

Chapitre 12

Variables aléatoires finies

Lorsqu'on étudie un phénomène, on est amené à étudier des variables, des grandeurs numériques liées à ce phénomène. De façon informelle, une variable aléatoire réelle est un nombre lié à une expérience aléatoire dont la valeur dépend exclusivement du résultat ω de cette expérience. On peut donc voir cela comme un objet qui, à une éventualité ω , associe un nombre réel dépendant de ω et qu'on notera $X(\omega)$. Mathématiquement, une variable aléatoire est donc une fonction à valeurs réelles définie sur l'univers Ω associé à l'expérience. Quelques exemples de variables aléatoires :

- la somme des chiffres obtenus en lançant deux dés.
- le nombre moyen d'appels reçus par un standard téléphonique en une heure.
- la durée de vie d'une ampoule.

Dans tout ce chapitre, $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ désigne un espace probabilisé fini.

I Variable aléatoire réelle finie

1) Définitions et exemples

Définition. Une variable aléatoire réelle finie sur Ω est une application X définie sur Ω et à valeurs réelles.

L'ensemble $X(\Omega) = \{X(\omega) \mid \omega \in \Omega\}$ est l'ensemble des valeurs prises par la variable aléatoire X . On l'appelle univers image de X .

Remarques :

- Comme Ω est finie, $X(\Omega)$ l'est aussi. Si $n = \text{card}(X(\Omega))$, alors on peut écrire $X(\Omega) = \{x_1; \dots; x_n\}$, où les x_i , $1 \leq i \leq n$ sont des réels distincts.
- Si $\omega \in \Omega$, on dit que $X(\omega)$ est une réalisation de X .

Exemples :

Pour le moment on se limite aux variables aléatoires définies sur un espace probabilisé fini.

Cette définition n'est valable que dans le cas des univers finis. Nous verrons au second semestre la notion de variables aléatoires réelles sur des espaces probabilisables quelconques.

Ces définitions permettent en quelque sorte d'« oublier » l'espace probabilisable sur lequel est définie la variable aléatoire X , et de voir X comme un nombre aléatoire. Le plus souvent on ne précisera pas l'univers et on définira les variables aléatoires par des phrases. Par exemple : « on lance deux dés et on note X la somme des chiffres des deux faces obtenues ». Mais gardons en tête la vraie nature de ces objets. En toute rigueur, on préférera écrire, par exemple :

- « $[X = a]$ est réalisé » plutôt que « $X = a$ ».
- « Si on obtient Pile, X prend la valeur 1 » plutôt que « on pose $X = 1$ si on obtient Pile ».
- « $[X = 1]$ sachant $[Y = 0]$ » plutôt que « $X = 1$ sachant que $Y = 0$ ».

Néanmoins beaucoup de sujets de concours ne s'embêtent pas avec cela (mais certains si) et les auteurs de ce livre ne le leur reprochent pas : c'est un point de vue typiquement probabiliste et, dans la majorité des cas, manipuler les variables aléatoires comme s'ils étaient des nombres aléatoires ne pose aucun problème (c'est toute l'idée de ces notations!).

Comme dans le chapitre précédent, la notion de système complet d'événements trouve son intérêt dans la formule des probabilités totales. Nous verrons des exemples dans les paragraphes à venir.

Pour simplifier, on note $\mathbb{P}(X \in A)$, $\mathbb{P}(X = x)$, $\mathbb{P}(X < x)$ etc. au lieu de $\mathbb{P}([X \in A])$, $\mathbb{P}([X = x])$, $\mathbb{P}([X < x])$, etc.

Définition. Soient $(a, b) \in \mathbb{R}^2$ tel que $a < b$ et X une variable aléatoire réelle finie sur Ω . On définit alors les événements suivants :

$$[X = a] = \{\omega \in \Omega \mid X(\omega) = a\}, \quad [X < a] = \{\omega \in \Omega \mid X(\omega) < a\},$$

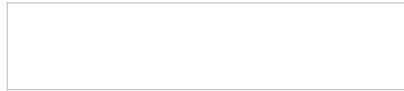
$$[X \leq a] = \{\omega \in \Omega \mid X(\omega) \leq a\}, \quad [X > a] = \{\omega \in \Omega \mid X(\omega) > a\},$$

$$[X \geq a] = \{\omega \in \Omega \mid X(\omega) \geq a\}, \quad [a \leq X \leq b] = \{\omega \in \Omega \mid a \leq X(\omega) \leq b\}.$$

Plus généralement, si A est une partie de \mathbb{R} , alors on note

$$[X \in A] = \{\omega \in \Omega \mid X(\omega) \in A\}.$$

Remarque : Si $a \in X(\Omega)$, alors $[X = a]$ est bien un événement (c'est-à-dire une partie de Ω). En effet c'est l'ensemble des antécédents de a par l'application X dans Ω . Si $a \in \mathbb{R} \setminus X(\Omega)$, alors $[X = a] = \emptyset$ est aussi un événement. Si $A \subset \mathbb{R}$, alors $[X \in A]$ est encore un événement : c'est l'ensemble des antécédents des réels de A par X . Il peut s'écrire comme l'union disjointe :



Exemple : Reprenons l'exemple précédent où X est la variable aléatoire représentant la somme des chiffres des faces obtenues par le lancer de deux dés à 6 faces. Nous avons, par exemple

Proposition. Soit X une variable aléatoire réelle finie sur Ω . La famille $([X = x])_{x \in X(\Omega)}$ est un système complet fini d'événements. On l'appelle le système complet associé à X .

DÉMONSTRATION. Pour tout $x \in X(\Omega)$, $[X = x] \in \mathcal{P}(\Omega)$ par définition. Si x et y sont distincts dans $X(\Omega)$, alors $[X = x] \cap [X = y] = \emptyset$ si bien que les événements $[X = x]$ et $[X = y]$ sont incompatibles. Enfin, si $\omega \in \Omega$, alors $\omega \in [X = X(\omega)] \subset \bigcup_{x \in X(\Omega)} [X = x] \subset \Omega$. Ainsi $\bigcup_{x \in X(\Omega)} [X = x] = \Omega$. \square

Exemple : On lance trois fois une pièce de monnaie. On peut considérer l'univers $\Omega = \{P; F\}^3$. Soit X la variable aléatoire qui donne le nombre de Pile obtenus.

2) Loi d'une variable aléatoire finie

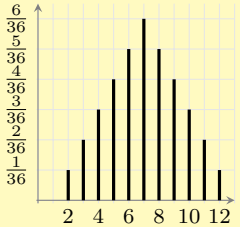
Définition (loi d'une variable aléatoire réelle finie). La loi (de probabilité) d'une variable aléatoire réelle finie X est la donnée de $X(\Omega)$ et de $\mathbb{P}([X = x])$ pour tout $x \in X(\Omega)$.

Pour représenter la loi d'une variable aléatoire réelle finie X , on peut donner une formule générale pour $\mathbb{P}(X = x)$, $x \in X(\Omega)$. On peut aussi (lorsque $X(\Omega)$ contient peu de

valeurs), dresser un tableau de valeurs ou construire un diagramme en bâtons (pour chaque $x \in X(\Omega)$, on trace un bâton de longueur $\mathbb{P}(X = x)$ situé à l'abscisse x).

Exemple : Reprenons l'exemple de la variable aléatoire X donnant la somme des chiffres des faces obtenues par le lancer de deux dés à 6 faces (on munit l'univers $\Omega = \llbracket 1 ; 6 \rrbracket^2$ de la probabilité uniforme). Déterminons sa loi :

On peut aussi tracer son diagramme en bâtons :



donc on obtient le tableau :

x	2	3	4	5	6	7	8	9	10	11	12
$\mathbb{P}(X = x)$											

On remarque que, pour tout $k \in \llbracket 2 ; 12 \rrbracket$, $\mathbb{P}(X = k) = \frac{6 - |7 - k|}{36}$.

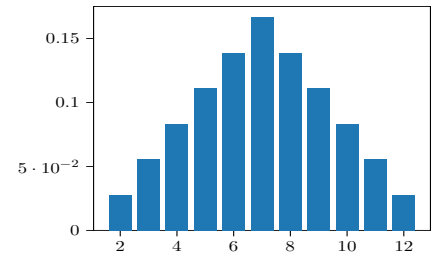
On peut utiliser Python pour représenter le diagramme à barres. Pour cela on remplace `plt.plot()` par `plt.bar()`. Traçons en Python le diagramme à barres correspondant :

La commande `plt.plot()` est très utile mais n'apparaît pas officiellement dans le programme.

```

1 X=range(2,13)
2 Y=np.array
  ([1,2,3,4,5,6,5,4,3,2,1])/36
3 plt.bar(X,Y)
4 plt.show()

```



Exemple : Soit $n \in \mathbb{N} \setminus \{0; 1\}$. On dispose d'une urne contenant une boule numérotée 1, de 2 boules numérotées 2, de 3 boules numérotées 3, ..., de $n - 1$ boules numérotées $(n - 1)$ et enfin de n boules numérotées n . On tire une boule au hasard dans l'urne. Si c'est la boule numérotée 1, le jeu s'arrête là et on ne gagne rien. Si c'est une boule numérotée k (avec $k \in \llbracket 2 ; n \rrbracket$), on lance un dé équilibré à k faces. Si la face obtenue porte le numéro j , on gagne $j - 1$ euros. On introduit X la variable aléatoire égale au numéro de la boule tirée et Y la variable aléatoire égale au montant gagné à l'issue du jeu. Déterminons les lois de X et de Y .

La probabilité de l'événement $[Y = j]$ dépend du dé que l'on a lancé donc de la boule tirée donc de la réalisation de X . On pense immédiatement à la formule des probabilités totales.

Même si on a déjà compris à ce stade que

$$\mathbb{P}_{[X=k]}(Y = j) = 0$$

lorsque $k \leq j$, on écrit quand même tous les termes dans la formule. En effet la famille $([X = k])_{k \geq j+1}$ n'est pas un système complet d'événements.

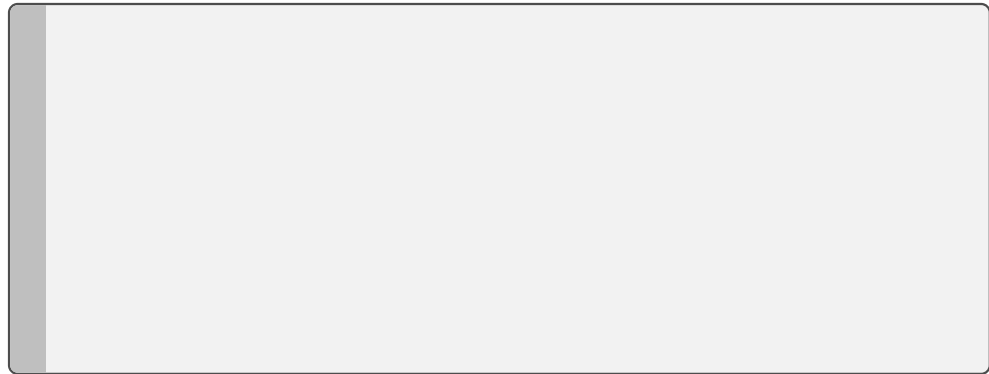


Simuler une variable aléatoire réelle d'une loi donnée à l'aide d'un ordinateur consiste à construire un nombre réel que l'on peut assimiler à une réalisation $X(\omega)$ d'une variable aléatoire X ayant cette loi.



Si X_1 et X_2 ont la même loi, on note parfois $X_1 \stackrel{\mathcal{L}}{=} X_2$. Attention, cela ne veut pas du tout dire que $X_1 = X_2$! Par exemple, ci-contre, le dé peut donner un nombre pair et la pièce tomber sur Face, et alors X_1 prend la valeur 0 tandis que X_2 prend la valeur 1. Avoir la même loi signifie prendre les mêmes valeurs avec les mêmes probabilités, mais pas forcément en même temps ! Plus fort : si X suit une loi de Bernoulli de paramètre $1/2$, alors $Y = 1 - X$ suit aussi une loi de Bernoulli de paramètre $1/2$ (cf. paragraphe III.2). On a $X \stackrel{\mathcal{L}}{=} Y$ mais X et Y ne sont jamais égales !

Écrivons une fonction Python qui prend en entrée n et qui simule Y .



Remarque : Deux variables aléatoires peuvent être définies sur des espaces probabilisés différents et avoir la même loi (elles prennent les mêmes valeurs avec les mêmes probabilités respectivement).

Par exemple : on lance une pièce de monnaie bien équilibrée on définit la variable aléatoire X_1 qui prend la valeur 1 si la pièce tombe sur Pile et 0 sinon (X_1 est définie sur $\Omega_1 = \{0; 1\}$ muni de la probabilité uniforme \mathbb{P}_1). On lance un dé équilibré à 6 faces et on définit la variable aléatoire X_2 qui prend la valeur 1 si le chiffre obtenu est pair et 0 sinon (X_2 est définie sur $\Omega_2 = \llbracket 1; 6 \rrbracket$ muni de la probabilité uniforme \mathbb{P}_2).

Proposition. Soit X une variable aléatoire réelle finie sur Ω . Si A est une partie de \mathbb{R} , alors



DÉMONSTRATION. Cela découle de la formule des probabilités totales appliquée au système complet d'événements associé à X . □

Exemple : Supposons que $X(\Omega) \subset \llbracket m; n \rrbracket$ avec m et n des entiers relatifs tels que $m \leq n$. Pour tout $k \in \llbracket m; n \rrbracket$, on a

Nous présenterons la fonction de répartition dans le cas des variables aléatoires discrètes au second semestre

Mais cela fonctionne même avec un élément n'appartenant pas à $X(\Omega)$. Par exemple, si

$X(\Omega) = \llbracket 1; n \rrbracket$, alors

Remarques :

- Si X est une variable aléatoire réelle finie, la fonction $F_X : t \in \mathbb{R} \mapsto \mathbb{P}(X \leq t)$ est appelée fonction de répartition de X . Elle jouera un rôle important en deuxième année.
- Toujours dans le cas où $X(\Omega) \subset \llbracket m; n \rrbracket$, retenons que, pour tout $k \in \llbracket m; n \rrbracket$,

Ces formules sont très utiles si on cherche notamment la loi d'un maximum ou d'un minimum, cf. exemple ci-dessous). Dans ce cas on retrouve la loi grâce aux formules ci-contre.

Exemple : Soient n et p dans \mathbb{N}^* . On dispose d'une urne contenant n boules numérotées de 1 à n . On tire successivement et avec remise p boules dans l'urne et on note X le plus grand numéro tiré.

On peut coder l'expérience par un p -uplet d'éléments de $\llbracket 1; n \rrbracket$ de telle sorte que, pour tout $i \in \llbracket 1; p \rrbracket$, x_i est le numéro de la $i^{\text{ème}}$ boule tirée. On prend $\Omega = \llbracket 1; n \rrbracket^p$ et on munit $(\Omega, \mathcal{P}(\Omega))$ de l'équiprobabilité \mathbb{P} .

Ce qu'on résume grossièrement par : « la somme des probabilités vaut 1. »

Corollaire. Si X est une variable aléatoire réelle finie sur Ω , alors

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

En notant $X(\Omega) = \{x_1; \dots; x_n\}$, on a $\sum_{i=1}^n \mathbb{P}(X = x_i) = 1$.

Forcément alors $p_i \in [0; 1]$ pour tout $i \in \llbracket 1; n \rrbracket$.

Théorème. Soit $n \in \mathbb{N}^*$. Soit $(p_i)_{1 \leq i \leq n}$ une famille finie de réels positifs tels que $\sum_{i=1}^n p_i = 1$. Soient x_1, \dots, x_n des réels deux à deux distincts. Alors il existe un espace probabilisé fini $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ et une variable aléatoire réelle finie X sur Ω telle que $X(\Omega) = \{x_1; \dots; x_n\}$, et

$$\forall i \in \llbracket 1; n \rrbracket, \quad \mathbb{P}(X = x_i) = p_i.$$

Il n'y a unicité ni de $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$, ni de la variable aléatoire X .



A priori Ω peut comporter des événements élémentaires de probabilité nulle et, dans ce cas, il se peut que la probabilité que X prenne certaines valeurs de $X(\Omega)$ soit nulle. Mais en général on suppose que Ω est tel que $\mathbb{P}(X = x) > 0$ pour tout $x \in X(\Omega)$.

DÉMONSTRATION. On considère $\Omega = \{x_1; \dots; x_n\}$ et on définit \mathbb{P} l'unique probabilité sur $(\Omega, \mathbb{P}(\Omega))$ telle que, pour tout $i \in \llbracket 1; n \rrbracket$, $\mathbb{P}(\{x_i\}) = p_i$. On prend $X : x \in \Omega \mapsto x$. On a $X(\Omega) = \Omega$ et, pour tout $i \in \llbracket 1; n \rrbracket$, $\mathbb{P}(X = x_i) = \mathbb{P}(\{x_i\}) = p_i$. \square

Exemple :



On a aussi $Y = g \circ X$. On dit que Y est un transfert de X par g .

Définition. Soit X une variable aléatoire réelle finie sur Ω . Soit g une fonction à valeurs réelles telle que $X(\Omega) \subset D_g$. Alors

$$Y : \begin{cases} \Omega & \longrightarrow & \mathbb{R} \\ \omega & \longmapsto & g(X(\omega)) \end{cases}$$

est une variable aléatoire réelle finie notée $g(X)$.



En posant

$$X(\Omega) = \{x_1; \dots; x_n\},$$

on obtient $Y(\Omega) = \{g(x_1); \dots; g(x_n)\}$ mais il se peut que les $g(x_i)$ ne soient pas distincts. En effet g peut ne pas être injective.

Soit X une variable aléatoire réelle finie sur Ω . On pose $X(\Omega) = \{x_1; \dots; x_n\}$ avec $n = \text{card}(X(\Omega)) \in \mathbb{N}^*$. Étudions la loi de $Y = g(X)$ dans certains cas particuliers :



Remarquons qu'il est facile de déterminer la loi du transfert d'une variable aléatoire réelle finie X (dont on connaît la loi) par une bijection sur un intervalle contenant $X(\Omega)$. Dans le cas général, pour obtenir la probabilité $\mathbb{P}[f(X) = y]$ on fait la somme sur tous les antécédents de y . Aucune formule générale n'est au programme, il faut revenir au cas par cas.

Exemple : On lance deux dés à 6 faces bien équilibrés. Notons X la somme des chiffres des dés et Y la différence des chiffres du premier dé avec le second. Posons $Z = X - 7$ et $U = |Y| + 1$.

Nous laissons le détail du calcul de la loi de Y en exercice. Par exemple il y a 5 façons d'obtenir $-1 : 5 - 6, 4 - 5, 3 - 4, 2 - 3$ et $1 - 2$.

x	-5	-4	-3	-2	-1	0	1	2	3	4	5
$\mathbb{P}(Z = x)$											
$\mathbb{P}(Y = x)$											

x	1	2	3	4	5	6
$\mathbb{P}(U = x)$						

4) Indépendance de variables aléatoires finies

Comme pour les événements, on omet souvent le mot « mutuellement » dans la pratique.

Définition. Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Soient X_1, \dots, X_n des variables aléatoires réelles finies sur $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$. On dit que X_1, \dots, X_n sont mutuellement indépendantes si, pour tout (x_1, x_2, \dots, x_n) dans $X_1(\Omega) \times X_2(\Omega) \cdots \times X_n(\Omega)$,

$$\mathbb{P} \left(\bigcap_{i=1}^n [X_i = x_i] \right) = \prod_{i=1}^n \mathbb{P}(X_i = x_i).$$

Officiellement la notion d'indépendance mutuelle de variables aléatoires n'apparaît qu'au second semestre. Elle ne représente pas de difficulté majeure à ce stade et il serait dommage de s'en priver pour les exercices. Nous y reviendrons plus longuement dans le chapitre 29.

On admet la caractérisation suivante :

Proposition. Soit $n \in \mathbb{N} \setminus \{0; 1\}$. Les variables aléatoires réelles finies X_1, \dots, X_n sont mutuellement indépendantes si et seulement si, pour tous intervalles I_1, \dots, I_n ,

$$\mathbb{P} \left(\bigcap_{i=1}^n [X_i \in I_i] \right) = \prod_{i=1}^n \mathbb{P}(X_i \in I_i)$$

II Espérance et variance

1) Espérance

a) Définition et exemples

Une variable aléatoire réelle finie admet toujours une espérance. Nous verrons au second semestre que c'est faux en général pour des variables aléatoires réelles quelconques.

Définition. Soit X une variable aléatoire réelle finie sur Ω . On appelle espérance de X le réel

En posant $X(\Omega) = \{x_1; \dots; x_n\}$, on a

L'espérance d'une variable aléatoire réelle finie est une moyenne pondérée. Si X représente le gain d'un jeu, alors $\mathbb{E}(X)$ représente le gain moyen que l'on peut espérer obtenir.

Exemples :

Si $c \in \mathbb{R}$, on note encore c la variable aléatoire constante égale à c (on parle alors de variable certaine). On a donc $\mathbb{E}(c) = c$.

L'espérance d'une variable aléatoire réelle finie ne dépend que de sa loi. Ainsi deux variables aléatoires ayant la même loi ont la même espérance. Attention la réciproque est fautive. Par exemple : on lance une pièce bien équilibrée et on pose X la variable aléatoire prenant pour valeur 1 si on tombe sur Pile et 0 sinon. Considérons aussi Y la variable aléatoire constante égale à $1/2$. Les variables aléatoires X et Y n'ont clairement pas la même loi ($X(\Omega) \neq Y(\Omega)$) et pourtant

$$\mathbb{E}(X) = \frac{1}{2} = \mathbb{E}(Y).$$

On rappelle que, pour tout $n \in \mathbb{N}$,

$$\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}.$$

- Soit $c \in \mathbb{R}$. Supposons que $X(\Omega) = \{c\}$. On a donc $\mathbb{P}(X = c) = 1$ et donc $\mathbb{E}(X) = c\mathbb{P}(X = c) = c$. L'espérance d'une variable aléatoire constante est donc égale à cette constante.
- Reprenons l'exemple du lancer de deux dés équilibrés à 6 faces. Si X donne la somme des chiffres des faces obtenues, alors

- Reprenons l'exemple de l'urne contenant une boule numérotée 1, de 2 boules numérotées 2, etc. et n boules numérotées n (cf. fin du paragraphe 1.2). On a calculé que, si Y désigne la variable aléatoire égale au montant gagné à l'issue du jeu, alors $Y(\Omega) = \llbracket 0; n-1 \rrbracket$ et, pour tout $j \in \llbracket 0; n-1 \rrbracket$, $\mathbb{P}(Y = j) = \frac{2(n-j)}{n(n+1)}$.

b) Propriétés de l'espérance

Proposition (espérance d'une somme). Si X et Y sont deux variables aléatoires réelles finies, alors $\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$.

DÉMONSTRATION. Quitte à attribuer des probabilités nulles à certaines valeurs, supposons que $X(\Omega) = \llbracket m; n \rrbracket$ et $Y(\Omega) = \llbracket p; q \rrbracket$ avec m, n, p, q des entiers tels que $m \leq n$ et $p \leq q$. Posons $Z = X + Y$. On a $Z(\Omega) = \llbracket m+p; n+q \rrbracket$ et

$$\mathbb{E}(Z) = \sum_{z=m+p}^{n+q} z \mathbb{P}(Z = z).$$

La formule des probabilités totales appliquée au système complet d'événements associé à Y donne :

$$\mathbb{E}(Z) = \sum_{z=m+p}^{n+q} z \left(\sum_{y=p}^q \mathbb{P}([Z = z] \cap [Y = y]) \right)$$

$$\begin{aligned}
&= \sum_{z=m+p}^{n+q} z \left(\sum_{y=p}^q \mathbb{P}([X = z - y] \cap [Y = y]) \right) \\
&= \sum_{y=p}^q \left(\sum_{z=m+p}^{n+q} z \mathbb{P}([X = z - y] \cap [Y = y]) \right).
\end{aligned}$$

Faisons le changement d'indice $x = z - y$ (à y fixé) dans la deuxième somme :

$$\mathbb{E}(Z) = \sum_{y=p}^q \left(\sum_{x=m+p-y}^{n+q-y} (x + y) \mathbb{P}([X = x] \cap [Y = y]) \right).$$

Lorsque $y \in \llbracket p; q \rrbracket$,
 $m + p - y \leq m$ et
 $n + q - y \geq n$. Or, si
 $x \notin \llbracket m; n \rrbracket$,

$[X = x] \cap [Y = y] = \emptyset$
est de probabilité nulle.

Dans la deuxième somme, seuls les termes d'indices m à n sont éventuellement non nuls :

$$\mathbb{E}(Z) = \sum_{y=p}^q \left(\sum_{x=m}^n (x + y) \mathbb{P}([X = x] \cap [Y = y]) \right).$$

Par linéarité de la somme et en invertissant l'ordre de sommation dans la première somme, on obtient

$$\mathbb{E}(Z) = \sum_{x=m}^n x \left(\sum_{y=p}^q \mathbb{P}([X = x] \cap [Y = y]) \right) + \sum_{y=p}^q y \left(\sum_{x=m}^n \mathbb{P}([X = x] \cap [Y = y]) \right).$$

En appliquant la formule des probabilités totales au système complet d'événements associé à Y dans la première somme et celui associé à X dans la deuxième somme, on obtient

$$\mathbb{E}(Z) = \sum_{x=m}^n x \mathbb{P}(X = x) + \sum_{y=p}^q y \mathbb{P}(Y = y) = \mathbb{E}(X) + \mathbb{E}(Z). \quad \square$$

Théorème (linéarité de l'espérance). Si X et Y sont deux variables aléatoires réelles finies et si $(a, b) \in \mathbb{R}^2$, alors

$$\mathbb{E}(aX + bY) = a \mathbb{E}(X) + b \mathbb{E}(Y).$$

DÉMONSTRATION. En appliquant le résultat précédent à aX et bY (au lieu de X et Y), on obtient $\mathbb{E}(aX + bY) = \mathbb{E}(aX) + \mathbb{E}(bY)$. Notons $X(\Omega) = \{x_1; \dots; x_n\}$.

- Si $a = 0$, on a $aX = 0$ donc $\mathbb{E}(aX) = 0 = a \mathbb{E}(X)$.
- Si $a \neq 0$, alors $(aX)(\Omega) = \{ax_1; \dots; ax_n\}$ donc

$$\mathbb{E}(aX) = \sum_{k=1}^n ax_k \mathbb{P}(aX = ax_k) = a \sum_{k=1}^n x_k \mathbb{P}(X = x_k) = a \mathbb{E}(X).$$

Ainsi $\mathbb{E}(aX) = a \mathbb{E}(X)$. De même on montre que $\mathbb{E}(bY) = b \mathbb{E}(Y)$. D'où le résultat. \square

Par récurrence, on obtient :

Théorème (linéarité de l'espérance). Soient X_1, \dots, X_n des variables aléatoires réelles finies et a_1, \dots, a_n des réels. On a

$$\mathbb{E} \left(\sum_{k=1}^n a_k X_k \right) = \sum_{k=1}^n a_k \mathbb{E}(X_k).$$

Théorème (un cas particulier important). Si X est une variable aléatoire réelle finie et si $(a, b) \in \mathbb{R}^2$, $\mathbb{E}(aX + b) = a \mathbb{E}(X) + b$.

DÉMONSTRATION. Il s'agit du cas particulier où Y est la variable aléatoire constant égale à 1. Son espérance vaut 1. \square

C'est le cas si X est positive (i.e. $X(\Omega) \subset \mathbb{R}_+$) sur Ω .

Proposition (positivité de l'espérance). Soit X une variable aléatoire réelle finie telle que $\mathbb{P}(X \geq 0) = 1$. Alors $\mathbb{E}(X) \geq 0$ avec égalité si et seulement si $\mathbb{P}(X = 0) = 1$.

DÉMONSTRATION. Si $x \in X(\Omega) \cap \mathbb{R}_-^*$, alors $[X = x] \subset [X < 0]$ donc $\mathbb{P}(X = x) \leq \mathbb{P}(X < 0) = 0$ donc $\mathbb{P}(X = x) = 0$. Ainsi

$$\mathbb{E}(X) = \sum_{x \in X(\Omega) \cap \mathbb{R}_+} \underbrace{x \mathbb{P}(X = x)}_{\geq 0} + \sum_{x \in X(\Omega) \cap \mathbb{R}_-^*} \underbrace{x \mathbb{P}(X = x)}_{=0} \geq 0.$$

Si l'espérance est nulle, alors la première somme est nulle. Ainsi (comme ses termes sont positifs), pour tout $x \in X(\Omega) \cap \mathbb{R}_+^*$, on a $x \mathbb{P}(X = x) = 0$ et donc $\mathbb{P}(X = x) = 0$. On a

$$\mathbb{P}(X = 0) = 1 - \mathbb{P}(X \neq 0) = 1 - \sum_{x \in X(\Omega) \cap \mathbb{R}_+^*} \mathbb{P}(X = x) = 1 - 0 = 1.$$

Réciproquement supposons que $\mathbb{P}(X = 0) = 1$. Alors pour tout $x \in X(\Omega) \cap \mathbb{R}_+^*$, $\mathbb{P}(X = x) \leq \mathbb{P}(X \neq 0) = 0$ et donc $\mathbb{P}(X = x) = 0$. On en déduit que $x \mathbb{P}(X = x) = 0$ pour tout $x \in X(\Omega)$. D'où $\mathbb{E}(X) = 0$. \square

Théorème (croissance de l'espérance). Si X et Y sont deux variables aléatoires réelles finies telles que $\mathbb{P}(X \leq Y) = 1$, alors $\mathbb{E}(X) \leq \mathbb{E}(Y)$.

DÉMONSTRATION. Posons $Z = Y - X$. On a $\mathbb{P}(Z \geq 0) = \mathbb{P}(X \leq Y) = 1$. La positivité de l'espérance entraîne alors que $\mathbb{E}(Z) \geq 0$. Par linéarité, on obtient que $\mathbb{E}(Y) - \mathbb{E}(X) = \mathbb{E}(Y - X) = \mathbb{E}(Z) \geq 0$ et donc $\mathbb{E}(X) \leq \mathbb{E}(Y)$. \square

Exemple : Nous avons vu précédemment, que si on lance deux dés équilibrés et que l'on note X la somme des chiffres des faces obtenues et Y la différence des chiffres du premier dé et du second, alors Y et $X - 7$ ont la même loi. Ainsi, par linéarité,

$$\mathbb{E}(Y) = \mathbb{E}(X - 7)$$

Définition. Une variable aléatoire réelle finie X d'espérance nulle est dite centrée.

Corollaire. Si X est une variable aléatoire réelle finie, alors la variable aléatoire $X - \mathbb{E}(X)$ est centrée.

DÉMONSTRATION.

\square

c) Le théorème de transfert

Théorème (de transfert). Soit X est une variable aléatoire réelle finie sur Ω . Si $g : X(\Omega) \rightarrow \mathbb{R}$, alors

$$\mathbb{E}(g(X)) = \sum_{x \in X(\Omega)} g(x) \mathbb{P}(X = x)$$

En posant $X(\Omega) = \{x_1; \dots; x_n\}$, on a

$$\mathbb{E}(g(X)) = \sum_{i=1}^n g(x_i) \mathbb{P}(X = x_i)$$

On peut interpréter l'espérance de X comme « la valeur moyenne de X », c'est-à-dire, **en gros**, que si on joue n fois (avec n très grand), alors on gagne environ $n \times \mathbb{E}(X)$. On dit donc qu'un jeu est favorable si $\mathbb{E}(X) > 0$, défavorable si $\mathbb{E}(X) < 0$ et équitable si $\mathbb{E}(X) = 0$. Attention, ce n'est pas parce que $\mathbb{E}(X) > 0$ que l'on doit être incité à jouer! Par exemple, si $X(\Omega) = \{-10^4; 10^8\}$, $\mathbb{P}(X = -10^4) = \frac{9999}{10^4}$ et $\mathbb{P}(X = 10^8) = \frac{1}{10^4}$, alors $\mathbb{E}(X) = \frac{1}{10^4} > 0$, mais qui veut jouer à ce jeu? Si on joue une fois, on a « toutes les chances de perdre ». Ce n'est qu'en jouant un très grand nombre de fois que les rares gains seront compensés par les rares pertes... mais on sera ruiné avant!

Le théorème de transfert, dont la preuve est admise conformément au programme, permet de calculer l'espérance du transfert d'une variable aléatoire uniquement à l'aide de sa loi. En clair : on applique g aux valeurs de l'univers image, mais pas aux probabilités!

Quelques cas particuliers :

Exemples :

2) Variance et écart type

La variance mesure la dispersion d'une variable aléatoire par rapport à son espérance, c'est-à-dire la manière dont la variable aléatoire se répartit autour de son espérance.

Définition. Soit X une variable aléatoire réelle finie sur Ω . On appelle variance de X le réel

Posons $X(\Omega) = \{x_1; \dots; x_n\}$ et notons $m = \mathbb{E}(X)$. Le théorème de transfert entraîne que

En pratique, on utilise toujours la formule de Koenig-Huygens pour calculer une variance.

Proposition (formule de Koenig-Huygens). Si X est une variable aléatoire réelle finie, alors

DÉMONSTRATION.

□

Exemple : Reprenons encore une fois l'exemple de l'urne contenant une boule numérotée 1, de 2 boules numérotées 2, etc. et n boules numérotées n (cf. paragraphes I.2 et II.1). On a calculé que $\mathbb{E}(Y) = \frac{n-1}{3}$.

Si $\mathbb{P}(X = a) = 1$, on prend en général la convention que $X(\Omega) = \{a\}$ et on a vu plus haut qu'alors $\mathbb{E}(X) = a$. Il est intuitif que la variance est nulle si et seulement si on est dans ce cas de figure (on dit que X suit une loi certaine, cf. paragraphe III.1) : comme dit plus haut, la variance mesure la dispersion d'une variable aléatoire par rapport à son espérance. Cette dispersion est nulle si et seulement si la variable aléatoire et son espérance sont égales (avec probabilité 1)!

Proposition. Si X est une variable aléatoire réelle finie, alors $\mathbb{V}(X) \geq 0$. De plus $\mathbb{V}(X) = 0$ si et seulement si il existe $a \in \mathbb{R}$ tel que $\mathbb{P}(X = a) = 1$.

DÉMONSTRATION. Puisque $(X - m)^2$ est une variable aléatoire positive, la propriété de positivité de l'espérance entraîne que $\mathbb{V}(X) = \mathbb{E}((X - m)^2) \geq 0$ et que, $\mathbb{V}(X) = 0$ si et seulement si $\mathbb{P}((X - m)^2 = 0) = 1$ si et seulement si $\mathbb{P}(X = m) = 1$ (d'où le résultat avec $m = a$). \square

Proposition. Soit X une variable aléatoire réelle finie. Si a et b sont deux réels, alors $\mathbb{V}(aX + b) = a^2\mathbb{V}(X)$.

DÉMONSTRATION.

Définition. Soit X une variable aléatoire réelle finie sur Ω . On appelle écart-type de X le réel $\sigma(X) = \sqrt{\mathbb{V}(X)}$.

Définition. Une variable aléatoire réelle finie X d'espérance nulle et d'écart-type égal à 1 est dite centrée réduite.

Comme la variance, l'écart type mesure la dispersion d'une variable aléatoire autour de son espérance. Plus son écart type est faible, plus la probabilité qu'une variable aléatoire prenne des valeurs éloignées de son espérance est faible.

Si $\sigma(X) > 0$, alors $\mathbb{E}\left(\frac{X - \mathbb{E}(X)}{\sigma(X)}\right) = 0$ et

$$\sigma\left(\frac{X - \mathbb{E}(X)}{\sigma(X)}\right) = \sqrt{\frac{\mathbb{E}((X - \mathbb{E}(X))^2)}{\sigma(X)^2}} = \sqrt{\frac{\mathbb{V}(X)}{\mathbb{V}(X)}} = 1.$$

D'où la définition suivante :

Définition. Soit X une variable aléatoire réelle finie sur Ω telle que $\sigma(X) > 0$. On appelle $X^* = \frac{X - \mathbb{E}(X)}{\sigma(X)}$ la variable aléatoire centrée réduite associée à X .

III Lois finies usuelles

1) Loi certaine

Définition. On dit qu'une variable aléatoire réelle finie suit une loi certaine si il existe $a \in \mathbb{R}$ tel que $X(\Omega) = \{a\}$.

On a déjà étudié les propriétés de variables certaines au fur et à mesure des paragraphes précédents. Résumons :

Proposition. On a $\mathbb{E}(X) = a$ et $\mathbb{V}(X) = 0$.

Réciproquement, on a vu que si X est une variable aléatoire de variance nulle alors il existe $m \in \mathbb{R}$ tel que $\mathbb{P}(X = m) = 1$. Quitte à enlever des valeurs de probabilités nulle, on peut supposer que $X(\Omega) = \{m\}$ et donc X est certaine.

2) Loi uniforme

a) Définition et interprétation

La loi uniforme est la loi que l'on rencontre dans les situations d'équiprobabilité : toutes les valeurs prises par une variable aléatoire X qui suit une loi uniforme sont équiprobables. Par exemple :

- On lance un dé équilibré à 6 faces. La variable aléatoire X qui donne le résultat obtenu suit la loi uniforme sur $\llbracket 1; 6 \rrbracket$.

- On dispose d'une urne contenant n boules numérotées de 1 à n . On tire une boule au hasard. La variable aléatoire X qui donne le numéro de la boule tirée suit la loi uniforme sur $\llbracket 1; n \rrbracket$.

Définition. Soit A une partie finie de \mathbb{R} . On dit qu'une variable aléatoire réelle finie X suit la loi uniforme sur A si et

On note $X \hookrightarrow \mathcal{U}(A)$

b) Propriétés

Proposition. Soit $n \in \mathbb{N}^*$. Si $X \hookrightarrow \mathcal{U}(\llbracket 1; n \rrbracket)$, alors

Remarque : Pour l'espérance, c'est intuitif : puisque X prend toutes les valeurs avec la même probabilité, la valeur moyenne est « le milieu » de l'ensemble !

DÉMONSTRATION.

Corollaire. Soient $(a, b) \in \mathbb{N}^2$ avec $a \leq b$. Si $X \hookrightarrow \mathcal{U}(\llbracket 1; n \rrbracket)$ avec $n = b - a + 1$, alors . En particulier :

Encore une fois, pour l'espérance, c'est intuitif : c'est le milieu !

DÉMONSTRATION.

□

C'est pour ça que la commande `rd.randint(1,n)<=c` renvoie bien True avec probabilité $\frac{c}{n}$. Cf. Python du chapitre précédent et ci-dessous.

Remarque : Soient c et n des entiers tels que $1 \leq c \leq n$. Soit $X \hookrightarrow \mathcal{U}(\llbracket 1; n \rrbracket)$. On a

c) Lois uniformes avec Python

Pour une implémentation en Python, on commence par :

```
1 import numpy.random as rd
```

Supposons que les réels a et b (tels que $a < b$) ont été implémentés en Python dans les variables a et b . Pour obtenir une réalisation d'une variable aléatoire de loi de $\mathcal{U}(\llbracket a; b \rrbracket)$, on peut utiliser la fonction :

```
1 X=rd.randint(a,b+1)
```

Ajouter une option N (l'implémentation d'un entier naturel N) à cette commande fournit une liste (ou plutôt un tableau unidimensionnel, cf. chapitre 19) de N réalisations indépendantes de variables aléatoires de la loi uniforme.

3) Loi de Bernoulli

a) Définition et interprétation

Définition. Soit $p \in]0; 1[$. On dit qu'une variable aléatoire réelle finie X suit la loi de Bernoulli de paramètre p si $\mathbb{P}(X = 1) = p$.
On note $X \hookrightarrow \mathcal{B}(p)$. Le paramètre p (resp. $q = 1 - p$) est appelé probabilité de succès (resp. d'échec).

Exemples :

- On lance une pièce de monnaie truquée de telle sorte que la probabilité qu'elle tombe sur Pile soit $p \in]0; 1[$. Soit X la variable aléatoire qui vaut 1 si la pièce tombe sur Pile et 0 si elle tombe sur face. Alors $X \hookrightarrow \mathcal{B}(p)$.
- Si $X \hookrightarrow \mathcal{B}(p)$, alors $X^2 \hookrightarrow \mathcal{B}(p)$. En effet, comme X ne prend que 0 et 1 pour valeurs, on a $X^2 = X$.
- Si $X \hookrightarrow \mathcal{B}(p)$, alors $1 - X \hookrightarrow \mathcal{B}(1 - p)$. En effet $1 - X$ ne prend que $1 = 1 - 0$ et $0 = 1 - 1$ pour valeurs et

$$\mathbb{P}(1 - X = 1) = \mathbb{P}(X = 0) = p.$$

La loi de Bernoulli est la loi que l'on rencontre lorsqu'il n'y a que deux issues possibles à une expérience : succès et échec. On code le succès par la valeur 1 et l'échec par la valeur 0. On peut dans tous les cas s'y ramener facilement : si a et b sont deux réels tels que $a < b$ et si X est une variable aléatoire réelle finie qui ne prend que les valeurs a et b (avec probabilités non nulles), alors

$$Y = \frac{X - a}{b - a} \hookrightarrow \mathcal{B}(p)$$

avec $p = \mathbb{P}(X = b)$.

b) Propriétés

Proposition. Soit $p \in]0; 1[$. Si $X \leftrightarrow \mathcal{B}(p)$, alors

DÉMONSTRATION.

□

La formule

$$\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$$

relie la probabilité d'un événement avec l'espérance d'une variable aléatoire.

Proposition. Soit A un événement tel que $\mathbb{P}(A) \in]0; 1[$. On définit $\mathbb{1}_A$ la variable aléatoire définie sur Ω par

$$\forall \omega \in \Omega, \quad \mathbb{1}_A(\omega) = \begin{cases} 1 & \text{si } \omega \in A, \\ 0 & \text{si } \omega \notin A. \end{cases}$$

Il s'agit d'une variable aléatoire de loi de Bernoulli de paramètre $\mathbb{P}(A)$ et donc $\mathbb{E}(\mathbb{1}_A) = \mathbb{P}(A)$.

DÉMONSTRATION. La variable aléatoire $\mathbb{1}_A$ ne prend que deux valeurs : 0 et 1. Elle suit donc une loi de Bernoulli de paramètre $p = \mathbb{P}(\mathbb{1}_A = 1) = \mathbb{P}(A)$. □

Remarque : Si une variable aléatoire ne prend que les valeurs 0 et 1, on peut affirmer directement qu'elle suit une loi de Bernoulli, il ne manque que le paramètre p . Or,

$$p = \mathbb{P}(X = 1) = \mathbb{E}(X).$$

Ainsi, selon les cas, il suffit de calculer $\mathbb{P}(X = 1)$ ou $\mathbb{E}(X)$ pour donner le paramètre : il est inutile de donner $\mathbb{P}(X = 0)$!

c) Loi de Bernoulli avec Python

Pour une implémentation en Python, on commence par :

```
1 import numpy.random as rd
```

Supposons que $p \in]0; 1[$ a été implémenté en Python dans la variable p . Pour obtenir une réalisation d'une variable aléatoire de loi de $\mathcal{B}(p)$, conformément à ce que l'on a vu dans le paragraphe précédent, on peut utiliser la commande `U=rd.random()` qui renvoie un réel choisi uniformément entre 0 et 1. Si on pose $X=1$ lorsque $U < p$ et $X=0$ sinon, alors $X=1$ avec fréquence p et $X=0$ avec fréquence $1 - p$. Voici ce que l'on obtient :

```
1 if rd.random() < p:
2     X=1
3 else:
4     X=0
```

Mais, plus simplement, on peut utiliser la fonction :

```
1 X=rd.binomial(1, p)
```

Si il existe deux entiers naturels c et n tels que $p = \frac{c}{n}$, alors on peut aussi utiliser :

```
1 if rd.randint(1, n+1) <= c:
2     X=1
3 else:
4     X=0
```

Cette première possibilité, bien que plus compliquée au premier abord que la seconde, est préférable car on peut facilement l'adapter si on veut autre chose que des 0 et 1 ou si on veut plusieurs alternatives à l'expérience. On verra des exemples en TD.

4) Loi binomiale

a) Définition

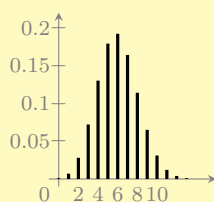
Il s'agit bien d'une loi de probabilité puisque, avec la formule du binôme de Newton, on vérifie que la somme des $\mathbb{P}(X = k)$ pour k allant de 0 à n , est égale à

$$(p + (1 - p))^n = 1.$$

Définition. Soient $n \in \mathbb{N}^*$ et $p \in]0; 1[$. On dit qu'une variable aléatoire réelle finie X sur Ω suit la loi de binomiale de paramètres n et p si et :

On note $X \hookrightarrow \mathcal{B}(n, p)$. Le paramètre p (resp. $q = 1 - p$) est appelé probabilité de succès (resp. d'échec).

Pour $n = 20$ et $p = 0,3$, on obtient le diagramme en bâtons :



Remarque : $\mathcal{B}(1, p)$ est la loi $\mathcal{B}(p)$.

b) Interprétation : succession d'épreuves de Bernoulli

Définition. Soit $p \in]0; 1[$. On appelle expérience (ou épreuve ou schéma) de Bernoulli de paramètre p toute expérience aléatoire n'ayant que deux issues possibles :

- l'une appelée succès et dont la probabilité de réalisation est p ,
- l'une appelée échec et dont la probabilité de réalisation est $q = 1 - p$.

Exemple : On lance une pièce de monnaie qui tombe sur pile avec probabilité $p \in]0; 1[$. On gagne le jeu si on tombe sur Pile. L'expérience est alors une épreuve de Bernoulli de probabilité de paramètre p .

Proposition. Soit $n \in \mathbb{N}^*$. On considère une épreuve de Bernoulli dont la probabilité de succès est $p \in]0; 1[$. Notons X la variable aléatoire comptant le nombre de succès dans n répétitions indépendantes de cette épreuve de Bernoulli. Alors X suit la loi binomiale de paramètres n et p .

Remarque : Avant de montrer cette proposition, soyons plus précis : si on répète n fois une même épreuve de Bernoulli de façon indépendante, quel espace probabilisé peut-on considérer ? On peut coder par exemple les succès par des 1 et les échecs par des 0 et donc modéliser cette expérience par l'espace probabilisé fini $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ avec $\Omega = \{0; 1\}^n$ et \mathbb{P} une probabilité telle que les événements S_i : « La $i^{\text{ème}}$ expérience est un succès », $i \in \llbracket 1; n \rrbracket$, sont mutuellement indépendants et de même probabilité p .

DÉMONSTRATION.

Nous allons voir dans la démonstration suivante que \mathbb{P} est alors uniquement déterminée : pour tout $\omega \in \Omega$,

$$\mathbb{P}(\{\omega\}) = p^k (1 - p)^{n-k},$$

où k est le nombre de 1 dans le n -uplet ω . La variable aléatoire X est alors bien définie sur Ω comme étant la fonction qui à $\omega \in \Omega$ associe le nombre de 1 dans le n -uplet ω .

□

Ainsi, pour montrer qu'une variable aléatoire X suit une loi binomiale, on a deux possibilités :

- Soit on calcule explicitement la loi de X : on montre qu'il existe $n \in \mathbb{N}^*$ et $p \in]0; 1[$ tels que $X(\Omega) = \llbracket 0; n \rrbracket$ et, pour tout $k \in \llbracket 0; n \rrbracket$,


$$\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

La variable aléatoire X suit alors la loi $\mathcal{B}(n, p)$.

- Soit on justifie que X compte le nombre de succès dans n répétitions indépendantes d'épreuves de Bernoulli de probabilité de succès p .

Il est impératif de justifier que les épreuves de Bernoulli sont indépendantes !

Exemples :

- On dispose d'une pièce de monnaie truquée de telle sorte que la probabilité qu'elle tombe sur Pile soit $p \in]0; 1[$. On lance $n \in \mathbb{N}^*$ fois la pièce successivement et on note X le nombre de fois où la pièce est tombée sur Pile. On peut supposer que les lancers successifs sont indépendants. La variable aléatoire X représente alors le nombre de succès dans n répétitions indépendantes d'épreuves de Bernoulli. Ainsi $X \leftrightarrow \mathcal{B}(n, p)$.  Raisonnement classique !
- On dispose d'une urne contenant r boules rouges et b boules bleues (avec $r \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$). On effectue n tirages successifs avec remise de boules dans l'urne et on note X le nombre de boules rouges obtenues. On peut supposer que les tirages successifs sont indépendants (car il y a remise). Tirer une boule rouge dans l'urne est une épreuve de Bernoulli de paramètre $p = \frac{r}{r+b}$. La variable X compte le nombre de succès dans n répétitions indépendantes de cette épreuve de Bernoulli. Ainsi $X \leftrightarrow \mathcal{B}\left(n, \frac{r}{r+b}\right)$.

c) Propriétés

Proposition. Soient $n \in \mathbb{N}^*$ et $p \in]0; 1[$. Si $X \leftrightarrow \mathcal{B}(n, p)$, alors

DÉMONSTRATION.

□

d) Loi binomiales avec Python

Pour une implémentation en Python, on commence par :

```
1 import numpy.random as rd
```

Supposons que $n \in \mathbb{N}^*$ et $p \in]0; 1[$ ont été implémentés en Python dans les variables n et p . Pour obtenir une réalisation d'une variable aléatoires de loi de $\mathcal{B}(n, p)$,

- on peut utiliser

```
1 X=rd.binomial(n,p)
```

- on peut utiliser simuler n variables de loi $\mathcal{B}(p)$ avec la `rd.random()` (cf. paragraphe précédent) et les sommer. En effet on peut considérer que les différents appels de cette fonction sont des réalisations de variables aléatoires mutuellement indépendants. Ainsi les sommer revient à compter le nombre de 1, donc compter le nombre de succès.

Ajouter une option `N` (l'implémentation d'un entier naturel N) à cette commande fournit une liste (ou plutôt un tableau unidimensionnel, cf. chapitre 19) de N réalisations indépendantes de variables aléatoires de la loi binomiale.

Cette deuxième possibilité, bien que plus compliquée au premier abord, est préférable car on peut facilement l'adapter si on somme des succès d'expériences non indépendantes ou non identiques. On verra des exemples en TP.

On utilise alors :

```
1 X=0
2 for k in range(n):
3     if rd.random()<p:
4         X=X+1
```

- on peut utiliser la commande `U=rd.random(n)` qui renvoie un vecteur contenant n réels choisis uniformément entre 0 et 1. La commande `U<p` renvoie un vecteur contenant des `True` aux coordonnées de U qui sont inférieurs à p et des `False` aux autres. Il suffit de sommer les coordonnées de `U<p` pour compter le nombre de `True` (le nombre de succès). Ainsi :

```
1 np.sum(rd.random(n)<p)
```

contient une réalisation d'une variable aléatoire de loi $\mathcal{B}(n, p)$.

IV Du hasard avec un ordinateur ?

Dans ce chapitre et le précédent, nous avons plusieurs fois simulé des variables aléatoires à l'aide de Python. Est-ce bien sérieux ?

Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.

John von Neumann

Simuler une variable aléatoire réelle d'une loi donnée à l'aide d'un ordinateur consiste à construire un nombre réel que l'on peut assimiler à une réalisation $X(\omega)$ d'une variable aléatoire X ayant cette loi.

Ce procédé repose en général sur deux étapes :

- Simuler des variables aléatoires indépendantes de loi uniforme sur $]0; 1[$.
- Réaliser des opérations sur les simulations afin d'obtenir la réalisation d'une variable aléatoire de loi voulue.

La première étape pose des problèmes à la fois conceptuels et pratiques... notamment comment demander à un ordinateur de faire un choix aléatoire, alors que celui-ci est programmé pour n'effectuer qu'une suite d'instructions déterministes ? Aucune solution totalement satisfaisante n'a été proposée à ce jour. La plupart des générateurs sont fondés sur des calculs de congruences sur des grands nombres de façon déterministe (mais que l'on peut initialiser avec l'horloge de l'ordinateur pour ajouter une dose de hasard). On parle alors de générateurs de nombres pseudo-aléatoires : les nombres générés possèdent les propriétés apparentes d'une suite de variables aléatoires indépendantes et de loi uniforme sur $]0; 1[$:

- La suite de nombres se comporte de façon chaotique, de sorte que les éléments successifs de cette suite de nombres semblent imprévisibles. Plus précisément, pour tout $k \in \mathbb{N}^*$, la connaissance des $k - 1$ premiers termes de la suite ne semble pas nous donner d'information sur le $k^{\text{ième}}$ terme.
- La moyenne des premiers nombres de la suite semble se concentrer asymptotiquement (quand le nombre de termes moyennés tend vers $+\infty$) vers une quantité fixe.

Presque toutes les fonctions du module dépendent de la fonction de base `random()`, qui génère un réel dans $]0; 1[$. Python utilise l'algorithme *Mersenne Twister* comme générateur de base. C'est l'un des générateurs de nombres aléatoires les plus largement testés qui existent. Cependant, étant complètement déterministe, il n'est pas adapté à tous les usages.

John von Neumann (1903-1957) est un mathématicien et physicien américano-hongrois.

Il existe plusieurs générateurs basés sur des phénomènes physiques (et certains sont brevetés et disponibles dans le commerce). Ils reposent par exemple sur des capteurs de bruit thermique dans les résistances de circuits électroniques, ou sur d'autres mécanismes basés sur la physique quantique, etc. Ces générateurs contiennent du vrai hasard mais ils sont encombrants, pas toujours fiables, pas facilement reproductibles et ne sont pas accessibles à une analyse mathématique rigoureuse.

Notamment il est totalement inadapté à des fins cryptographiques