1. Probabilités discrètes
   - Espace de probabilité
   - Probabilité conditionnelle
   - Indépendance
   - Variables aléatoires et Espérance

Motivation

En informatique

- les données peuvent être aléatoires ou bruitées
- les algorithmes peuvent être probabilistes (Ex. test de primalité)
- les pannes sont imprévisibles

On souhaite avoir des algorithmes efficaces (pour des données typiques), résistants (aux pannes aléatoires), corrects (presque corrects, presque toujours),...

Dénombrement et probabilité

Exemple

Un algorithme trouve votre mot de passe une fois sur deux.

- Si on exécute l'algorithme 3 fois, combien de résultats sont possibles ?
- Quel est le pourcentage de chances de trouver votre mot de passe ?

Exemple

Un algorithme choisit au hasard 3 sommets d'un graphe et répond Vrai si les 3 sommets forment un triangle.

- Combien y a-t-il d'exécutions possibles ?
- Si le graphe est complet, quelle est la probabilité de trouver un triangle ? Si le graphe contient un unique triangle ?

Dénombrement et probabilité

Exemple

Considérant une famille qui a au plus trois enfants :

- Combien y a-t-il de fratries possibles ?
- Combien y a-t-il de fratries avec au moins un garçon et au moins une fille ?
- Quel est le pourcentage des familles à au plus trois enfants qui ont au moins un garçon et au moins une fille ?

Tirages, événements

Un tirage consiste à prendre un élément au hasard dans un ensemble fini Ω, appelé univers. Un évènement concerne une propriété de l'élément choisi.

Exemple

Il y a 3 dragibus roses, 4 dragibus verts et 5 dragibus bleus dans un sac. Alice aime uniquement les dragibus verts. Quelle est la probabilité qu'elle en obtienne un si elle tire un bonbon au hasard ?

Si B représente l'ensemble des bonbons, V représente l'ensemble des dragibus verts, et x est le bonbon tiré par Alice alors l'événement "Alice a tiré un dragibus verts" se traduit par "$x \in V$". On identifie cet évènement à l'ensemble V. Sa probabilité est $\mathbb{P}(V) = \frac{|V|}{|B|}$.

Tirages, événements

Exemple

Il y a 3 dragibus roses, 4 dragibus verts et 5 dragibus bleus dans un sac. Alice aime uniquement les dragibus verts et les roses. Quelle est la probabilité qu'elle en ait un si elle tire un bonbon au hasard ?

Si V représente l'ensemble des dragibus verts, R l'ensemble des dragibus roses, et x est le bonbon tiré par Alice alors l'événement "Alice a tiré un dragibus vert ou rose" se traduit par "$x \in V$ ou $x \in R$" ce qui revient à dire "$x \in V \cup R$". Sa probabilité est $\mathbb{P}(V \cup R) = \frac{|V \cup R|}{|B|}$.

Tirages, événements

Exemple

Il y a 6 couleurs différentes de dragibus, 4 de chaque couleur dans un sac. Alice aime tous les dragibus sauf les bleus. Quelle est la probabilité qu'elle en ait tiré un qu'elle aime un si elle tire un bonbon au hasard ?

Si N représente l'ensemble des dragibus bleus, et x est le bonbon tiré par Alice alors l'événement "Alice n'a pas tiré un dragibus bleu" se traduit par "$x \notin N$" ce qui revient à dire "$x \in B \setminus N$". Sa probabilité est $\mathbb{P}(\overline{N}) = \frac{|B|-|N|}{|B|}$.
Attention : on a supposé que chaque bonbon avait la même probabilité d'être tiré !

Espaces et univers

Définition

Un espace de probabilité (ou espace probabilisé) est un couple $(\Omega, \mathbb{P})$.

- L'ensemble fini (ou discret) Ω est appelé univers.
- Les éléments de Ω sont appelés évènements élémentaires.
- L'application $\mathbb{P} : \Omega \to [0,1]$ de probabilité est telle que :

$$\sum_{x \in \Omega} \mathbb{P}(x) = 1$$

- Un sous-ensemble $A \subseteq \Omega$ est un évènement et sa probabilité est

$$\mathbb{P}(A) = \sum_{x \in A} \mathbb{P}(x).$$

Exemples

lancers de un dé, de deux dés, prélèvement de deux boules dans une urne ...

Pour s'échauffer

Exercice(s)

Exercices 1 à 3 de la feuille de TD5

Tirages indépendants

Un tirage peut être composé de plusieurs tirages indépendants. Par exemple, on tire un dé deux fois, on répète un algorithme 2 fois, etc. Si on tire un élément dans $(\Omega, \mathbb{P})$ et on tire indépendamment un élément dans $(\Omega', \mathbb{P}')$, alors la distribution jointe sera un tirage dans $(\Omega \times \Omega', \mathbb{P} \cdot \mathbb{P}')$.

Exemple

On tire à pile ou face avec une pièce non-biaisée. L'univers $\Omega = \{P, F\}$ et $\mathbb{P}(P) = \mathbb{P}(F) = \frac{1}{2}$. Si on effectue 2 tirages successifs de façon indépendantes, l'univers est

$$\{P, F\} \times \{P, F\} = \{(P, P), (P, F), (F, P), (F, F)\}.$$

La probabilité de (P, P) est

$$\mathbb{P}(P) \cdot \mathbb{P}(P) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}.$$

Probabilité uniforme

Définition

Une probabilité est dite uniforme quand pour tout évènement élémentaire $\omega \in \Omega$, on a :

$$\mathbb{P}(\omega) = \frac{1}{|\Omega|}$$

Exemple

Probabilité uniforme : Lancer d'un dé cubique équilibré. Lancer de 2 pièces équilibrées.

Probabilité non-uniforme : Une urne contient 3 boules rouges et 3 boules bleues. On tire 2 boules au hasard, sans remise. Quelle est la probabilité de tirer 2 boules bleues ? Quelle est la probabilité de tirer une bleue et une rouge (dans cet ordre) ?

Probabilité non-uniforme

Exemple

Un algorithme trouve votre mot de passe une fois sur trois.

- Si on exécute l'algorithme 3 fois, quels sont les huit évènements élémentaires ?
- Quelle est la probabilité de chaque événement élémentaire ?
- A quel ensemble d'événements élémentaires correspond l'événement "le mot de passe a été trouvé" ?
- Quelle est la probabilité de trouver votre mot de passe ?

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

Un dé rouge et un dé vert sont lancés, quelle est la probabilité que l'un des deux dés donne un 2 ?

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

Un dé rouge et un dé vert sont lancés, quelle est la probabilité que l'un des deux dés donne un 2 ?

$$\begin{aligned} P(R2 \cup G2) &= P(R2) + P(G2) - P(R2 \cap G2) \\ &= \frac{1}{6} + \frac{1}{6} - \frac{1}{36} \\ &= \frac{11}{36} \end{aligned}$$

Propriété des probabilités

Proposition

- $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$ *(principe d'inclusion exclusion)*
- $\mathbb{P}(A \cup A^c) = 1$
- *Si* $A \subseteq B$, $\mathbb{P}(A) \leq \mathbb{P}(B)$.

Exemple

- Quelle est la probabilité que lors du lancer d'un dé, le dé donne 1 ou un nombre strictement plus grand que 1 ?
- Lors du lancer d'un dé, que dire de la probabilité d'obtenir un 2 par rapport à celle d'obtenir un nombre pair ?

Pour s'échauffer

Exercice(s)

Exercices 4 à 8 de la feuille de TD5

Parenthèse combinatoire : Principe d'inclusion-exclusion

Rappel

Soient A et B deux évènements.

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$$

Théorème

Soit $A_1, \ldots, A_n$ des ensembles. Le nombre d'éléments de $A_1 \cup \ldots \cup A_n$ est donné par :

$$\begin{aligned} |A_1 \cup \ldots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_{n-2}| \\ &= \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}| \end{aligned}$$

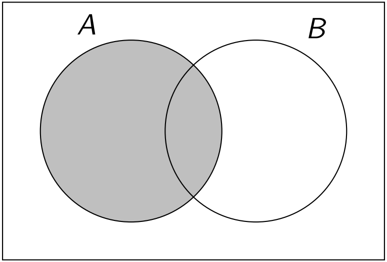
Pour s'échauffer

Exercice(s)

Exercice 10 et 11 de la feuille de TD 5

Probabilité conditionnelle

Étant donné deux événements A et B, la probabilité conditionnelle de B sachant A est la probabilité de B sachant que l'événement A est avéré.
Si A est avéré, l'univers des événements élémentaires qui restent possibles est limité à l'ensemble A.
La loi de probabilité sur l'univers réduit à l'ensemble A doit être *renormalisée* afin que les probabilités somment à 1. On calcule donc la probabilité de B, sachant A, par rapport à cette nouvelle distribution.



Loi de Bayes

Proposition

Si $\mathbb{P}(B) \neq 0$, la probabilité conditionnelle de B sachant A est donnée par :

$$\mathbb{P}(B|A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(A)}.$$

ou de façon équivalente :

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot P(B|A).$$

“Choisir A et B revient à choisir A, puis choisir B sachant que A s’est produit”

Indépendance

Soient A et B deux événements sur un même espace de probabilité $(\Omega, \mathbb{P})$. Intuitivement deux événements sont indépendants si l'un n'influence pas la probabilité de l'autre.

Exemple

On lance un dé. L'événement "le résultat est pair" et l'événement "le résultat est 4" ne sont PAS indépendants !

Indépendance

Définition

Si $\mathbb{P}(B) \neq 0$, A et B sont indépendants si et seulement si

$$\mathbb{P}(A|B) = \mathbb{P}(A).$$

Proposition

A et B sont indépendants si et seulement si

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B).$$

Indépendance

Exemple

On lance onze fois de suite une pièce équilibrée. Que dire des événements

- $A =$ "le résultat des 10 premiers lancers est face" et
- $B =$"le onzième lancer donne face"?

Indépendance

Exemple

On lance 2 dés. On considère trois événements.

- A = “Le premier est un 2”
- B = “Le second est un 5”
- C = “La somme des dés est 7.”

Quelles sont les paires d’événements indépendants ?
Pensez-vous que les 3 événements sont indépendants ?

Indépendance

Soient $A_1, \ldots, A_k$, k événements.

Définition

Les A_k sont indépendants si et seulement si

$$\mathbb{P}(A_{i_1} \cap \ldots \cap A_{i_p}) = \prod_{j=1}^{p} \mathbb{P}(A_{i_j}),$$

pour tout $\{i_1, \ldots, i_p\} \subseteq \{1, \ldots, k\}$, $i_1 < i_2 < \ldots < i_p$.

Attention

Parfois il faut conditionner sur plusieurs événements pour voir apparaître un effet sur la probabilité conditionnelle d'un autre événement. (voir TD 5 Exercice 13 pour autre exemple)

Pour s'échauffer

Exercice(s)

Exercice 1 à 3 TD6

Exercice 9 TD5

Probabilités conditionnelles et indépendance

Exemple

Supposons que quatre pièces équilibrées sont lancées. Considérons les trois événements suivants
A="Au moins deux pièces sont côté face",
B="Au plus deux pièces sont côté face"
et C="Exactement deux pièces sont côté face".
Calculez :

1. $\mathbb{P}(A)$
2. $\mathbb{P}(B)$
3. $\mathbb{P}(C)$
4. $\mathbb{P}(A|B)$
5. $\mathbb{P}(A|C)$
6. $\mathbb{P}(A \cup B)$

Bonus : Indépendance vs disjonction

Attention

Différence entre indépendance et disjonction ! !

Considérons un jeu de 52 cartes dans lequel on tire au hasard une carte.
K="cette carte est un roi"
T="cette carte est un trèfle"
Q="cette carte est une reine"

Question

- K et T sont-ils indépendants ? disjoints ?
- Q et T sont-ils indépendants ? disjoints ?

exemple d'événements indépendants et disjoints ? il faut que l'un des deux soit trivial

Bonus : Indépendance vs disjonction

Attention

Différence entre indépendance et disjonction ! !

Considérons un jeu de 52 cartes dans lequel on tire au hasard une carte.
K="cette carte est un roi"
T="cette carte est un trèfle"
Q="cette carte est une reine"

Question

- K et T sont-ils indépendants ? disjoints ?
- Q et T sont-ils indépendants ? disjoints ?

Réponse

K et T sont indépendants mais non disjoints et K et Q sont disjoints mais non indépendants.

exemple d'événements indépendants et disjoints ? il faut que l'un des deux

Un peu de pratique

Exercice(s)

Exercice 4 TD6

Variable aléatoire

On peut associer une valeur aux événements élémentaires.

Définition

Une variable aléatoire est une application de Ω dans $\mathbb{R}$ (souvent dans $\mathbb{N}$).

Soit X une variable aléatoire. On associe au prédicat "$X = v$" l'ensemble d'événements élémentaires correspondant : $X^{-1}(v) = \{\omega \in \Omega | X(\omega) = v\}$.

Notation

Nous écrirons $\mathbb{P}(X = v)$ pour la probabilité de l'événement associé $\mathbb{P}(X^{-1}(v))$.

Exemple

À une expérience de lancer successif de deux dés, on peut associer les variables aléatoires suivantes, pour w le résultat des deux lancers :
$S(w) =$ somme des points sur le dessus du dé
$P(w) =$ produit des points sur le dessus du dé

Espérance (=comportement moyen)

Définition

La *valeur moyenne*, ou *espérance*, d'une variable aléatoire X est définie par

$$\mathbb{E}(X) = \sum_{\omega \in \Omega} \mathbb{P}(\omega) \cdot X(\omega).$$

Proposition

Si X et Y sont deux variables aléatoires,

$$\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y).$$

Plus généralement, l'espérance est linéaire, c'est-à-dire que pour tout α, β,

$$\mathbb{E}(\alpha X + \beta Y) = \alpha \mathbb{E}(X) + \beta \mathbb{E}(Y).$$

Espérance

Exemple

- $\mathbb{E}(S)$
- $\mathbb{E}(\mathbb{1}_A)$ pour $A \in \Omega$ et $\mathbb{1}_A$ la variable aléatoire qui vaut 1 sur les événements élémentaires $\omega \in A$ et 0 sinon.
- ...

Indépendance des variables aléatoires

Définition

Si les variables ne prennent que des valeurs entières positives, les variables aléatoires X et Y sont indépendantes si et seulement si pour tout couple (m, n) de nombres naturels,

$$\mathbb{P}((X = m) \cap (Y = n)) = \mathbb{P}(X = m) \cdot \mathbb{P}(Y = n).$$

Exemple

Les variables aléatoires S et P sont-elles indépendantes ?

Espérance

Proposition

Si X et Y sont deux v.a. sur le même espace de probabilité, on a :

$$\mathbb{E}(X+Y) = \mathbb{E}(X) + \mathbb{E}(Y).$$

Plus généralment, l'espérance est linéaire, c'est-à-dire que pour tout α, β,

$$\mathbb{E}(\alpha X + \beta Y) = \alpha\mathbb{E}(X) + \beta\mathbb{E}(Y).$$

De plus, si X et Y sont indépendantes,

$$\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$$

Exemple

Calculer $\mathbb{E}(P)$.
Considérons un lancer de dé, $X = \mathbb{1}_{\omega=1}$ et $Y = \mathbb{1}_{\omega=2}$, calculer $\mathbb{E}(XY)$, $\mathbb{E}(X)$ et $\mathbb{E}(Y)$.

Un peu de pratique

Exercice(s)

Exercices 5 et 6 de la feuille de TD6

Loi binomiale

On effectue n tirages indépendants d'une expérience qui réussit avec probabilité $1/2$ et échoue avec probabilité $1/2$. Soit X la variable aléatoire qui représente le nombre de succès obtenus sur les n tirages. Que vaut $\mathbb{P}(X = k)$?

Si maintenant on effectue n tirages indépendants d'une expérience qui réussit avec probabilité p, que vaut $\mathbb{P}(X = k)$?

On appelle cette loi la loi binomiale.

Rappel : Identité binomiale de Newton...

Complexité en moyenne

Si un algorithme prend un temps $t(x)$ sur un exemplaire $x \in X$ et que l'exemplaire x se produit avec probabilité $p(x)$ alors la complexité en moyenne de l'algorithme sur les exemplaires X est $\sum_{x \in X} p(x)t(x)$.

Un peu de pratique

Exercice(s)

Exercice 7 et suivants de la feuille de TD6

Bonnes fêtes de fin d'année et bonnes révisions !