Probabilités Discrètes

Cours n°5 - Probabilités

EPITA 2025-2026

1 Introduction

Pour le moment, dans ce cours, nous avons travaillé les statistiques, la théorie des ensembles et la combinatoire. Nous verrons que chacun des outils définis lors des séances précédentes aura une utilité en probabilité.

Cette nouvelle séance est en majorité dédiée à la définition d'objets probabilistes classiques, et à leurs liens avec les notions étudiées précédemment.

En dernière partie nous verrons également un exemple illustrant le fait que les probabilités peuvent parfois paraître très contre-intuitive, et que pour les utiliser correctement il faut procéder de façon rigoureuse.

2 Vocabulaire

Afin de travailler au mieux en mathématiques, il est toujours nécessaires de se donner un cadre. Les probabilités n'échappent pas à ce constat, et cette partie est donc dédiée à la définition (d'une partie) du vocabulaire probabiliste que nous utiliserons dans la suite du cours.

Pour étudier une expérience via le prisme des probabilités, celle-ci doit être décrite par :

- des **issues**
- un **univers**
- des **évènements**
- une **probabilité**

Définissons donc ces différents objets.

Définition : On appelle **issue** d'une expérience probabiliste tous les résultats possibles de cette expérience. Une issue est souvent notée ω.

Définition : On appelle **univers** d'une expérience probabiliste l'ensemble des issues de cette expérience. On le note souvent Ω.

Remarque : Ce cours est un cours de probabilités discrètes, cela signifie que tous les univers que nous étudierons seront soit finis, soit dénombrables.

Définition : On appelle **évènement** d'une expérience probabiliste un sous-ensemble de l'univers de cette expérience.

Notation : Un évènement se note comme suit :

$$\{nom\ de\ l'évènement\} : "\{description\ de\ l'évènement\}"$$

Exemple :
A : "n est un nombre pair"
B : "Deux personnes font la même taille"

Avant de définir ce qu'est une probabilité, nous avons besoin d'un petit rappel de théorie des ensembles.

Rappel : Soit E un ensemble. On appelle **ensemble des parties** de E l'ensemble qui contient tous les sous-ensembles de E. On note cet ensemble $\mathcal{P}(E)$.

Nous pouvons maintenant revenir à la définition de probabilité.

Définition : Dans une expérience probabiliste d'univers Ω, on appelle **probabilité**, ou **loi de probabilité**, toute fonction $\mathbb{P}$ définie sur l'ensemble des parties de Ω, et à valeur dans $[0, 1]$, telle que

$$\begin{cases} \sum_{\omega\in\Omega} \mathbb{P}(\omega) = 1 \\ \mathbb{P}(A) = \sum_{\omega\in A} \mathbb{P}(\omega) \qquad \forall A \in \mathcal{P}(\Omega) \end{cases} .$$

Remarque : Une issue ω n'est jamais dans $\mathcal{P}(\Omega)$ (par contre $\{\omega\} \in \mathcal{P}(\Omega)$), les formules ci-dessus utilisent donc l'abus de notation

$$\mathbb{P}(\omega) = \mathbb{P}(\{\omega\}) .$$

Pour conclure cette partie, il nous reste une dernière définition importante à donner :

Définition : On appelle (dans ce cours) **espace de probabilité** tous couple $(\Omega, \mathbb{P})$ où Ω est un ensemble discret et $\mathbb{P}$ une probabilité sur Ω.

3 Opérations probabilistes

Comme nous l'avons vu dans la partie précédente, les *évènements* avec lesquels nous travaillons en probabilité sont des ensembles, nous pouvons donc les manipuler avec les opérateurs ensemblistes que nous connaissons. De même, les *probabilités* sont des fonctions réelles, c'est à dire qu'elles prennent des valeurs numériques réelles, on peut donc traiter leurs valeurs avec des opérateurs numériques. Nous verrons de plus dans cette partie qu'il y a une correspondance entre les ensembles, les probabilités sur ces ensembles, et les opérations utilisables sur chacun.

Remarque : Il faut donc bien faire attention à utiliser des opérateurs ensemblistes pour manipuler des évènements, et des opérateurs numériques pour manipuler leurs probabilités.

Tout d'abord, la définition de probabilités nous permet directement d'obtenir quelques résultats intéressants. Si l'on étudie un espace de probabilité $(\Omega, \mathbb{P})$, on a les assertions suivantes :

- $\mathbb{P}(\Omega) = 1$.
- $\mathbb{P}(\emptyset) = 0$.
- $\forall A \in \mathcal{P}(\Omega)$, $\mathbb{P}(\overline{A}) = 1 - \mathbb{P}(A)$.
- $\forall A, B \in \mathcal{P}(\Omega)$, $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$. En particulier, si $A \cap B = \emptyset$, on a $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$ et $\mathbb{P}(\Omega) = \mathbb{P}(A \cup \overline{A}) = \mathbb{P}(A) + \mathbb{P}(\overline{A}) = 1$.
- $\forall A, B \in \mathcal{P}(\Omega)$ tels que $A \subset B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.
- $\forall A, B \in \mathcal{P}(\Omega)$, $\mathbb{P}(A) = \mathbb{P}(A \backslash B) + \mathbb{P}(A \cap B)$.

4 Exemple de loi de probabilité : la loi uniforme

En probabilité on peut définir des lois de probabilités de bien des façons, mais certaines sont plus connues que d'autres, on les appelles **lois usuelles**. Nous définissons ici un premier exemple de loi usuelle.

Définition : Soit Ω un ensemble de cardinal $n \in \mathbb{N}$.
On appelle **loi uniforme** sur Ω la probabilité $\mathbb{P}$ définie par

$$\forall \omega \in \Omega \ , \ \mathbb{P}(\omega) = \frac{1}{n} \ .$$

5 Un exemple contre-intuitif : le paradoxe des anniversaires

L'objectif de cette partie est d'étudier un premier exemple de loi de probabilité contre-intuitif, afin de motiver l'utilisation rigoureuse du formalisme mathématiques en probabilité. L'exemple que nous allons voir est de plus très utile en cybersécurité.

Nous nous plaçons dans le contexte suivant : En observant un groupe de $n \in \mathbb{N}$ personnes, et en sachant qu'aucune d'entre n'est née un 29 février, quelle est la probabilité que deux personnes soit né le même jour dans l'année ? Quelle doit être la valeur de n pour que cette probabilité dépasse $0,5$?

Pour répondre à cette question, nous devons tout d'abord définir l'univers Ω de notre expérience. Notons $G = \{1, ..., n\}$ l'ensemble des personnes du groupe, et $D = \{1, ..., 365\}$ leurs dates de naissance possibles. L'univers Ω est alors l'ensemble des associations possibles de chaque élément de G à un élément de D. Autrement dit, c'est l'ensemble des applications de G dans D. Cet ensemble est noté D^G, et il est de cardinal 365^n.

Comme la date de naissance de chaque personne a une chance égale de tomber n'importe quel jour dans l'année, nous sommes dans un cas de loi uniforme pour chaque date d'anniversaire. On en déduit que pour $A \in \mathcal{P}(\Omega)$,

$$\mathbb{P}(A) = \frac{|A|}{|\Omega|} = \frac{|A|}{365^n} \ .$$

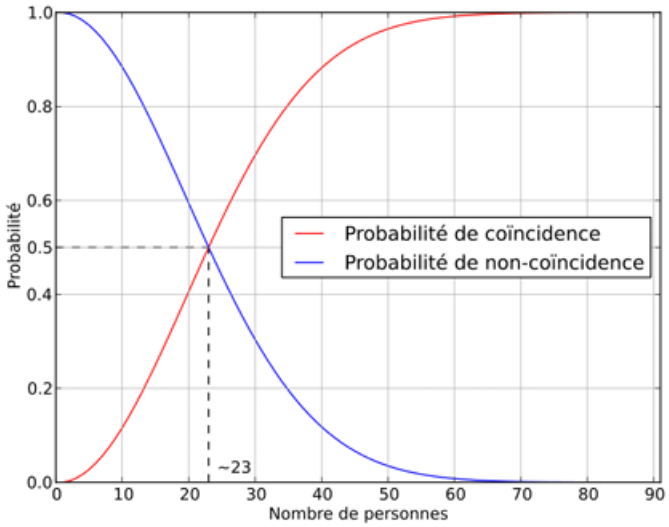
Intéressons nous maintenant à l'évènement C : "deux personnes sont nées le même jour". Pour

calculer $\mathbb{P}(C)$ on calcule plutôt $\mathbb{P}(\overline{C})$, c'est plus simple. On obtient :

$$\mathbb{P}(C) = 1 - \mathbb{P}(\overline{C}) = 1 - \frac{A_n^{365}}{365^n} = 1 - \frac{365!}{(365-n)!365^n} \ .$$

Remarque : Si $n > 365$, on peut tout de suite en déduire que $\mathbb{P}(C) = 1$.

Si on trace le graphe des fonctions $f : n \mapsto 1 - \frac{365!}{(365-n)!365^n}$ et $g : n \mapsto \frac{365!}{(365-n)!365^n}$ on obtient :



Remarque : f représente la probabilité de coïncidence en fonction du nombre de personnes n, et g la probabilité de non-coïncidence.

Trouver n tel que la probabilité de C soit égale à $0,5$ revient à résoudre l'équation

$$\mathbb{P}(C) = \mathbb{P}(\overline{C})$$

c'est-à-dire

$$1 - \frac{365!}{(365-n)!365^n} = \frac{365!}{(365-n)!365^n}$$

Le graphique nous indique que la solution sera environ $n = 23$.

Remarque : En général on considère que pour trouver, avec probabilité 0.5, deux éléments identiques dans un ensemble à N éléments, il faudra tester $n \approx \sqrt{N}$ éléments.

Cette solution peut paraître contre-intuitive car 23 peut paraître très petit en comparaison de 365. Ceci entraîne un paradoxe que l'on appelle paradoxe des anniversaires en hommage au problème que l'on vient de traiter. Ce paradoxe est dû à la confusion entre le problème auquel on vient de répondre, et le problème suivant :

Dans un groupe de n personnes, trouver une personne qui a la même date de naissance que la personne numéro 1 (et qui n'est pas la personne numéro 1).

La différence entre les deux problèmes réside dans le fait que le second problème fixe une date à trouver, alors que le premier recherche une collision entre deux dates anniversaires, sans fixer cette date.

6 Exercices

Exercice 1 :

1. Combien existe-t-il de nombre entier s'écrivant avec exactement k chiffres significatifs en base 2 ?
   Remarque : Lorsqu'on lit les nombres de gauche à droite, un chiffre significatif est un chiffre placé à droite du premier chiffre non nul.
2. Combien existe-t-il de nombres entiers s'écrivant avec au plus k chiffres significatifs en base 2 ?
3. Comment répondre rapidement à la question 2 sans faire de somme ?
4. Faire le lien avec l'ensemble des parties.

Exercice 2 :
On considère un jeu de pile ou face infini : on tire une pièce à pile ou face une infinité de fois. Proposer un univers pour cette expérience.

Exercice 3 :
On jette deux fois un dé équilibré à 6 faces (numérotées de 1 à 6). On considère les évènements

E : "La somme des points obtenus est paire."
F : "Le 3 est obtenu au moins une fois."

1. Calculer $\mathbb{P}(E)$ et $\mathbb{P}(F)$.
2. Donner la signification et la probabilité des évènements $E \cap F$, $E \cup F$, $E \cap \overline{F}$, $E \cap \overline{F} \cup \overline{E}$.

Exercice 4 :
Une urne contient 2 boules blanches et quatre boules noires. On tire successivement et au hasard toutes les boules de l'urne. Quelle est la probabilité que toutes les boules blanches soient tirées lors des 4 premiers tirages ?

Exercice 5 :
Soit Ω un ensemble de cardinal $n \in \mathbb{N}^*$. Montrer qu'il y a 2^{n-1} éléments de cardinal pair dans $\mathcal{P}(\Omega)$.

Exercice 6 :
Une urne contient n boules dont b boules blanches et r boules rouges. On tire une première boule, on la remet dans l'urne et on ajoute une seconde boule de la même couleur dans l'urne. On tire ensuite une seconde boule.

1. Décrire l'univers Ω de cette expérience.
2. Quelle est la probabilité de tirer deux boules blanches ?
3. Quelle est la probabilité que la seconde boule tirée soit blanche ?

Exercice 7 :
Soient Ω un ensemble et $A, B \subset \mathcal{P}(\Omega)$.
Démontrer les formules du cours :

1. $\mathbb{P}(\overline{A}) = 1 - \mathbb{P}(A)$.
2. $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.
3. Si $A \cap B = \emptyset$, $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$
4. $\mathbb{P}(\Omega) = \mathbb{P}(A \cup \overline{A}) = \mathbb{P}(A) + \mathbb{P}(\overline{A}) = 1$.
5. Si $A \subset B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.
6. $\mathbb{P}(A) = \mathbb{P}(A \backslash B) + \mathbb{P}(A \cap B)$.

Exercice 8 : Fonction de hachage
En informatique, une fonction de hachage est une fonction qui prend en entrée une donnée de taille quelconque, et qui renvoie une donnée de taille fixe. On dit que l'on hache la donnée en entrée. C'est un type de fonction souvent utilisé en cybersécurité. Dans cet exercice, nous allons voir un exemple de fonction de hachage.
Attention : c'est un exemple très basique, à ne surtout pas utiliser en pratique !

Soient $n \in \mathbb{N}$ et h la fonction qui prend en entrée une chaîne de bits de taille $m \geq n$ quelconque et qui renvoie les n bits de poids faibles de la chaîne.

Définition : on appelle collision de h deux éléments $x_1 \neq x_2$ de l'ensemble de définition D_h de h tels que $h(x_1) = h(x_2)$.

1. Pour $n = 2$ et si D_h est l'ensemble des chaînes de bits de taille supérieur ou égale à 2, trouver une collision sur h.

Dans la suite on considère que h renvoie n bits de l'entrée, mais on ignore lesquels.

2. Quelle est le cardinal de l'image de h ?
3. Combien de chaînes de bits devra-t-on tester pour avoir environ une chance sur deux de trouver une collision sur h ?