Licence d'informatique – deuxième année
Année 2019-2020
Support pour le cours de mathématiques discrètes

Sommaire

1 Démonstration par Récurrence (rappel)

Le raisonnement par récurrence est l'une des méthodes mathématiques de démonstration les plus utilisées. Particulièrement efficace (souvent beaucoup plus facile à appliquer que les autres méthodes pour un problème donné), cette méthode ne peut s'appliquer que sous certaines conditions :

- le résultat à démontrer doit être explicité (impossible d'utiliser cette méthode pour chercher en même temps à formuler et à démontrer un résultat) ;
- ce résultat doit porter sur des nombres entiers ou plus généralement sur des structures séquentielles ou récursives (suites, mots, arbres, graphes etc...).

1.1 Le principe du raisonnement par récurrence

C'est une méthode pour démontrer des propositions du type :

$$\forall n \in \mathbb{N}\ P(n)$$

ou plus généralement :

$$\forall\, n \geq n_0\, P(n)$$

où P est une propriété du nombre entier générique n (propriété relative à n, à une expression dans laquelle figure n, etc...).

Le principe de démonstration par récurrence est le suivant :

(a) On vérifie $P(0)$ (plus généralement $P(n_0)$)

(a) On suppose que $P(n)$ (l'hypothèse de récurrence) est vraie pour n n étant supérieur ou égal à n_0) et on montre que sous cette hypothèse, $P(n+1)$ est encore vérifiée.

Exemple Soit à montrer, pour tout $n \geq 1$:

$$P(n) :\ 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

(a) On vérifie $P(1)$: $1 = 1$

(b) On suppose que $n \geq 1$ et $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.
Alors on a :

$$1+2+\cdots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{(n+2)(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

et $P(n+1)$ est vérifiée.

(c) On peut alors conclure d'après le principe de récurrence que $P(n)$ est vraie $\forall n \geq 1$.

1.2 Variante de la démonstration par récurrence (exemples)

(a) On vérifie $P(n_0)$;

(b) On suppose que $n \geq n_0$ et que les propositions $P(n_0)$, $P(n_0+1)$,$\cdots P(n)$ sont toutes vraies ; on montre que, sous cette hypothèse, $P(n+1)$ est encore vraie.

Cette variante revient en fait à faire une démonstration par récurrence classique, avec comme hypothèse de récurrence le prédicat suivant, défini pour $n \geq n_0$:

$$Q(n) = P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(n).$$

En effet, on vérifie bien que :

(a) $Q(n_0)$ est vraie, puisque $P(n_0)$ l'est ;

(b) Si $Q(n)$ est vraie pour $n \geq n_0$, alors $Q(n+1)$ est encore vraie, puisque $Q(n+1)$ équivaut à $Q(n) \wedge P(n+1)$.

2 Induction structurale : rappels et compléments : les arbres

On peut généraliser le principe des preuves par récurrence à des ensembles autres que $\mathbb{N}$. Il suffit que ces ensembles soient inductifs.

2.1 Ensembles définis inductivement

Les ensembles définis inductivement sont des ensembles pour lesquels on a un moyen de construction (des éléments de base et des constructeurs) : Soit E un ensemble. On défini inductivement un sous-ensemble X de E lorsque l'on se donne des règles de construction des éléments de X, règles que l'on sépare en deux types de règles :
i) les règles de bases : qui indiquent les éléments qui sont dans X
ii) les règles inductives : qui donnent un moyen de construire les éléments de X à partir de ceux déjà construits.

Exemple On considère l'ensemble E des mots non vides constitués de 0 et de 1. $E = \{0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$.
On définit inductivement l'ensemble X_d par :
i) 1 est dans X_d

ii) si m appartient à X_d alors le mot $m0$ appartient à X_d
X_d est alors l'ensemble des mots commençant par 1 et suivi de 0 : $\{1, 10, 100, \ldots\}$.

Plus formellement : Soit E un ensemble, une définition inductive d'une partie X de E est la donnée :
i) d'une partie B de E
ii) d'un ensemble O_p d'opérations sur les éléments de E
X est alors le plus petit ensemble vérifiant :
i) base : tous les éléments de B appartiennent à X
ii) induction : pour toute opération f de O_p à n arguments et pour tout $x_1, \ldots, x_m \in X$:$f(x_1, \ldots, x_m) \in X$

2.2 Preuve par induction structurelle

Il s'agit d'une généralisation de la preuve par récurrence.
Soit X un ensemble défini inductivement à partir d'une base B et d'un ensemble d'opérateurs O_p. On veut démontrer qu'une propriété P est vraie pour tout élément de X, autrement dit :$\forall x \in X, P(x)$.

Si les deux conditions sont vérifiées :
i) base : $P(x)$ est vraie pour tout $x \in B$
ii) induction : pour tout f de O_p à n arguments et pour tout $x_1, \ldots, x_m \in X$ si $P(x_1), \ldots, P(x_k)$ sont vraies, alors $P(f(x_1, \ldots, x_k))$ est vraie.

alors P est vraie pour tout élément de X.

Exemple On considère D ensemble des mots sur l'alphabet $\{a, b\}$, mots construits avec le schéma suivant :
— le mot vide (noté ε) appartient à D
— Si $m \in D$ alors $amb \in D$ et $bma \in D$.
On veut montrer que tout mot de D possède autant de a que de b

On note $n_i(m)$ le nombre de lettres i du mot m.
Soit $P(m)$ la propriété $n_a(m) = n_b(m)$

Si $m = \varepsilon$ alors $n_a(m) = n_b(m) = 0$ donc $P(m)$ est vraie.
Supposons $M \in D$ et $P(m)$ vraie.
Alors $n_a(amb) = 1 + n_a(m) = 1 + n_b(m) = n_b(amb)$ car $n_a(m) = n_b(m)$ car $P(m)$ est vraie. Donc $P(amb)$ est vraie.
De même $n_a(bma) = 1 + n_a(m) = 1 + n_b(m) = n_b(bma)$ car $n_a(m) = n_b(m)$ car $P(m)$ est vraie. Donc $P(bma)$ est vraie.
On en déduit par induction que $P(m)$ est vraie pour tout $m \in D$.

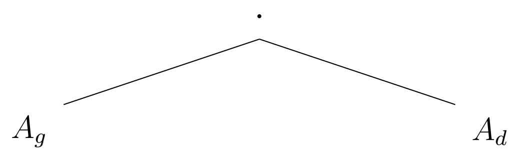
2.3 Arbres binaires

Un arbre binaire est un ensemble de *noeuds*, organisés de façon hiérarchique, à partir d'un noeud distingué, appelé *racine*. La structure d'arbre est sans doute la structure la plus importante en informatique ; c'est par exemple la structure d'organisation des fichiers sous UNIX et la structure des documents de format XML.

La structure d'arbre binaire est récursive et on peut la définir (inductivement) avec le **schéma d'induction** suivant :

(1) $\emptyset$ est un arbre

(2) si A_g et A_d sont deux arbres, alors :

A = 

est un arbre,

où $(.)$ désigne la racine, A_g s'appelle le sous-arbre gauche et A_d le sous-arbre droit.

2.3.1 Vocabulaire sur les arbres

— Les noeuds terminaux (qui n'ont pas de descendants) sont appelés **feuilles**.
— Les noeuds non-terminaux sont appelés **noeuds internes**.
— Un noeud Y, situé (immédiatement) sous un noeud X, est appelé le **descendant** (direct) de X. Inversement, X est appelé **l'ancêtre** (direct) de Y.
— Soit X un noeud intérieur et Y un descendant (direct ou indirect) de X. Notons $\mathcal{C} = (X, X_1, \ldots, X_k, Y)$ le **chemin allant de X à Y**. La longueur du chemin est $k + 1$. La **profondeur** d'un noeud X est la longueur du chemin de la racine jusqu'à X. En particulier, la profondeur de la racine est 0.
— La **hauteur** d'un noeud est la longueur du plus long chemin depuis ce noeud jusqu'à une feuille.
— La **hauteur** $h(A)$ d'un arbre A est la hauteur de la racine. Elle se définit inductivement de la manière suivante :

  (1) s'il se réduit à une racine alors $h(A) = 0$.

  (2) sinon il est de hauteur $1 + max(h(A_g), h(A_d))$.

— les noeuds de **niveau** k sont tous les noeuds de profondeur k.

2.3.2 Arbres binaires particuliers

1. un arbre **dégénéré** ou **filiforme** est un arbre de hauteur $n - 1$, où n est le nombre de noeuds.

2. un arbre **complet** est un arbre où tous les niveaux sont complètement remplis.

3. un arbre est **localement complet** lorsqu'il est non vide et que ses noeuds ont soit aucun fils soit deux fils.

4. un arbre binaire est **parfait** ou **presque complet** lorsque tous les niveaux sont entièrement remplis sauf éventuellement le dernier niveau, et dans ce cas, les feuilles du dernier niveau sont regroupées le plus à gauche possible.

5. un arbre binaire est **quasi parfait** lorsque tous les niveaux sont entièrement remplis sauf éventuellement le dernier niveau où aucune condition n'est imposée.

2.3.3 Démonstration par induction structurale sur un arbre binaire

Globalement le principe de démonstration par induction structurale pour une propriété P des arbres binaires est le suivant (quand l'arbre vide est la base) :

(1) On vérifie $P(\emptyset)$.

(2) On suppose que l'hypothèse d'induction P est vraie pour deux arbres binaires quelconques A_g et A_d et on montre qu'elle est alors nécessairement vraie pour l'arbre A ayant comme sous-arbres A_g et A_d.

Exemple de preuve par induction

Montrons que tous les arbres localement complets ont un nombre impair de noeuds. Notons $N(A)$ le nombre de noeuds d'un arbre A.

(1) la propriété est vraie pour $A = (.)$, car $N(A) = 1$.

(2) Soit A un arbre localement complet de sous arbres A_g et A_d. Par définition, A_g et A_d sont localement complets. Supposons qu'il existe p et $q \in \mathbb{N}$ tels que $N(A_g) = 2p + 1$ et $N(A_d) = 2q + 1$ (hypothèse d'induction).
$N(A) = 1 + N(A_g) + N(A_d) = 2(p + q + 1) + 1$, donc $N(A)$ est impair.

3 Ensembles et Opérations élémentaires sur les ensembles

3.1 Qu'est-ce qu'un ensemble ?

La théorie des ensembles a été fondée au XIX$^{\text{ème}}$ siècle notamment par des mathématiciens tels que Georg Cantor et Julius Dedekind. Qu'est-ce qu'un ensemble ? C'est une très bonne question, mais ce n'est pas facile d'y répondre rigoureusement. On souhaite regrouper des choses plus ou moins semblables dans un tout que l'on va nommer ensemble, ces choses deviennent alors les **éléments** de cet ensemble, on dit qu'un élément **appartient** à un ensemble. En général, cette notion intuitive est suffisante et nous manipulons tous les jours des ensembles : les élèves d'une classe, les livres d'une bibliothèque…

La manière la plus naturelle pour définir un ensemble est de donner la liste de ses éléments. Par exemple, l'ensemble des chiffres en base 10 est $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, l'ensemble des lettres de notre alphabet est

$\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$.

Cette définition permet un accès aux éléments, à partir des chiffres on peut écrire n'importe quel nombre en base 10.

On dit que l'ensemble est défini en **extension**.

Parfois ce n'est pas possible de donner une telle liste. On cherche alors à donner une **propriété** que va partager ces éléments. Par exemple, l'ensemble des objets contenus dans une pièce.

D'autre part, dans le cas où l'ensemble est infini, il n'est plus possible de donner la liste des éléments.

Exemple Notons $\mathcal{P}air(\mathbb{N})$ (respectivement $\mathcal{I}mpair(\mathbb{N})$), l'ensemble des entiers naturels pairs (respectivement impairs). On peut définir ces deux ensembles de la manière suivante :

$$\begin{array}{rcl} \mathcal{P}air(\mathbb{N}) & = & \{n \in \mathbb{N} \mid n \text{ est divisible par } 2\} \\ \mathcal{I}mpair(\mathbb{N}) & = & \{n \in \mathbb{N} \mid n \notin \mathcal{P}air(\mathbb{N})\}. \end{array}$$

On dit dans ce cas que l'ensemble est défini en **compréhension**.

Une définition naïve des ensembles entraîne rapidement des contradictions. Il existe des paradoxes célèbres à ce sujet qui divisèrent les mathématiciens sur la manière de définir proprement les ensembles :

— *Le barbier rasera tous les hommes qui ne se rasent pas eux-même.* (Bertrand Russel) Qui rasera le barbier ?

— *le plus petit nombre entier ne pouvant être exprimé en moins de quinze mots*

— *l'ensemble des ensembles qui ne se contiennent pas comme élément*
Variante : on écrit un livre contenant tous les livres d'une bibliothèque qui ne se citent pas. Ce livre ne peut appartenir à la bibliothèque !

3.2 Opérations sur les ensembles

Définition 3.1 Inclusion Soient $\mathcal{A}$ et $\mathcal{B}$ deux ensembles.
Nous dirons que $\mathcal{A}$ est inclus dans $\mathcal{B}$, noté $\mathcal{A} \subset \mathcal{B}$, lorsque pour tout $a \in \mathcal{A}$ nous

avons $a \in \mathcal{B}$.

Définition 3.2 Parties d'un ensemble Soit E un ensemble, nous noterons $\mathcal{P}(E)$ l'ensemble des parties (sous-ensembles) de E. Nous avons alors l'équivalence entre

- $\mathcal{A} \in \mathcal{P}(E)$.
- $\mathcal{A} \subset E$.

Remarque E et $\emptyset$, l'ensemble vide, sont toujours des éléments de $\mathcal{P}(E)$.

Définition 3.3 Égalité Soient A et B deux ensembles. Nous dirons que A et B sont égaux et nous écrirons $A = B$ lorsqu'ils ont exactement les mêmes éléments, autrement dit $B \subset A$ et $A \subset B$.

Notation 3.1 Dans toute la suite, nous utiliserons dans les énoncés mathématiques le symbole $\wedge$ pour désigner le **et** et $\vee$ pour désigner le **ou**. Ainsi "x appartient à A et à B" s'écrira $x \in A \wedge x \in B$. De même, "x appartient à A ou à B" s'écrira $x \in A \vee x \in B$.

Remarque **ou** désigne un **ou non exclusif**, c'est-à-dire que dans l'énoncé $x \in A \vee x \in B$, x peut appartenir à la fois à A et à B.

Définition 3.4 Intersection Soient A et B deux ensembles. L'intersection de A et B, notée $A \cap B$, est l'ensemble des éléments appartenant à A et à B :

$$\{x \mid x \in A \wedge x \in B\}$$

Définition 3.5 Réunion *ou* Union Soient A et B deux ensembles. L'union de A et B, noté $A \cup B$, est l'ensemble des éléments appartenant à au moins un des deux ensembles :

$$\{x \mid x \in A \vee x \in B\}$$

Nous avons toujours

$$A \cap B \subset A \cup B.$$

Définition 3.6 Complémentaire de A dans E Soient A et E deux ensembles tels que $A \subset E$, le complémentaire de A dans E, noté $\mathcal{C}_E^A$, est l'ensemble

$$\{x \in E \mid x \notin A\}$$

Lorsqu'il n'y a pas d'ambiguïté (qu'il n'est pas nécessaire de mentionner l'ensemble E), on peut écrire $\overline{A}$ ou $\mathcal{C}^A$ au lieu de $\mathcal{C}_E^A$.

Définition 3.7 Différence
Si A et B sont deux parties d'un ensemble E alors $A \setminus B$ est l'ensemble défini par

$$\{x \in A \mid x \notin B\}.$$

Définition 3.8 Différence symétrique Si A et B sont deux parties d'un ensemble E alors $A \Delta B$ est l'ensemble des éléments de E appartenant soit à A, soit à B, mais pas aux deux :

$$A \Delta B = A \setminus B \cup B \setminus A.$$

Définition 3.9 Produit cartésien Soient E et F deux ensembles, nous noterons $E \times F$ l'ensemble

$$\{(x, y) \mid x \in E \wedge y \in F\}$$

Définition 3.10 Partition Soient E un ensemble, $k \in \mathbb{N}^*$ et $F_1, \ldots, F_k$, k sous-ensembles de E. Nous dirons que $\mathcal{F} = \{F_1, \ldots, F_k\}$ forme une partition de E lorsque les deux conditions suivantes sont vérifiées :

i) $\mathcal{F}$ forme un recouvrement de E (leur réunion et égale à E) : pour tout $x \in E$, il existe $i \in \{1, \ldots k\}$ tel que $x \in F_i$.

ii) Les ensembles de $\mathcal{F}$ sont deux à deux disjoints :
pour tout $x \in E$, soient i et $j \in \{1, \ldots k\}$ tels que $x \in F_i$ et $x \in F_j$ alors $i = j$.

Remarque Lorsque E est infini, on peut étendre cette définition avec $\mathcal{F}$ non fini.
Exemples

1. $(\mathcal{P}air(\mathbb{N}), \mathcal{I}mpair(\mathbb{N}))$ forme une partition de $\mathbb{N}$.
2. Soit p un nombre premier. Notons $N(p)$ l'ensemble des entiers naturels dont p est le plus petit diviseur strictement supérieur à 1.
$(N(p))_{p \text{ premier}}$ forme une partition infinie de $\mathbb{N} \setminus \{0, 1\}$.

4 Fonctions, applications, injections et surjections

Définition 4.1 Fonction Une fonction est une correspondance d'un ensemble A vers un ensemble B, qui à tout élément de A associe au plus un élément de B.

Exemples

$$\begin{array}{rccc} f_1 : & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & sin\, x \end{array} \qquad \begin{array}{rccc} f_2 : & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & \frac{1}{x} \end{array}$$

Définition 4.2 Application Une application est une opération qui consiste à faire correspondre à tout élément d'un ensemble A un élément d'un ensemble B et un seul.

Définition 4.3 Image Soient A et B deux ensembles et soit f une application de A vers B. Soit $a \in A$, on appelle image de a par f l'élément $f(a)$ de B.

Définition 4.4 Antécédent Soient A et B deux ensembles et soit f une application de A vers B. Soit $b \in B$, on appelle antécédent de b par f un élément a de A vérifiant $f(a) = b$.

Reprenons les deux fonctions ci-dessus, f_1 est une application, mais f_2 n'en est pas une car 0 n'a pas d'image. On obtient toujours une application à partir d'une fonction en prenant comme ensemble de départ le domaine de définition de la fonction, ainsi pour f_2 nous prendrons l'ensemble $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Remarque Un élément a de A a toujours une image dans B, mais un élément b de B n'a pas toujours un antécédent, il peut également avoir plusieurs antécédents.

Définition 4.5 Soit b un élément de B, on note $f^{-1}(\{b\})$ l'ensemble des éléments de A qui ont b comme image :

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}.$$

Définition 4.6 Image d'un ensemble Soit $C \subset A$, $f(C)$ est l'ensemble des images des éléments de C :

$$f(C) = \{b \in B \mid \exists c \in C \ f(c) = b\}.$$

Définition 4.7 *Soit $D \subset B$,*

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

Définition 4.8 Injectivité f est injective si et seulement si tout élément b de B a **au plus** un antécédent.

Définition 4.9 Surjectivité f est surjective si et seulement si tout élément b de B a **au moins** un antécédent.

Définition 4.10 Bijectivité f est bijective si et seulement si elle est à la fois injective et surjective.

Remarque f^{-1} est une fonction lorsque f est injective. Si f est bijective alors c'est une application (qui est bijective).

Propriété 4.1 f est injective lorsque, pour tous a_1 et a_2 de A, si $f(a_1) = f(a_2)$ alors $a_1 = a_2$.

Définition 4.11 Composition d'applications Soient A, B et C trois ensembles, f une application de A vers B et g une application de B vers C.
La composition de f et g, notée $g \circ f$ est l'application de A vers C définie par

$$g \circ f(a) = g(f(a)).$$

Propriétés 4.1

- Si f et g sont surjectives alors $g \circ f$ est surjective.
- Si f et g sont injectives alors $g \circ f$ est injective.
- Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

5 Relations

5.1 Définition générale

Définition 5.1 Soit E un ensemble et $k \in N^*$. Une relation R d'arité k sur E est un sous-ensemble de E^k (produit cartésien de k fois l'ensemble E). On peut également voir R comme une application de E^k vers $\{0,1\}$. Les deux assertions suivantes sont alors équivalentes :

1. $(e_1, \ldots, e_k) \in R$.
2. $R(e_1, \ldots, e_k) = 1$.

E est souvent appelé le domaine ou l'univers.

Remarque Comme une relation est un sous-ensemble, nous avons vu qu'elle pouvait être définie en extension (on donne la liste des k-uplets) ou en compréhension (les k-uplets vérifiant une propriété, par exemple une équation mathématique).

Exemples Soient $+$ et $\times$ les relations ternaires (d'arité 3) sur $\mathbb{Z}$ définies par

$$\begin{array}{rcl} + & = & \{(x,y,z) \in \mathbb{Z}^3 \mid x + y = z\} \\ \times & = & \{(x,y,z) \in \mathbb{Z}^3 \mid x * y = z\} \end{array}$$

Nous avons, par exemple, $(2,3,5) \in +$ et $(4,5,20) \in \times$.
On montre $+ \cap \times = \{(0,0,0),(2,2,4)\}$.

Définition 5.2 Relation unaire (arité 1)
Une relation unaire U sur un ensemble E est un sous-ensemble de E. Par exemple, $\mathcal{P}air(\mathbb{N})$ et $\mathcal{I}mpair(\mathbb{N})$ sont deux relations unaires sur $\mathbb{N}$.

Définition 5.3 Relation binaire (arité 2)
Une relation binaire $\Re$ sur un ensemble E est un sous-ensemble de $E \times E$.
Pour les relations binaires, on utilise très souvent la notation $e \,\Re\, f$ au lieu de $\Re(e,f)$.

Soit (e,f) un couple de E (une paire ordonnée), nous écrirons indifféremment

(e,f) appartient à la relation $\Re$	(e,f) n'appartient pas à la relation $\Re$
$(e,f) \in \Re$	$(e,f) \in \neg\Re$
$\Re(e,f)$	$\neg\, \Re(e,f)$
$\Re(e,f) = 1$	$\mathbb{R}(e,f) = 0$
$e\, \Re f$	$\neg\, e\Re f$

5.2 Propriétés des relations binaires

On retrouve très souvent des relations binaires lorsque l'on étudie des ensembles en mathématiques ou en informatique. Parmi les propriétés que peuvent vérifier ces relations on distingue notamment deux actions : la relation peut servir à regrouper les éléments (relation d'équivalence) ou au contraire à les trier (relation d'ordre).

Exemple Une relation se définit souvent de manière très naturelle. Prenons un exemple où l'ensemble est l'ensemble des étudiants de L2 Info et où la relation fait intervenir le choix des options. On définit une relation entre les étudiants de L2 par :

etudiant1 $\Re$ *etudiant2 lorsqu'ils ont au moins une option commune.*

Définition 5.4 Réflexivité
Une relation sur un ensemble E est dite **réflexive** lorsque

$$\forall e \in E \ \ e \Re e.$$

Définition 5.5 Irréflexivité
Une relation sur un ensemble E est dite **irréflexive** lorsque

$$\forall e \in E \ \ \neg(e \Re e).$$

Définition 5.6 Symétrie
Une relation sur un ensemble E est dite symétrique lorsque

$$\forall e \in E \, \forall f \in E \; e \Re f \implies f \Re e.$$

Définition 5.7 Antisymétrie
Une relation sur un ensemble E est dite antisymétrique lorsque

$$\forall e \in E \, \forall f \in E \; (e \Re f \wedge f \Re e) \implies e = f.$$

Définition 5.8 Transitivité
Une relation sur un ensemble E est dite transitive lorsque

$$\forall e \in E \, \forall f \in E \, \forall g \in E \; (e \Re f \wedge f \Re g) \implies e \Re g.$$

5.3 Relations d'équivalences

Définition 5.9 Relation d'équivalence
Une relation sur un ensemble E est une relation d'équivalence lorsqu'elle vérifie les trois propriétés suivantes

- réflexivité.
- symétrie.
- transitivité.

Définition 5.10 Classe d'équivalence
Soit $\Re$ une relation d'équivalence sur un ensemble E.
Pour tout $a \in E$, on définit sa classe d'équivalence par

$$[a] = \{x \in E \mid a \Re x\}$$

Propriété 5.1 *L'ensemble des classes d'équivalence forme une partition de E, pour cela on montre les points suivants :*

1. *pour tout* $a \in E, a \in [a]$
2. $[a] = [b]$ *si et seulement si* $a \Re b$
3. *si* $[a] \neq [b]$ *alors* $[a]$ *et* $[b]$ *sont disjointes*

Exemple La relation $\Re$ sur $\mathbb{Z}^{*^2} \times \mathbb{Z}^{*^2}$ définie par

$$(a, b) \Re (c, d) \text{ si et seulement si } ad = bc$$

est une relation d'équivalence.

5.4 Relations d'ordre

Définition 5.11 Ordre large
Une relation $\preceq$ sur un ensemble E est une relation d'ordre partiel large lorsqu'elle vérifie les trois propriétés suivantes
— réflexivité
— antisymétrie
— transitivité.

Définition 5.12 Ordre strict
Une relation $\prec$ sur un ensemble E est une relation d'ordre partiel strict lorsqu'elle vérifie les propriétés suivantes
— irréflexivité
— transitivité.

Remarque : si une relation est irréfléxive et transitive elle est forcément antisymétrique.

Exemple On définit un ordre partiel strict $\prec$ à partir d'un arbre généalogique. *Personne1* $\prec$ *Personne2* lorsque *Personne1* est un ancêtre de *Personne2*.

Définition 5.13 Ensemble partiellement ordonné
E est partiellement ordonné lorsqu'il est muni d'un ordre partiel $\preceq$.

Définition 5.14 Ensemble totalement ordonné
Soit $\preceq$ un ordre partiel sur E. E est totalement ordonné par $\preceq$ lorsque pour tout couple $(a, b) \in E \times E$,

$$a \preceq b \vee b \preceq a$$

Définition 5.15 Ordre total strict
Soit $\prec$ un ordre partiel strict sur E. E est totalement ordonné par $\prec$ lorsque pour tout couple $(a, b) \in E \times E$,

$$a \prec b \vee b \prec a \vee a = b.$$

Définition 5.16 Ordre lexicographique Soit $\mathcal{A}$ un alphabet (ensemble fini de symboles). Supposons que $\mathcal{A}$ soit muni d'une relation d'ordre total strict $\prec$. Soit $\mathcal{A}^*$ l'ensemble des mots que l'on peut écrire avec des lettres de $\mathcal{A}$, autrement dit

$$\mathcal{A}^* = \bigcup_{n \in \mathbb{N}} \mathcal{A}^n,$$

où $\mathcal{A}^n$ est l'ensemble des mots sur $\mathcal{A}$ de longueur n.

Le mot vide (de longueur 0) est souvent noté ε.
Soient m_1 et m_2 deux mots quelconque de $\mathcal{A}^*$, pour tout $k \in \mathbb{N}$, on notera $m_1[i]$ et $m_2[i]$ la $i^{\text{ème}}$ lettre de m_1 et m_2.
L'ordre lexicographique $\prec^*$ sur $\mathcal{A}^*$ est définie par

$$m_1 \prec^* m_2 \text{ lorsque } \exists k \in \mathbb{N} \left(\forall h < k \; m_1[h] = m_2[h]\right) \wedge (m_1[k] \prec m_2[k])$$

6 Combinatoire.

6.1 Principe des choix successifs

Quand on fait n choix successifs, s'il y a p_1 possibilités pour le premier choix, p_2 pour le deuxième, ..., p_n choix pour le dernier, alors il y a en tout $p_1 \cdot p_2 \cdots p_n$ façons d'enchaîner ces n choix.

6.2 Cardinal d'un produit cartésien

Proposition 6.1 *Soient A et B deux ensembles finis. Le cardinal de $A \times B$ est égal au produit des cardinaux de A et de B,*

$$card(A \times B) = card(A) \times card(B).$$

Preuve Il y a $card(A)$ possibilités de choix pour les éléments de A, et pour chaque choix d'un élément $a \in A$, il y a $card(B)$ possibilités de choix pour les éléments de B ; en tout $card(A) \times card(B)$ choix possibles pour les couples (a, b) éléments de $A \times B$.

Ce résultat se généralise pour $E_1 \times E_2 \times \ldots \times E_n$, un produit de n ensembles finis. La démonstration se fait facilement par récurrence, on se ramène à $n = 2$ en écrivant

$$E_1 \times E_2 \times \ldots \times E_n = E_1 \times (E_2 \times \ldots E_n).$$

Il vient

$$card(E_1 \times E_2 \times \ldots \times E_n) = card(E_1) \times card(E_2) \ldots \times card(E_n).$$

6.3 Nombre d'applications de A vers B.

Proposition 6.2 *Soient A et B deux ensembles, et $\mathcal{F}(A,B)$ l'ensemble des applications de A vers B. Si A et B sont finis, avec $card(A) = p$ et $card(B) = n$, il vient*

$$card(\mathcal{F}(A,B)) = n^p.$$

Preuve On peut toujours numéroter les éléments d'un ensemble fini. Soit $A = \{a_1, a_2, \ldots, a_p\}$. Une application f de A vers B est complètement déterminée par le p-uplet $(f(a_1), f(a_2), \ldots, f(a_p))$. Il y a n choix possibles pour chaque élément $f(a_i)$ du p-uplet, et donc en tout n^p choix possibles.

Corollaire 6.1 *Soient A un ensemble et $\mathcal{P}(A)$ l'ensemble des parties de A. Si A est de cardinal p, alors $\mathcal{P}(A)$ est de cardinal 2^p.*

Preuve À toute partie C de A, on associe la fonction caractéristique de C, notée $\mathbf{1}_C$, définie sur A et à valeurs dans l'ensemble $\{0,1\}$. Cette fonction vérifie

$$\mathbf{1}_C(x) = 1 \quad \text{pour } x \in C, \qquad \mathbf{1}_C(x) = 0 \quad \text{pour } x \notin C$$

L'application $\Psi : \mathcal{P}(A) \to \mathcal{F}(A, \{0,1\})$ définie par $\Psi(C) = \mathbf{1}_C$ est une bijection.

Remarque Les fonctions caractéristiques vérifient d'autres propriétés importantes.

6.4 Arrangements - Nombre d'injections de A vers B.

Soient A et B deux ensembles finis, avec $card(A) = p$ et $card(B) = n$. Une injection de A dans B est complètement déterminée par la donnée d'une suite ordonnée de p éléments dans l'ensemble B de cardinal n. Une telle suite ordonnée est appelée aussi un arrangement de p éléments pris parmi un ensemble de n éléments. C'est pourquoi le nombre de telles suites (qui est donc aussi égal au nombre d'injections d'un ensemble de cardinal p dans un ensemble de cardinal n) est désigné par A_n^p.

Proposition 6.3 *Soient A et B deux ensembles, et $\mathcal{I}(A,B)$ l'ensemble des injections de A vers B. Si A et B sont finis, avec $card(A) = p$ et $card(B) = n$, alors le cardinal de $\mathcal{I}(A,B)$ (nombre d'arrangements de p éléments pris parmi n) est égal à*

$$\begin{aligned} A_n^p &= n(n-1)(n-2)\ldots(n-p+1) = \frac{n!}{(n-p)!}, && \textit{pour } n \geq p \\ &= 0 && \textit{pour } n < p. \end{aligned}$$

Preuve Soit $A = \{a_1, a_2, \ldots, a_p\}$. Une injection f de A vers B est complètement déterminée par le p-uplet $(f(a_1), f(a_2), \ldots, f(a_p))$ d'éléments de B tous distincts. Il y a n possibilités pour le premier élément $f(a_1)$ du p-uplet, puis $n-1$ possibilités pour le deuxième élément $f(a_2)$ du p-uplet, et en général $n-i+1$ possibilités pour le i-ième élément $f(a_i)$ du p-uplet.

6.5 Permutations

Soit A un ensemble, et $\Sigma(A)$ l'ensemble des bijections de A dans lui-même. Supposons que A soit fini, posons $n = card(A)$. Le cardinal de $\Sigma(A)$ est égal à $n!$. Une bijection de A dans lui-même est appelée aussi une permutation de A.

Permutations et mots Soit $a_1 \ldots a_n$ un mot formé de symboles tous distincts. Chaque permutation σ sur $A = \{a_1, \ldots, a_n\}$ correspond à l'unique mot $\sigma(a_1) \ldots \sigma(a_n)$. On peut donc former $n!$ mots de longueur n contenant toutes les lettres de A.

6.6 Combinaisons et coefficient binomial

On appelle combinaison de p éléments d'un ensemble fini A toute partie de A possédant p éléments.

Proposition 6.4 *Soit A un ensemble de cardinal n, et C_n^p l'ensemble des combinaisons de p éléments de A. Alors le cardinal de C_n^p est égal à*

$$\begin{aligned}\binom{n}{p} &= \frac{n\,(n-1)\,(n-2)\,\ldots(n-p+1)}{p!} = \frac{n!}{(n-p)!\,p!},\ \textit{pour}\ n \geq p\\ &= 0\ \textit{pour}\ n < p.\end{aligned}$$

Remarque le nombre $\binom{n}{p}$ est appelé coefficient du binôme et s'écrit également C_n^p.

Preuve Il y a $p!$ manières d'ordonner une partie de p éléments en une suite ordonnée de p éléments, et chaque suite ordonnée de p éléments définit de manière unique une injection d'un ensemble de cardinal p dans un ensemble de cardinal n. On a donc $p! \times C_n^p = A_n^p$.

Propriétés 6.1 Le coefficient binomial vérifie les propriétés suivantes :

$$\begin{aligned}\binom{n}{p-1} + \binom{n}{p} &= \binom{n+1}{p} && \text{Triangle de Pascal}\\ (x+y)^n &= \sum_{k=0}^{n} \binom{n}{k}\, x^k\, y^{n-k} && \text{Binôme de Newton}\end{aligned}$$

6.7 Coefficient multinomial

On s'intéresse au nombre de partages d'un ensemble A en m parties de cardinal fixé $a_1, \ldots a_m$.

Proposition 6.5 *Soit* $(a_1, \ldots, a_m)$ *un* m*-uplets d'entiers naturels vérifiant* $a_1 + \ldots + a_m = n$*. Soit* A *un ensemble de cardinal* n*, et* $\mathcal{C}(n, a_1, \ldots, a_m)$ *l'ensemble des partages de* A *en* m *parties de cardinal* $a_1, \ldots, a_m$*. Alors le cardinal de* $\mathcal{C}(a_1, \ldots, a_m)$ *est égal à*

$$\frac{n!}{a_1! \ldots a_m!}.$$

Remarque Ce nombre est appelé coefficient multinomial est désigné par le symbole

$$\binom{n}{a_1, \ldots, a_m} = C_n^{a_1, \ldots, a_m}.$$

Le nom provient du développement du multinôme $(x_1 + \ldots + x_m)^n$ en fonction des monômes $x_1^{a_1} \ldots x_m^{a_m}$ où les exposants $a_1, \ldots, a_m$ vérifient $a_1 + \ldots + a_m = n$. On a

$$(x_1 + \ldots + x_m)^n = \sum_{\substack{(a_1, \ldots, a_m) \\ a_1 + \ldots + a_m = n}} \binom{n}{a_1, \ldots, a_m} x_1^{a_1} \ldots x_m^{a_m}.$$

6.8 Principe des tiroirs

Soient n et m sont deux entiers tels que $n < m$. On veut placer m objets dans n tiroirs. Alors au moins un tiroir contiendra 2 objets ou plus.

6.9 Principe d'inclusion-exclusion

Soient deux parties A et B d'un ensemble fini E. La relation $\overline{A \cup B} = \overline{A} \cap \overline{B}$ montre, en utilisant les fonctions caractéristiques, que $\mathbf{1} - \mathbf{1}_{A \cup B} = (\mathbf{1} - \mathbf{1}_A)(\mathbf{1} - \mathbf{1}_B)$, ce qui donne en développant $\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \mathbf{1}_B$.

En sommant sur tous les éléments x de E, on obtient

$$card(A \cup B) = card(A) + card(B) - card(A \cap B).$$

Plus généralement, lorsque l'on a m parties $A_1, A_2, \ldots A_m$ de E, on a

$$\overline{A_1 \cup A_2 \cup \ldots \cup A_m} = \overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_m,$$

ce qui montre que

$$\mathbf{1} - \mathbf{1}_{A_1 \cup A_2 \cup \ldots \cup A_m} = (\mathbf{1} - \mathbf{1}_{A_1})(\mathbf{1} - \mathbf{1}_{A_2}) \ldots (\mathbf{1} - \mathbf{1}_{A_m}).$$

Finalement,

$$
\begin{aligned}
&card(A_1 \cup A_2 \cup \ldots \cup A_m) = \sum_{i=1}^{m} card(A_i) - \sum_{1 \leq i < j \leq m} card(A_i \cap A_j) \\
&+ \sum_{1 \leq i < j < k \leq m} card(A_i \cap A_j \cap A_k) + \ldots \\
&+(-1)^{l-1} \sum_{1 \leq i_1 < i_2 < i_3 < \ldots < i_l \leq m} card(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_l}) + \ldots \\
&+(-1)^{m-1} card(A_1 \cap A_2 \cap \ldots \cap A_m).
\end{aligned}
$$

Cette formule permet de calculer le cardinal de la réunion de m parties lorsqu'on connaît les cardinaux de toutes les intersections possibles. Remarquons qu'il existe exactement $\binom{m}{l}$ suites $(i_1, i_2, \ldots, i_l)$ qui satisfont $1 \leq i_1 < i_2 < i_3 < \ldots < i_l \leq m$, de telle sorte que le $l^{\text{ième}}$ terme est une somme portant elle-même sur $\binom{m}{l}$ termes.

7 Probabilités discrètes

7.1 Introduction

La théorie des probabilités est un outil fondamental dans beaucoup de domaines notamment en informatique. Sa première application est l'analyse en moyenne d'algorithmes. La combinatoire permet de dénombrer les éléments d'un ensemble, de compter le nombre d'algorithmes sur une donnée ; mais lorsque l'ensemble ou les données varient, le nombre d'opérations ou de données se met à varier aussi, et les probabilités entrent en jeu pour étudier les valeurs moyennes, l'écart par rapport à ces valeurs moyennes... Les probabilités sont aussi très utiles dans d'autres domaines de l'informatique comme par exemple :

— les algorithmes probabilistes : un algorithme probabiliste effectue des tirages aléatoires lors de son exécution. Il peut donc donner des résultats différents si on l'exécute plusieurs fois avec la même instance. Il peut s'avérer plus efficace qu'un algorithme déterministe (qui lui donne toujours le même résulat pour une instance fixée).

— la modélisation aléatoire : les probabilités interviennent lorsque l'on souhaite modéliser des phénomènes physiques, biologiques ou sociaux.

— la théorie des files d'attente : par exemple, étude du temps d'attente pour l'accès à certains points névralgiques d'un réseau de télécommunications.

— le traitement du signal

7.2 Évènements, espace de probabilités

Espaces de probabilités

Définition 7.1 Expérience aléatoire Une expérience aléatoire est une expérience dont on ne connait pas le résultat à l'avance

Exemples lancer deux dés, tirer 5 cartes dans un jeu de 32cartes...

Définition 7.2 Espace de probabilité On appelle espace de probabilité ou univers des possibles l'ensemble des résultats possibles d'une expérience aléatoire

Exemple : pour 2 jets successifs d'une pièce de monnaie, l'espace de probabilité est $\{FF, FP, PF, PP\}$

Remarque Nous travaillerons uniquement sur des espaces de probabilité finis ou dénombrables.

Évènement

Soit E un espace de probabilité

Définition 7.3 Toute partie de E est appelé évènement

Remarque : on peut écrire événement ou évènement, la première écriture étant ancienne.

Définition 7.4 évènement élémentaire Un évènement qui contient un unique élément de E est un évènement élémentaire.

Définition 7.5 évènement certain, évènement impossible L'ensemble E tout entier est l'évènement certain, l'ensemble vide est l'évènement impossible.

Définition 7.6 évènement contraire L'évènement contraire d'un évènement A que l'on note $\overline{A}$ est l'évènement constitué par le complémentaire de A dans E.

Définition 7.7 évènements incompatibles Deux évènements sont incompatibles s'ils ne peuvent être réalisés simultanément. On a alors $A \cap B = \varnothing$.

Distribution de probabilités

Définition 7.8 Une distribution de probabilité sur un ensemble $E = \{e_1, e_2, ..., e_n\}$ est une fonction P de E dans $\mathbb{R}$ telle que, pour tout $k = \{1, \ldots, n\}$, on a

— $0 \leq p(e_k) \leq 1$.

— $\sum_{k=1}^{n} P(e_k) = 1$.

Définition 7.9 probabilité Etant donnée une distribution de probabilité P sur E on appelle probabilité la fonction P de $\mathcal{P}(E)$ dans $\mathbb{R}$ définie par $P(A) = \sum_{e_i \in A} P(e_i)$
Pour tout évènement $A \subseteq E$, la probabilité de A est P(A).

Exemple

Dans l'expérience où l'on jette un dé à 6 faces, l'ensemble Ω des résultats possibles est l'ensemble $\Omega = \{1, 2, 3, 4, 5, 6\}$ et l'ensemble des événements possibles est l'ensemble $\mathcal{P}(\Omega)$ des parties de Ω. Comme chacune des faces a autant de chances d'être tirée, on attribue à chaque élément ω de Ω la probabilité $p(\omega) = 1/6$. L'événement « le chiffre tiré est pair »est $A = \{2, 4, 6\}$ qu'on munit de la probabilité

$$P(A) = \sum_{\omega \in A} P(w) = 1/6 + 1/6 + 1/6 = 1/2.$$

Définition 7.10 Espace probabilisé On appelle espace probabilisé un espace muni d'une probabilité.

Proposition 7.1 *Une probabilité P sur Ω possède les propriétés suivantes :*

1. $P(\Omega) = 1$.
2. *Pour tout couple d'événements (A, B) vérifiant $A \cap B = \emptyset$, on a :* $P(A \cup B) = P(A) + P(B)$.
3. *Pour tout couple d'événements (A, B), on a :* $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
4. *Pour tout événement A, si on désigne par $\overline{A}$ son complémentaire, on a :* $P(\overline{A}) = 1 - P(A)$.

Distribution uniforme

Définition 7.11 On appelle distribution uniforme, la distribution qui assigne à tout évènement élémentaire la même valeur.
On a alors évidemment,

$$P(A) = \frac{cardA}{cardE}$$

Exemple : pour le lancer de dé, si le dé est non pipé alors la distribution est uniforme.

7.3 Suites d'expériences indépendantes – Probabilité produit

Soient $(\Omega_1, P_1), (\Omega_2, P_2), \dots (\Omega_m, P_m)$ m espaces probabilisés. On peut munir l'espace produit $\Omega = \Omega_1 \times \Omega_2 \times \dots \times \Omega_m$ de la probabilité P définie par

$$P(\omega) = P_1(\omega_1)\, P_2(\omega_2) \dots P_m(\omega_m) \text{ pour } \omega = (\omega_1, \omega_2, \dots \omega_m)$$

Définition 7.12 Probabilité produit La probabilité P est appelée la probabilité produit. Elle vérifie en particulier pour tout événement $A_i \subset \Omega_i$

$$P(A_1 \times A_2 \times \dots \times A_m) = P_1(A_1)\, P_2(A_2)\, \dots P_m(A_m)$$

L'espace probabilisé (Ω, p) ainsi défini correspond alors à l'expérience totale formée par la suite des expériences associées aux espaces probabilisés (Ω_i, p_i), lorsque ces expériences sont indépendantes, i.e., lorsque le résultat d'une expérience ne dépend pas du résultat des autres expériences.

7.4 Probabilités conditionnelles, évènements indépendants.

Définition 7.13 probabilité conditionnelle Soit (Ω, p) un espace probabilisé et un événement fixé A de probabilité $P(A)$ non nulle. La probabilité conditionnelle en A, ou encore probabilité sachant que A est réalisé est définie par l'application $P_A : \Omega \to [0,1]$

$$P_A(B) = \frac{P(A \cap B)}{P(A)}, \text{ noté aussi } P(B|A),$$

Celle-ci définit une probabilité sur Ω associée à la suite

$$\begin{array}{rcl} q_\omega & = & \frac{P(\omega)}{P(A)} \text{ pour } \omega \in A \\ & = & 0 \text{ pour } \omega \notin A. \end{array}$$

L'espace $(A, P(.|A))$ est alors un espace probabilisé.

Probabilités composées

Par définition des probabilités conditionnelles,

$$\text{si } P(A) \neq 0 \qquad P(A \cap B) = P(A)\, P(B|A),$$

$$\text{si } P(B) \neq 0 \qquad P(A \cap B) = P(B)\, P(A|B).$$

Plus généralement (preuve par récurrence sur m),

$$\begin{array}{rcl} P(A_1 \ldots \cap A_m) & = & P(A_1 \cap \ldots \cap A_{m-1})\, P(A_m | A_1 \cap \ldots \cap A_{m-1}) \\ & = & P(A_1)\, P(A_2|A_1)\, P(A_3|A_1 \cap A_2)\, \ldots P(A_m|A_1 \cap \ldots \cap A_{m-1}). \end{array}$$

Événements indépendants

Définition 7.14 Deux événements A et B d'un espace probabilisé (Ω, p) sont indépendants lorsque

$$P(A \cap B) = P(A)\, P(B).$$

Remarque Il est équivalent de dire $P(B|A) = P(B)$ ou $P(A|B) = P(A)$. Dire que deux événements sont indépendants signifie que la réalisation d'un des deux événements n'influe pas sur la réalisation de l'autre.

On emploie le même mot *indépendance* pour qualifier des expériences (et donc des espaces probabilisés) différents et des événements (qui appartiennent au même espace probabilisé). On peut construire un cadre commun où regrouper ces deux notions en une seule. C'est pourquoi le même mot est employé.

On dit que deux événements A et B sont incompatibles si $A \cap B = \emptyset$. Il ne faut pas confondre les deux notions d'incompatibilité et d'indépendance. Au contraire, l'incompatibilité représente une forme de dépendance.

(i) Soient A et B sont des événements de probabilités non nulles, i.e., $P(A) \neq 0, P(B) \neq 0$. S'ils sont incompatibles, ils sont dépendants. La réciproque est fausse.

(ii) Soient A et B sont des événements vérifiant $A \subset B$, et $p(B) \neq 1$. Alors A et B sont dépendants.

Le phénomène d'indépendance s'applique donc généralement à des événements A et B en position générale (i.e., non disjoints et non inclus l'un dans l'autre). Par exemple, si Ω représente l'ensemble d'un jeu de 52 cartes, les événements $A = \ll$ on tire un roi $\gg$ et $B = \ll$ on tire une carte rouge $\gg$ sont indépendants. Par contre, les événements $C = \ll$ on tire le roi de coeur $\gg$ et B ne sont pas indépendants.

Événements indépendants. Généralisation

Définition 7.15 Soient m événements $A_1, A_2, \dots A_m$ d'un même espace probabilisé (Ω, p). Ils sont dits indépendants (dans leur ensemble) si et seulement si, pour toute partie $J \subset \{1, 2, \dots m\}$,

$$P(\bigcap_{j \in J} A_j) = \prod_{j \in J} P(A_j).$$

Remarque Pour $m = 3$, trois événements A, B, C indépendants dans leur ensemble sont nécessairement indépendants deux à deux. La réciproque est fausse.

Théorème de Bayes (probabilité des hypothèses)

On dispose d'une famille finie de parties B_i $(1 \leq i \leq m)$ qui forment une partition de Ω et dont les probabilités $P(B_i)$ sont non nulles. Par ailleurs, on considère un événement A, dont on veut calculer la probabilité. Souvent, on ne dispose que des probabilités $P(B_i)$ et des probabilités conditionnelles $P(A|B_i)$ de l'événement A sachant que B_i est réalisée. On a alors

$$P(A) = \sum_{i=1}^{m} P(A \cap B_i) = \sum_{i=1}^{m} P(A|B_i)\, p(B_i),$$

car les parties $A \cap B_i$ forment une partition de A. On peut alors calculer la probabilité $P(B_i|A)$,

$$P(B_i|A) = \frac{P(B_i \cap A)}{P(A)} = \frac{P(A|B_i)\, P(B_i)}{\sum_{i=1}^{m} P(A|B_i)\, P(B_i)}.$$

Cette relation permet de renverser les rôles : dans le membre de droite, ce sont les B_i qui jouent le rôle de différentes hypothèses ; dans le membre de gauche, c'est A qui a le statut d'hypothèse.

7.5 Variables aléatoires

Généralités

Une même expérience aléatoire , lorsqu'on la répète, fournit des résultats différents. Le caractère aléatoire de ces résultats sera traduit par la notion de variable aléatoire.

Définition 7.16 Variable aléatoire Soit (Ω, A, p) un espace probabilisé. On appelle variable aléatoire sur Ω toute application de Ω dans **R** telle que si I est un intervalle de $\mathbb{R}$, alors $X^{-1}(I) \in A$.

L'ensemble des valeurs de la variable aléatoire X est donc égal à $X(\Omega)$, il est fini ou dénombrable et on désigne par x_i ses éléments, $X(\Omega) = \{x_1, x_2, \ldots, x_i, \ldots\}$.

On appelle loi de probabilité de la variable aléatoire X l'application P_X définie sur l'ensemble des parties B de $X(\Omega)$ par

$$P_X(B) = P(X^{-1}(B)) = P(\{\omega \in \Omega \mid X(\omega) \in B\}).$$

L'application P_X est une probabilité sur $X(\Omega)$ complètement déterminée par les

$$p_i = P(\{\omega \in \Omega \mid X(\omega) = x_i\}) = P(X^{-1}(\{x_i\})) = P(X = x_i)$$

La donnée des p_i détermine donc la loi de la variable aléatoire X.

Exemple On jette une paire de dés non pipés.
On obtient alors pour univers des possibles l'ensemble S équiprobable : $S = \{(1,1)(1,2)\ldots(6,6)\}$.
On suppose qu'à chaque couple (a,b) on fasse correspondre X(a,b)= max(a,b).
Alors X est une variable aléatoire sur S ayant pour espace image $X(S) = \{1,2,3,4,5,6\}$
Alors $f(1) = P(X = 1) = P(1,1)) = \frac{1}{36}$
$f(2) = P(X = 2) = P(\{(1,2)(2,1)(2,2)\}) = \frac{3}{36}$
$f(3) = P(X = 3) = P(\{(1,3)(3,1)(2,3)(3,2)(3,3)\}) = \frac{5}{36}$
$f(4) = P(X = 4) = P(\{(1,4)(4,1)(2,4)(4,2)(3,4)(4,3)(4,4)\}) = \frac{7}{36}$
$f(5) = P(X = 4) = \frac{9}{36}$
$f(6) = P(X = 4) = \frac{11}{36}$

Si on considère la fonction $Y(a,b) = a + b$ on obtient une autre variable aléatoire sur S ayant pour espace image $Y(S) = \{2,3,4,5,6,7,8,9,10,11,12\}$ et, par exemple, $g(4) = P(Y = 4) = \frac{3}{36}$.

L'histogramme de la v.a. (variable aléatoire) X est alors la courbe (discrète) lieu des points (x_i, p_i).

Fonction de répartition d'une variable aléatoire

On appelle fonction de répartition de la variable aléatoire X la fonction F :$\mathbb{R} \to [0, 1]$ définie par $F(x) = P(X \leq x)$

La fonction F est alors une fonction croissante, qui vérifie
— $0 \leq F(x) \leq 1$
— $\lim_{x\to-\infty} F(x) = 0$,
— $\lim_{x\to+\infty} F(x) = 1$.

En particulier, pour tout entier x, on désigne par $I(x)$ les indices i pour lesquels $x_i \leq x$, alors

$$F(x) = \sum_{i\in I(x)} p_i,$$

et la fonction F est donc une fonction en escalier.

Espérance et variance d'une variable aléatoire

Soit $(x_k)_{k\in N}$ l'ensemble des valeurs prises par la v.a. X.

Définition 7.17 Espérance On désigne par $E(X)$ la somme de la série, si elle existe,

$$E(X) = \sum_{k\in N} x_k \; P(X = x_k).$$

Dans tous les cas où elle existe, la quantité $E(X)$ s'appelle la valeur moyenne de la v.a. X, son espérance ou encore le moment d'ordre 1.

Définition 7.18 Variance La variance de la v.a. X est, par définition la valeur moyenne de la v.a. $(X - E(X))^2$. Elle est désignée par var(X).

On a donc

$$var(X) = E[(X - E(X))^2].$$

Remarque Le moment d'ordre n est défini par $E(X^n) = \sum_{k\in N} x_k^n \; P(X = x_k)$.

Définition 7.19 Ecart-type La racine carrée de la variance est appelée l'écart-type et est désignée par $\sigma(X)$.

Proposition 7.2 *La variance est égale au moment d'ordre* 2 *moins l'espérance au carré, c'est-à-dire* $var(X) = E(X^2) - (E(X))^2$.

Exemple : si on reprend l'exemple du non pipé lancé deux fois. Son espérance est : $E(X) = \sum i * P(X = i) = 1 * \frac{1}{36} + 2 * \frac{3}{36} + 3 * \frac{5}{36} + 4 * \frac{7}{36} + 5 * \frac{9}{36} + 6 * \frac{11}{36} = \frac{161}{36}$

$E(X^2) = \sum x_i^2 f(x_i) = 1^2 * \frac{1}{36} + 2^2 * \frac{3}{36} + 3^2 * \frac{5}{36} + 4^2 * \frac{7}{36} + 5^2 * \frac{9}{36} + 6^2 * \frac{11}{36} = \frac{791}{36}$

d'où $var(X) = \frac{791}{36} - \frac{161^2}{36^2} = \frac{2555}{36^2} = 1,97$, et $\sigma(X) = 1,4$

Variables aléatoires indépendantes

Deux variables aléatoires X et Y définies sur le même espace probabilisé (Ω, p) sont indépendantes si, étant donnés $X(\Omega) = \{x_1, x_2, \ldots, x_i, \ldots\}$ et $Y(\Omega) = \{y_1, y_2, \ldots, x_j, \ldots\}$, on a pour tout (i, j)

$$P((X = x_i) \text{ et } (Y = y_j)) = P(X = x_i)\, P(Y = y_j).$$

Proposition 7.3 *Soient deux variables aléatoires X et Y définies sur le même espace probabilisé (Ω, p). On a toujours*

$$E(X + Y) = E(X) + E(Y), \qquad E(\lambda X) = \lambda E(X).$$

Si de plus X et Y sont des v.a. indépendantes, alors

$$E(XY) = E(X)\, E(Y), \qquad var(X + Y) = var(X) + var(Y).$$

7.6 Lois classiques

7.6.1 Loi uniforme discrète

Une urne contient n boules numérotées de 1 à n. On en tire une au hasard et on note X la variable aléatoire correspondant au nombre obtenu. Alors X suit une loi uniforme discrète.

Définition 7.20 loi uniforme discrète Soit $\{x_1, x_2, \ldots, x_n\}$ une partie à n éléments. X suit une loi uniforme discrète si $X(\Omega) \subset \{x_1, x_2, \ldots, x_n\}$ et $P(X = x_i) = \frac{1}{n}$.

Si on fixe $x_i = i$, pour $i = 1 \ldots n$, on a alors $E(X) = \frac{n+1}{2}$ et $var(X) = \frac{n^2 - 1}{12}$.

7.6.2 Loi de Bernoulli

On considère une épreuve aléatoire à deux issues : échec ou succès, la probabilité du succès étant p. Elle suit alors une loi de Bernoulli de paramètre p.

Définition 7.21 loi de Bernoulli On dit que X suit une loi de Bernoulli de paramètre p si : $X(\Omega) = \{0, 1\}$ et P(X=1)= p et P(X=0)= 1-p.

Proposition 7.4 *On a alors $E(X) = p$ et $var(X) = p(1 - p)$.*

Loi binomiale

Définition 7.22 essais de Bernoulli On suppose que l'on effectue une expérience aléatoire E possèdant une probabilité p de succès (et donc $1 - p$ d'échec). On repète cette expérience n fois. On suppose que les essais sont indépendants et que la probabilité de succès est la même à chaque expérience. Alors ces expériences constituent des essais de Bernoulli.

Soit l'expérience qui consiste à lancer n fois de suite et indépendamment une pièce biaisée. Les épreuves sont numérotées de 1 à n. On désigne par X_i le résultat de la i-ème épreuve : X_i a donc deux valeurs possibles 0 ou 1 et on pose $p = P(X_i = 1), q = (1 - p) = P(X_i = 0)$. On désigne par Y la variable aléatoire

$$Y = X_1 + X_2 + X_3 + \ldots + X_n.$$

L'ensemble $Y(\Omega)$ est exactement l'ensemble $\{0, 1, \ldots, n\}$, mais P_Y n'est plus la probabilité uniforme sur cet ensemble. L'événement $(Y = k)$ a pour probabilité

$$P(Y = k) = \binom{n}{k} p^k q^{n-k}.$$

On dit que Y suit la loi de Bernoulli de paramètres (n, p), et on la désigne par $\mathcal{B}(n, p)$.

Définition 7.23 loi binomiale On dit que X suit une loi binomiale de paramètres n et p si : $X(\Omega)$ = $\{0, 1, \ldots, n\}$, et

$$P(X = k) = \binom{n}{k} p^k q^{n-k}.$$

Proposition 7.5 *La valeur moyenne d'une v. a. qui suit une loi binomiale $\mathcal{B}(n, p)$ est égale à $n\ p$. Sa variance est égale à $n\ p\ (1 - p)$.*

Exemple On considère un tirage avec remises de boules dans une urne contenant une proportion de p boules blanches (et des boules rouges). On fait n tirages successifs et on appelle X la variable aléatoire correspondant au nombre de boules blanches tirées.

Alors X suit une loi binomiale de paramètres n et p.

7.6.3 Loi géométrique

On effectue des essais de Bernoulli(toujours avec une probabilité p de succès). On considère la variable aléatoire X qui désigne le nombre d'essais nécessaires pour obtenir un premier succès. On dit que X suit une loi géométrique de paramètre p notée Géom(p).
Exemple : Soit E un ensemble tel que $|E| = n, |A| = k$. On suppose qu'on effectue un tirage uniforme sur l'ensemble E. On effectue ces tirages parmi les éléments de E jusqu'au moment où on a tiré un élément de A. On désigne par X le nombre de tirages effectués.

Puisque le tirage est uniforme, la probabilité de tirer un élément de A est égale à $p = k/n$. On a alors $P(X = 1) = p$. L'algorithme effectue au moins $k + 1$ itérations, i.e., $P(X \geq k + 1)$. quand les k premiers tirages sont tombés à l'extérieur de A.
Ces tirages étant indépendants, on a

$$P(X \geq k + 1) = (1 - p)^k.$$

il vient,

$$\begin{aligned} P(X = k+1) &= P((X \geq k+1) \cap (X < k+2)) \\ &= P(X < k+2 \mid X \geq k+1)\; P(X \geq k+1) \\ &= p\,(1-p)^k. \end{aligned}$$

Définition 7.24 Loi géométrique On dit que X suit la loi géométrique de paramètre p si $X(\Omega) = \mathbb{N}^*$ et $P(X = k) = p\,(1-p)^{k-1}$

Proposition 7.6 *Soit X une variable aléatoire suivant la loi géométrique, on a alors*

$$E(X) = \frac{1}{p} \text{ et } var(X) = \frac{1-p}{p^2}.$$

7.6.4 Loi de Pascal

Soit $k \in \mathbb{N}^*$, on effectue des essais de Bernoulli (toujours avec une probabilité p de succès). On considère la variable aléatoire Y qui désigne le nombre d'essais nécessaires pour obtenir k succès. On dit que Y suit une loi de Pascal de paramètre p et k. Comme le nombre d'essais nécessaires pour obtenir un succès est indépendant du nombre d'essais nécessaires pour obtenir les succès précédents, Y correspond à la somme de k variables aléatoires de loi géométrique de paramètre p.
On montre

$$P(Y = k) = \binom{n-1}{k-1}\, p^k q^{n-k}.$$

$$E(X) = \frac{k}{p} \text{ et } var(X) = k\,\frac{1-p}{p^2}.$$

7.6.5 Loi hypergéométrique

On considère une urne contenant M boules dont n blanches. On tire sans les remettre, p boules successivement ($p \leq n$). On considère la variable aléatoire X correspondant au nombre de boules blanches sorties après ces p tirages. Alors X est une variable aléatoire hypergéométrique de paramètres (N, n, p).

Définition 7.25 Loi hypergéométrique Soient n, N, m trois entiers positifs tels que $n \leq N$ et $m < N$. On dit que X suit une loi hypergéométrique de paramètres N, n et m si $X(\Omega) \subset \{0, 1, \ldots, n\}$ et

$$P(X = k) = \frac{\binom{m}{k}\binom{N-m}{n-k}}{\binom{N}{n}}.$$

Proposition 7.7 *Soit X suivant une loi hypergéométrique, on a alors*

$$E(X) = \frac{nm}{N} \text{ et } var(X) = \frac{N-n}{N-1}\,\frac{nm}{N}\,(1 - \frac{m}{N}).$$