

Événements, probabilités, variables aléatoires.

1 Espaces de probabilités.

Définition 1. Un *espace de probabilité* est la donnée de

- ▷ un ensemble Ω ;
- ▷ un ensemble $\mathcal{F} \subseteq \wp(\Omega)$ de parties de Ω , appelées *événements* ;
- ▷ une fonction $P : \mathcal{F} \rightarrow [0, 1]$ qui associe à un événement sa probabilité ;

qui vérifie les axiomes suivants

1. l'ensemble \mathcal{F} est une *tribu* (ou σ -algèbre) :
 - ▷ $\Omega \in \mathcal{F}$;
 - ▷ si $A \in \mathcal{F}$ alors $\Omega \setminus A \in \mathcal{F}$;
 - ▷ si $(A_n)_{n \in \mathbb{N}}$ est dans \mathcal{F} alors $\bigcup_{n \in \mathbb{N}} A_n \in \mathcal{F}$;
2. l'application P est une *mesure de probabilité* :
 - ▷ $P(\Omega) = 1$;
 - ▷ $P(\emptyset) = 0$;
 - ▷ [σ -additivité] si $(A_n)_{n \in \mathbb{N}}$ sont des événements disjoints (*i.e.* $A_n \cap A_m = \emptyset$ si $n \neq m$) alors

$$P\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sum_{n \in \mathbb{N}} P(A_n).$$

On supposera donné un espace de probabilité (Ω, \mathcal{F}, P) .

Exemple 1. Si Ω est un ensemble fini, on peut choisir $\mathcal{F} = \wp(\Omega)$ et $P(A) = |A|/|\Omega|$. On dit que P est la *probabilité uniforme* sur Ω .

Exemple 2. Si Ω est fini ou dénombrable et si $(p_\omega)_{\omega \in \Omega}$ sont des réels positifs tels que $\sum_{\omega \in \Omega} p_\omega = 1$, on peut prendre $\mathcal{F} = \wp(\Omega)$ et poser $P(A) = \sum_{\omega \in A} p_\omega$. On a alors défini une probabilité à partir de $p_\omega = P(\{\omega\}) = p_\omega$.

Si A et B sont deux événements avec $A \subseteq B$ alors $P(A) \leq P(B)$. En effet, il suffit d'écrire $P(B) = P(A) + P(B \setminus A)$.

Lemme 1 (Borne de l'union). Si $(A_n)_{n \in I}$ est une famille finie ou dénombrable d'événements, alors

$$P\left(\bigcup_{n \in I} A_n\right) \leq \sum_{n \in I} P(A_n).$$

Preuve. On pose $B_n = A_n \setminus \left(\bigcup_{k < n} A_k\right)$. Les (B_n) sont disjoints, et $\bigcup_{n \in I} A_n = \bigcup_{n \in I} B_n$. On a donc

$$P\left(\bigcup_{n \in I} A_n\right) = P\left(\bigcup_{n \in I} B_n\right) = \sum_{n \in I} P(B_n) \leq \sum_{n \in I} P(A_n).$$

□

Une question naturelle est : pourquoi ne pas prendre toujours $\mathcal{F} = \wp(\Omega)$?

- ▷ Il y a des cas où on ne peut pas, pour des raisons liées à l'infini (en particulier dans le cas non dénombrable).
- ▷ Même dans le cas discret, on a parfois intérêt à considérer plusieurs tribus.

2 Indépendance.

Définition 2. Deux événements A et B sont *indépendants*, noté $A \perp B$, si $P(A \cap B) = P(A) \times P(B)$.

Définition 3. Si $P(B) > 0$, la *probabilité de A selon B* est la probabilité $P(A | B) = P(A \cap B)/P(B)$. On a donc $A \perp B \iff P(A | B) = P(A)$.

Lemme 2. Si (A_n) est une partition fini ou dénombrable de Ω en événements et B un événement,

$$P(B) = \sum_n P(B \cap A_n) = \sum_n P(B | A_n) \cdot P(A_n).$$

□

Définition 4. Si (A_i) est une famille finie ou infinie d'événements, on dit qu'ils sont *indépendants* si, pour tout $J \subseteq I$ non-vide,

$$P\left(\bigcap_{i \in J} A_i\right) = \prod_{i \in J} P(A_i).$$

Exemple 3. On a que (A, B, C) sont indépendants si et seulement si les quatre conditions sont vérifiées :

- ▷ $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$;
- ▷ $P(A \cap B) = P(A) \cdot P(B)$;
- ▷ $P(A \cap C) = P(A) \cdot P(C)$;
- ▷ $P(B \cap C) = P(B) \cdot P(C)$.

Remarque 1. On a l'implication « (A_n) indépendant » \implies « (A_n) deux-à-deux indépendant » mais la réciproque est *fausse*.

3 Théorèmes d'existence.

Le théorème suivant justifie l'existence des suites finies ou dénombrables de « *bits* aléatoires indépendants ».

- Théorème 1** (Existence de *bits* aléatoires). 1. Pour tout entier $n \in \mathbb{N}$, il existe un espace de probabilité $(\Omega_n, \mathcal{F}_n, P_n)$ qui contient n événements indépendants de probabilité $\frac{1}{2}$.
2. Il existe un espace de probabilité (Ω, \mathcal{F}, P) qui contient une suite dénombrable d'événements de probabilité $\frac{1}{2}$.

Preuve. 1. On pose $\Omega_n = \{0, 1\}^n$, $\mathcal{F}_n = \wp(\Omega_n)$, et P_n la probabilité uniforme. Si on pose

$$A_k = \{ \omega = (\omega_1, \dots, \omega_n) \in \{0, 1\}^n \mid \omega_k = 1 \},$$

alors

$$P(A_k) = \frac{|A_k|}{|\Omega_n|} = \frac{2^{n-1}}{2^n} = \frac{1}{2}.$$

Si $J \subseteq \{1, \dots, n\}$, en notant $p = |J|$, alors

$$P\left(\bigcap_{j \in J} A_j\right) = \frac{\left|\bigcap_{j \in J} A_j\right|}{|\Omega_n|} = \frac{2^{n-p}}{2^n} = \frac{1}{2^p} = \prod_{j \in J} P(A_j).$$

On a donc indépendance de $(A_k)_{1 \leq k \leq n}$.

2. On l'admet (\triangleright existence de la mesure de Lebesgue).

□