on s'intéresse à une variante de la formule de Crofton pour des courbes tracées sur la sphère unité $\mathbb{S}^{n-1}\subset\mathbb{R}^n$, avec $n\geqslant 2$.
Dans ce cadre, les hyperplans affines sont remplacés par des équateurs de $\mathbb{S}^{n-1}$, c'est-à-dire des sous-ensembles de la forme $\mathbb{S}^{n-1}\cap\theta^\perp\simeq\mathbb{S}^{n-2}$, avec $\theta\in\mathbb{S}^{n-1}$. Chaque équateur est défini par exactement deux vecteurs de $\mathbb{S}^{n-1}$, opposés l'un de l'autre, induisant des orientations opposés sur $\theta^\perp$. On peut donc penser à $\theta\mapsto\mathbb{S}^{n-1}\cap\theta^\perp$ comme une bijection de $\mathbb{S}^{n-1}$ vers l'ensemble des "équateurs orientés".

Théorème 5.1 (Formule de Crofton)**.** *Soit $I\subset\mathbb{R}$ un intervalle. Soit $\gamma : I\to\mathbb{R}^n$ une courbe paramétrée de classe $\mathcal{C}^1$ et régulière. Notons $\ell=\int_I\|\gamma'(t)\|\,\mathrm{d}t\in[0,+\infty]$ sa longueur. On suppose que $\gamma(I)\subset\mathbb{S}^{n-1}$. Soit θ une variable aléatoire uniforme dans $\mathbb{S}^{n-1}$, alors :*

$$\mathbb{E}\Big[\#\Big(\gamma(I)\cap\theta^\perp\Big)\Big] = \frac{\ell}{\pi}.$$

Remarque. Comme dans le cas euclidien, $\#\big(\gamma(I)\cap\theta^\perp\big)$ est un abus de notation pour $\#\gamma^{-1}(\theta^\perp)$.

La preuve est la même que dans le cas euclidien. La différence principale est qu'on remplace les segments de droites par des arcs de grands cercles, qui sont les géodésiques sur $\mathbb{S}^{n-1}$.

5.1 Cas d'un arc de grand cercle

Soient $x,y\in\mathbb{S}^{n-1}$ distincts et non antipodaux. Alors $\mathrm{Vect}(x,y)$ est un plan et $\mathbb{S}^{n-1}\cap\mathrm{Vect}(x,y)\simeq\mathbb{S}^1$ est l'unique *grand cercle* de $\mathbb{S}^{n-1}$ contenant x et y. Le plus court des deux arcs joignant x à y dans $\mathbb{S}^{n-1}\cap\mathrm{Vect}(x,y)$ est $p([x,y])$, où on a noté $p:\mathbb{R}^n\setminus\{0\}\to\mathbb{S}^{n-1}$ la projection radiale.
On admettra que cet arc $p([x,y])$ est l'unique chemin de longueur minimale de x à y dans $\mathbb{S}^{n-1}$.

Définition 5.2 (Géodésique)**.** L'arc $p([x,y])$ est appelé la *géodésique* entre x et y.

Commençons par prouver le théorème 5.1 dans le cas où $\gamma(I)$ est une géodésique de longueur $\ell<\pi$. La mesure $\mathrm{d}\theta$ étant $SO_n(\mathbb{R})$-invariante, on peut se ramener à $\gamma : t\mapsto(\cos(t),\sin(t),0,\dots,0)$ de $I=[-\frac{\ell}{2},\frac{\ell}{2}]$ dans $\mathbb{S}^{n-1}$.
Soit $\theta\in\mathbb{S}^{n-1}$. Si $\theta\in\mathbb{S}^{n-1}\cap(\{0\}\times\mathbb{R}^{n-2})\simeq\mathbb{S}^{n-3}$ alors $\gamma(I)\subset\theta^\perp$ et $\#\big(\gamma(I)\cap\theta^\perp\big)=+\infty$. Heureusement, cet ensemble est de mesure nulle pour $\mathrm{d}\theta$ (c'est la mesure de $\{0\}\times\mathbb{R}^{n-2}$ pour la gaussienne standard de $\mathbb{R}^n$).
Sinon, $\mathbb{R}^2\times\{0\}$ n'est pas inclus dans $\theta^\perp$. Donc l'intersection de ces deux espaces est une droite vectorielle. Donc

$$\gamma(I)\cap\theta^\perp\subset(\mathbb{R}^2\times\{0\})\cap\theta^\perp\cap\mathbb{S}^{n-1}$$

est de cardinal au plus 2, et en fait au plus 1 car $\gamma(I)$ ne peut pas contenir deux points antipodaux. On a donc

$$\mathbb{E}\Big[\#\Big(\gamma(I)\cap\theta^\perp\Big)\Big]=\mathbb{P}\Big[\gamma(I)\cap\theta^\perp\neq\emptyset\Big]=\mathbb{P}\big[\exists t\in I,\langle\gamma(t)\,,\theta\rangle=0\big]=\mathbb{P}\left[\theta\in\bigcup_{t\in I}\gamma(t)^\perp\right].$$

Cette probabilité est la proportion de $\mathbb{S}^{n-1}$ occupée par $\bigcup_{t\in I}\gamma(t)^\perp$. Cette proportion est la même que la proportion du cercle $\mathbb{S}^{n-1}\cap\big(\mathbb{R}^2\times\{0\}\big)$ qui rencontre $\bigcup_{t\in I}\gamma(t)^\perp$. On obtient donc

$$\mathbb{E}\Big[\#\Big(\gamma(I)\cap\theta^\perp\Big)\Big]=\mathbb{P}\left[\theta\in\bigcup_{t\in I}\gamma(t)^\perp\right]=\frac{2\ell}{2\pi}=\frac{\ell}{\pi}.$$

5.2 Cas général

Passer du cas I compact au cas I quelconque se fait exactement comme dans le cas euclidien. Il s'agit donc de traiter le cas où $I=[0,\ell]$ et γ est un paramétrage par longueur d'arc.
Pour tout $k\geqslant 0$ et $i\in\{1,\dots,2^k\}$ on note $\widetilde{S}_{k,i}=p(S_{k,i})$ la géodésique de $\gamma\big(\frac{i-1}{2^k}\ell\big)$ à $\gamma\big(\frac{i}{2^k}\ell\big)$. On note $\widetilde{C}_k=p(C_k)=\bigcup_{i=1}^{2^k}\widetilde{S}_{k,i}$, qui est une approximation géodésique par morceaux de $\gamma(I)$. On peut alors montrer les équivalents des lemmes 4.2, 4.3 et 4.4 dans ce cadre, avec des preuves similaires. Commentons rapidement les différences.
Convergence des longueurs. Notons $\widetilde{\ell}_{k,i}$ la longueur de $\widetilde{S}_{k,i}$ et $\widetilde{\ell}_k$ celle de $\widetilde{C}_k$. Pour tout (k,i), $\ell_{k,i}\leqslant\widetilde{\ell}_{k,i}\leqslant\frac{\ell}{2^k}$, où $\frac{\ell}{2^k}$ est la longueur de la courbe joignant $\gamma\big(\frac{i-1}{2^k}\ell\big)$ à $\gamma\big(\frac{i}{2^k}\ell\big)$ en suivant γ.
En sommant sur i on obtient que : $\ell_k\leqslant\widetilde{\ell}_k\leqslant\ell$ pour tout $k\geqslant 0$. Le lemme 4.2 et le théorème des gendarmes montrent alors que $\widetilde{l}_k\xrightarrow[k\to+\infty]{}\ell$ sans faire plus d'efforts.
Condition de tangence. On veut montrer que l'équivalent de la condition 2 du lemme 4.3 est satisfaite presque surement. C'est-à-dire, on veut montrer que :

$$\mathbb{P}\Big[\theta^\perp\text{ est tangent à }\gamma(I)\Big]=\mathbb{P}\big[\exists t\in I\text{ tel que }\langle\gamma(t)\,,\theta\rangle=0=\langle\gamma'(t)\,,\theta\rangle\big]=0.$$

Malheureusement, le lemme 4.5 ne suffit pas à établir ce résultat. Il faut utiliser une version plus évoluée du théorème de Sard qui sort du cadre de ce cours.

6 Racines de polynômes aléatoires

On va maintenant appliquer la formule de Crofton sphérique (thm. 5.1) au calcul du nombre moyen de racines réelles d'un polynôme aléatoire.
L'ensemble des polynômes de $\mathbb{R}_d[X]$ (ou $\mathbb{C}_d[X]$) admettant une racine complexe multiple est décrit par une équation polynomiale en les coefficients (penser au discriminant quand $d=2$). C'est donc une hypersurface algébrique, qui sera de mesure nulle pour toute loi naturelle. Autrement dit, tout polynôme aléatoire raisonnable $P\in\mathbb{R}_d[X]$ (ou $\mathbb{C}_d[X]$), a presque surement d racines complexes.
Qu'en est-il du nombre de racines réelles ? Un polynôme générique de $\mathbb{C}_d[X]$ n'a pas de racine réelle. On se pose donc la question pour un polynôme aléatoire dans $\mathbb{R}_d[X]$.

6.1 Polynômes de Kac

Définition 6.1 (polynôme de Kac)**.** Un *polynôme de Kac* de degré d est un polynôme aléatoire $P\in\mathbb{R}_d[X]$ de la forme $P=\sum_{i=0}^d a_iX^i$, où les $(a_i)_{0\leqslant i\leqslant d}$ sont des $\mathcal{N}(0,1)$ indépendantes.

Théorème 6.2 (Kac, 1943)**.** *Soit P un polynôme de Kac de degré d, pour tout intervalle $I \subset \mathbb{R}$,*

$$\mathbb{E}\big[\#\big(P^{-1}(0)\cap I\big)\big] = \int_I \rho_d(t)\,\mathrm{d}t, \qquad \text{où} \qquad \rho_d : t \longmapsto \frac{1}{\pi}\sqrt{\frac{1}{(1-t^2)^2} - \frac{(d+1)t^{2d}}{(1-t^{2d+2})^2}}.$$

Corollaire 6.3. $\mathbb{E}\big[\#P^{-1}(0)\big] = \int_{\mathbb{R}} \rho_d(t)\,\mathrm{d}t \sim \frac{2}{\pi}\ln(d)$.

Exercice. Prouver le corollaire.

La fonction ρ_d est strictement positive sur $\mathbb{R}\setminus\{-1,1\}$ et diverge en ± 1. Elle donne la répartition en moyenne des racines de P dans $\mathbb{R}$. On peut vérifier (exercice) qu'en tant que mesures de probabilités :

$$\frac{\rho_d\,\mathrm{d}t}{\int_{\mathbb{R}}\rho_d(t)\,\mathrm{d}t} \xrightarrow[d\to+\infty]{\text{loi}} \frac{1}{2}(\delta_{-1}+\delta_1).$$

C'est-à-dire que les racines des polynômes de Kac se concentrent autour de ± 1 lorsque $d \to +\infty$.

Démonstration du théorème 6.2. La démonstration qu'on présente n'est pas démonstration originale de Kac [Kac43], mais une preuve alternative due à Edelman et Kostlan [EK95].
Soit $P = \sum_{i=1}^d a_i X^i \in \mathbb{R}_d[X]\setminus\{0\}$ déterministe, pour le moment. Notons $a = (a_0,\dots,a_d) \in \mathbb{R}^{d+1}$. Soit $m : t \mapsto (1,t,\dots,t^d)$ de $\mathbb{R}$ dans $\mathbb{R}^{d+1}$ la *courbe des moments*. Pour tout $t \in \mathbb{R}$,

$$P(t) = 0 \iff \sum_{i=1}^d a_i t^i = 0 \iff \langle a\,, m(t)\rangle = 0 \iff \left\langle \frac{a}{\|a\|}\,, \frac{m(t)}{\|m(t)\|}\right\rangle = 0 \iff \gamma(t) \in \theta^\perp,$$

où on a noté $\theta = \frac{a}{\|a\|}$ et $\gamma : t \mapsto \frac{m(t)}{\|m(t)\|}$.
Si maintenant P est un polynôme de Kac, alors $a \sim \mathcal{N}(0,\mathrm{Id})$ dans $\mathbb{R}^{d+1}$ et θ est uniforme dans $\mathbb{S}^d$. Par la formule de Crofton,

$$\mathbb{E}\big[\#(P^{-1}(0)\cap I)\big] = \mathbb{E}\Big[\#(\gamma^{-1}(\theta^\perp)\cap I)\Big] = \mathbb{E}\Big[\#(\gamma(I)\cap\theta^\perp)\Big] = \frac{1}{\pi}\int_I \|\gamma'(t)\|\,\mathrm{d}t.$$

Pour conclure il suffit de vérifier que $\|\gamma'(t)\|^2 = \frac{1}{(1-t^2)^2} - \frac{(d+1)t^{2d}}{(1-t^{2d+2})^2}$ pour tout $t \in \mathbb{R}$. □

Exercice. Faire le calcul.

6.2 Polynômes de Kostlan

Définition 6.4 (polynôme de Kostlan)**.** Un *polynôme de Kostlan* de degré d est un polynôme aléatoire $Q \in \mathbb{R}_d[X]$ de la forme $Q = \sum_{i=0}^d a_i\sqrt{\binom{d}{i}}X^i$, où les $(a_i)_{0\leqslant i\leqslant d}$ sont des $\mathcal{N}(0,1)$ indépendantes.

Théorème 6.5 (Kostlan, 1993)**.** *Soit $Q \in \mathbb{R}_d[X]$ polynôme de Kostlan, pour tout intervalle $I \subset \mathbb{R}$,*

$$\mathbb{E}\big[\#\big(Q^{-1}(0)\cap I\big)\big] = \sqrt{d}\int_I \frac{1}{(1+t^2)}\frac{\mathrm{d}t}{\pi}.$$

En particulier $\mathbb{E}\big[\#Q^{-1}(0)\big] = \sqrt{d}$.

Démonstration. La preuve est la même que celle du théorème 6.2, en remplaçant m par la courbe $\widetilde{m} : t \mapsto \left(1,\dots,\sqrt{\binom{d}{i}}t^i,\dots,t^d\right)$. Il suffit de vérifier que $\forall t \in \mathbb{R}$, $\|\widetilde{\gamma}'(t)\| = \frac{\sqrt{d}}{1+t^2}$, où $\widetilde{\gamma} = \frac{\widetilde{m}}{\|\widetilde{m}\|}$. □

On a de nouveau une densité moyenne de racines donnée par $\widetilde{\rho}_d = \sqrt{d}\rho$, où $\rho : t \mapsto \frac{1}{\pi(1+t^2)}$ est la densité de la loi de Cauchy. En particulier, la répartition en moyenne des racines ne dépend pas de d.

6.3 Pourquoi la loi de Kostlan ?

Une idée sous-jacente dans tout ce cours est que les mesures naturelles sur un espace sont les mesures invariantes sous l'action d'un groupe sympathique. De ce point de vue, on peut s'étonner du fait que la mesure de Kostlan sur $\mathbb{R}_d[X]$ donne un résultat plus sympathique que la mesure de Kac. En effet, Kac $\sim \mathcal{N}(0, \mathrm{Id})$ est invariante sous $O_{d+1}(\mathbb{R})$ alors que Kostlan $\sim \mathcal{N}(0, \Lambda_d)$ ne l'est pas, où

$$\Lambda_d = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \binom{d}{i} & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Cependant, choisir une gaussienne centrée revient à choisir sa matrice de covariance Λ, ce qui revient au choix d'un produit scalaire. Ici, Kac $\sim \mathcal{N}(0, \mathrm{Id})$ pour le produit scalaire tel que $(X^i)_{0 \leqslant i \leqslant d}$ est orthonormée, mais Kostlan $\sim \mathcal{N}(0, \mathrm{Id})$ pour le produit scalaire rendant $(\sqrt{\binom{d}{i}} X^i)_{0 \leqslant i \leqslant d}$ orthonormée. Sur $\mathbb{R}^n$ on avait un produit scalaire canonique. Sur $\mathbb{R}_d[X]$ on a plein de produits scalaires pertinents, par exemple les produits scalaires L^2 à poids. La question devient donc à savoir pourquoi le produit scalaire de Kostlan est plus pertinent que celui hérité de $\mathbb{R}^{d+1}$ en identifiant un polynôme au vecteur de ses coefficients.
Pour cela, remarquons que $\mathbb{R}_d[X] \simeq \mathbb{R}_d^{\mathrm{hom}}[X, Y]$ l'espace des polynômes homogènes de degré d en 2 variables, via $\sum_{i=1}^d a_i X^i \mapsto \sum_{i=1}^d a_i X^i Y^{d-i}$. Le produit de Kostlan correspond au produit scalaire sur $\mathbb{R}_d^{\mathrm{hom}}[X, Y]$ qui rend $(\sqrt{\binom{d}{i}} X^i Y^{d-i})_{0 \leqslant i \leqslant d}$ orthonormée. On peut vérifier qu'il est défini par :

$$\langle P \,, Q \rangle = \frac{1}{4\pi^2 d!} \int_{(w,z) \in \mathbb{C}^2} P(w, z) \overline{Q(w, z)} e^{-\frac{|w|^2 + |z|^2}{2}} \, \mathrm{d}w \, \mathrm{d}z. \tag{2}$$

À un facteur près, c'est le produit L^2 à poids gaussien standard pour les fonctions sur $\mathbb{C}^2 \simeq \mathbb{R}^4$.
Par ailleurs $O_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ naturellement, et donc $O_2(\mathbb{R}) \curvearrowright \mathbb{R}_d^{\mathrm{hom}}[X, Y]$ par $\Omega \cdot P = P \circ \Omega^{-1}$. On voit sur la formule (2) que le produit scalaire de Kostlan est invariant sous cette action. Il en est donc de même de la loi de Kostlan, c'est-à-dire la $\mathcal{N}(0, \mathrm{Id})$ sur $\mathbb{R}_d^{\mathrm{hom}}[X, Y]$ pour ce produit scalaire. Ce n'est pas le cas de la loi de Kac, ce qui explique pourquoi la loi de Kostlan est plus naturelle.
Si on voit $P \in \mathbb{R}_d^{\mathrm{hom}}[X, Y]$ comme une fonction sur $\mathbb{R}^2$, ses coefficients dépendent de la base orthonormée de $\mathbb{R}^2$ qu'on utilise pour les définir. En revanche, si P suit la loi de Kostlan, la loi de ses coefficients dans $\mathbb{R}^{d+1}$ ne dépend pas de la base de $\mathbb{R}^2$ utilisée pour les définir.
Pour conclure, remarquons que le produit scalaire de Kostlan sur $\mathbb{R}_d^{\mathrm{hom}}[X, Y]$ n'est pas l'unique produit scalaire invariant sous l'action de $O_2(\mathbb{R})$, même à constante près. Il existe une famille à paramètres de tels produits scalaires. En revanche, la formule (2) définit l'unique produit hermitien sur $\mathbb{C}_d^{\mathrm{hom}}[X, Y]$ invariant sous l'action de $U_2(\mathbb{C})$ par précomposition, à une constante près.

Références

[EK95] A. Edelman and E. Kostlan, *How many zeros of a random polynomial are real ?*, Bull. Amer. Math. Soc. **32** (1995), no. 1, 1–37.

[Kac43] M. Kac, *On the average number of real roots of a random algebraic equation*, Bull. Amer. Math. Soc. **49** (1943), no. 4, 314–320.