HEC/ESSEC I 2020

On s'intéresse dans ce sujet au problème de la *double dépense* de *bitcoins* par un groupe d'individus mal intentionnés.
On rappelle que le bitcoin est une monnaie virtuelle dont l'utilisation pour des transactions est associée à une structure unique appelée *blockchain*, partagée sur le réseau des usagers de cette monnaie et ayant pour but de sécuriser ces transactions.
La modélisation étudiée ne nécessite pas de connaissances particulières sur le *bitcoin* et la *blockchain*.

Partie I - Deux résultats généraux

On démontre dans cette partie deux résultats préliminaires, aux questions ***5.*** et ***6***. Ces résultats seront utilisés dans la suite du sujet et pourront être admis.

Calcul d'une probabilité

Soient X et Y deux variables aléatoires sur un espace probabilisé, à densité et indépendantes.
On note F_X et F_Y les fonctions de répartition de X et Y.
On suppose que Y est à valeurs positives et possède une densité f_Y dont la restriction à $[0,+\infty[$ est continue sur cet intervalle.
Pour tout $x \in \mathbb{R}_+$, on pose : $H(x) = \mathbb{P}(\,[X \leqslant Y] \cap [Y \leqslant x]\,)$.

1. a) Montrer que H est une fonction croissante sur $\mathbb{R}_+$ qui admet une limite finie en $+\infty$.

Démonstration.

- Soit $(x, y) \in \mathbb{R}_+ \times \mathbb{R}_+$.

$$\begin{array}{lrcl} \text{On suppose} & x & \leqslant & y \\ \text{on a alors} & [Y \leqslant x] & \subset & [Y \leqslant y] \\ \text{donc} & [X \leqslant Y] \cap [Y \leqslant x] & \subset & [X \leqslant Y] \cap [Y \leqslant y] \\ \text{donc} & \underbrace{\mathbb{P}\big(\,[X \leqslant Y] \cap [Y \leqslant x]\,\big)}_{=H(x)} & \leqslant & \underbrace{\mathbb{P}\big(\,[X \leqslant Y] \cap [Y \leqslant y]\,\big)}_{=H(y)} \end{array}$$

$$\boxed{\text{On en conclut que la fonction } H \text{ est croissante sur } \mathbb{R}_+.}$$

Commentaire

- La seule difficulté de cette question est de connaître la définition de croissance d'une fonction. Pour les fonctions dérivables, la propriété de croissance est souvent obtenue par la caractérisation à l'aide du signe de la dérivée. Rappelons cependant que la définition de la croissance n'utilise pas de propriété de régularité de la fonction.
- Démontrons formellement l'inclusion : $[Y \leqslant x] \;\subset\; [Y \leqslant y]$.
  Soit $\omega \in \Omega$. Supposons $\omega \in [Y \leqslant x]$.
  On a alors $Y(\omega) \leqslant x$ et ainsi :
  $$Y(\omega) \leqslant x \leqslant y$$
  On en conclut : $\omega \in [Y \leqslant y]$.

- La fonction H est :
  - $\times$ croissante sur $\mathbb{R}_+$.
  - $\times$ majorée. En effet, pour tout $x \in \mathbb{R}$, $\mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant x] \big) \leqslant 1$.

$$\boxed{\text{On en déduit, par le théorème de la limite monotone, que la fonction admet une limite finie en } +\infty.}$$

$\square$

b) En utilisant la suite $\big(H(n)\big)_{n\in\mathbb{N}}$, démontrer : $\lim\limits_{x\to+\infty} H(x) = \mathbb{P}(\,[X \leqslant Y]\,)$.
Que vaut $H(0)$?

Démonstration.
On note $(\Omega, \mathscr{A}, \mathbb{P})$ l'espace probabilisé évoqué dans l'énoncé.

- Démontrons tout d'abord : $\Omega = \bigcup\limits_{k=0}^{+\infty} [Y \leqslant k]$. On procède par double inclusion.

($\subset$) Soit $\omega \in \Omega$. Notons $m = \lceil Y(\omega) \rceil$. On a alors :

$$Y(\omega) \leqslant \lceil Y(\omega) \rceil = m$$

Ainsi : $\omega \in [Y \leqslant m] \ \subset \ \bigcup\limits_{k=0}^{+\infty} [Y \leqslant k]$.

$$\boxed{\Omega \ \subset \ \bigcup_{k=0}^{+\infty} [Y \leqslant k]}$$

($\supset$) Comme pour tout $k \in \mathbb{N}$, $[Y \leqslant k] \in \mathscr{A}$, alors : $\bigcup\limits_{k=0}^{+\infty} [Y \leqslant k] \in \mathscr{A}$.

$$\boxed{\text{En particulier : } \bigcup_{k=0}^{+\infty} [Y \leqslant k] \ \subset \ \Omega.}$$

- On en déduit alors :

$$\begin{array}{rcl} [X \leqslant Y] & = & [X \leqslant Y] \cap \left(\bigcup\limits_{k=0}^{+\infty} [Y \leqslant k] \right) \\ & = & \bigcup\limits_{k=0}^{+\infty} \Big([X \leqslant Y] \cap [Y \leqslant k] \Big) \end{array}$$

$$\begin{array}{rcll} \text{Finalement } \ \mathbb{P}\big([X \leqslant Y] \big) & = & \mathbb{P}\left(\bigcup\limits_{k=0}^{+\infty} \Big([X \leqslant Y] \cap [Y \leqslant k] \Big) \right) & \\ & = & \lim\limits_{N\to+\infty} \mathbb{P}\left(\bigcup\limits_{k=0}^{N} \Big([X \leqslant Y] \cap [Y \leqslant k] \Big) \right) & \textit{(d'après le théorème de la limite monotone)} \\ & = & \lim\limits_{N\to+\infty} \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant N] \big) & \textit{(car } \big([X \leqslant Y] \cap [Y \leqslant k] \big)_{k\in\mathbb{N}} \textit{ est une suite croissante d'événements)} \\ & = & \lim\limits_{N\to+\infty} H(N) & \\ & = & \lim\limits_{x\to+\infty} H(x) & \textit{(car, d'après la question précédente, } H \textit{ admet une limite en } +\infty\textit{)} \end{array}$$

$$\boxed{\text{On a bien : } \lim_{x\to+\infty} H(x) \ = \ \mathbb{P}\big([X \leqslant Y] \big).}$$

Commentaire

- Cette question est à juger comme difficile car elle exige beaucoup d'initiatives de la part du candidat. Il y a là un saut de difficulté par rapport à la question précédente.
- On n'a pas détaillé ci-dessus le fait que $\big([X \leqslant Y] \cap [Y \leqslant k]\big)_{k\in\mathbb{N}}$ est une suite croissante d'événements. C'est une application directe de la question précédente. En effet, on a démontré que pour tout $(x,y) \in \mathbb{R}_+ \times \mathbb{R}_+$:

$$x \leqslant y \ \Rightarrow\ [X \leqslant Y] \cap [Y \leqslant x] \subset [X \leqslant Y] \cap [Y \leqslant y]$$

Soit $n \in \mathbb{N}$. En choisissant $x = n$ et $y = n+1$ on obtient le résultat souhaité, à savoir :

$$[X \leqslant Y] \cap [Y \leqslant n] \subset [X \leqslant Y] \cap [Y \leqslant n+1]$$

- Par définition :

$$\begin{array}{rcll} H(0) & = & \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant 0]\big) & \\ & \leqslant & \mathbb{P}\big([Y \leqslant 0]\big) & \textit{(car } [X \leqslant Y] \cap [Y \leqslant 0] \subset [Y \leqslant 0]\textit{)} \\ & = & \mathbb{P}\big([Y < 0]\big) & \textit{(car } Y \textit{ est une v.a.r. à densité)} \\ & = & \mathbb{P}(\varnothing) & \textit{(car } Y \textit{ est à valeurs positives)} \\ & = & 0 & \end{array}$$

$$\boxed{H(0) = 0}$$

□

2. Soit (u,v) un couple de réels positifs tels que : $u < v$.

a) Montrer : $H(v) - H(u) = \mathbb{P}(\,[X \leqslant Y] \cap [u < Y \leqslant v]\,)$. Puis :

$$F_X(u)\ \frac{F_Y(v) - F_Y(u)}{v-u} \ \leqslant\ \frac{H(v)-H(u)}{v-u} \ \leqslant\ F_X(v)\ \frac{F_Y(v) - F_Y(u)}{v-u}$$

Démonstration.

- Il s'agit de démontrer :

$$\begin{array}{rcl} H(v) & = & H(u) + \mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v]\big) \\ & = & \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant u]\big) + \mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v]\big) \end{array}$$

où $H(v) = \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant v]\big)$. Pour ce faire, démontrons :

$$[X \leqslant Y] \cap [Y \leqslant v] \ = \ [X \leqslant Y] \cap [Y \leqslant u] \ \cup\ [X \leqslant Y] \cap [u < Y \leqslant v]$$

ou plus simplement : $[Y \leqslant v] \ = \ [Y \leqslant u] \ \cup\ [u < Y \leqslant v]$.

Commentaire

L'énoncé demande ici de démontrer une égalité entre probabilités de différents événements. Il est classique, pour ce faire, d'agir comme suit :

1) on démontre tout d'abord une égalité entre les événements concernés.

2) on applique alors l'application probabilité $\mathbb{P}$ de part et d'autre de l'égalité. On conclut à l'aide des propriétés de $\mathbb{P}$.

Il est à noter que l'égalité entre événements à démontrer s'obtient évidemment à partir de l'égalité entre probabilités à démontrer. Pour ce faire, on aura en tête les triptyques :

union / incompatibilité / somme	intersection / indépendance / produit

On procède par double inclusion. Soit $\omega \in \Omega$.

($\subset$) Supposons $\omega \in [Y \leqslant v]$. Ainsi : $Y(\omega) \leqslant v$.
Deux cas se présentent alors :

× si $Y(\omega) \leqslant u$ alors $\omega \in [Y \leqslant u]$.

× si NON$(Y(\omega) \leqslant u)$ alors $Y(\omega) > u$.
Comme on sait de plus : $Y(\omega) \leqslant v$, on en conclut : $\omega \in [u < Y \leqslant v]$.

$$\boxed{\text{Finalement, on a bien : } \omega \in [Y \leqslant u] \cup [u < Y \leqslant v].}$$

($\supset$) Supposons $\omega \in [Y \leqslant u] \cup [u < Y \leqslant v]$. Ainsi : $Y(\omega) \leqslant u$ OU $u < Y(\omega) \leqslant v$.
Deux cas se présentent alors :

× si $Y(\omega) \leqslant u$ alors, comme $u < v$, on a $Y(\omega) \leqslant u < v$ et ainsi $\omega \in [Y \leqslant v]$.

× si NON$(Y(\omega) \leqslant u)$ alors, comme $Y(\omega) \leqslant u$ OU $u < Y(\omega) \leqslant v$, on a forcément : $u < Y(\omega) \leqslant v$. En particulier : $Y(\omega) \leqslant v$, et donc : $\omega \in [Y \leqslant v]$.

$$\boxed{\text{Finalement, on a bien : } \omega \in [Y \leqslant v].}$$

$$\boxed{\text{On en conclut : } [Y \leqslant v] \ = \ [Y \leqslant u] \ \cup \ [u < Y \leqslant v].}$$

Commentaire

- La démonstration de cette égalité a été développée ici afin d'illustrer la méthode. Cependant, cette égalité n'étant pas mentionnée dans l'énoncé, il est probable que l'écrire suffise à récupérer une grande partie des points alloués à la question.
- L'égalité initiale entre probabilités fait apparaître une différence entre probabilités de certains événements. Une telle égalité est généralement la conséquence d'une égalité entre événements où apparaît une différence ensembliste d'événements. Plus précisément, on pourrait mettre ici en place le raisonnement suivant :

$$[Y \leqslant v] \ \backslash \ [Y \leqslant u] = [u < Y \leqslant v] \quad \Rightarrow \quad \mathbb{P}\big([Y \leqslant v]\big) - \mathbb{P}\big([Y \leqslant u]\big) = \mathbb{P}\big([u < Y \leqslant v]\big)$$

Profitons-en pour rappeler que pour tout événement $(A, B) \in \mathscr{A} \times \mathscr{A}$, on a :

$$\mathbb{P}(A \setminus B) \ = \ \mathbb{P}\big(A \setminus A \cap B\big) \ = \ \mathbb{P}(A) - \mathbb{P}(A \cap B)$$

Afin de faciliter la résolution de cette question, on a préféré ici réordonner les termes de l'égalité de sorte à faire apparaître une somme entre probabilités d'événements. Une telle égalité est issue d'une réunion d'événements (le plus souvent incompatibles ou à tout le moins d'intersection négligeable) ce qui permet d'éviter d'avoir à gérer une différence ensembliste. Ce qui amène ici au raisonnement suivant :

$$[Y \leqslant u] \cup [u < Y \leqslant v] = [Y \leqslant v] \quad \Rightarrow \quad \mathbb{P}\big([Y \leqslant u]\big) + \mathbb{P}\big([u < Y \leqslant v]\big) = \mathbb{P}\big([Y \leqslant v]\big)$$

- Ainsi $\qquad [Y \leqslant v] \ = \ [Y \leqslant u] \ \cup \ [u < Y \leqslant v]$

et
$$\begin{aligned}[X \leqslant Y] \cap [Y \leqslant v] &= [X \leqslant Y] \cap \Big([Y \leqslant u] \ \cup \ [u < Y \leqslant v]\Big) \\ &= [X \leqslant Y] \cap [Y \leqslant u] \ \cup \ [X \leqslant Y] \cap [u < Y \leqslant v]\end{aligned}$$

enfin
$$\begin{aligned}\mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant v]\big) &= \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant u] \ \cup \ [X \leqslant Y] \cap [u < Y \leqslant v]\big) \\ &= \mathbb{P}\big([X \leqslant Y] \cap [Y \leqslant u]\big) + \mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v]\big)\end{aligned}$$

La dernière égalité est obtenue par incompatibilité des deux événements considérés. En effet :

$$[Y \leqslant u] \cap [u < Y \leqslant v] = \varnothing$$

et ainsi : $[X \leqslant Y] \cap [Y \leqslant u] \ \cap \ [X \leqslant Y] \cap [u < Y \leqslant v] = \varnothing$.

$$\boxed{\text{On a bien : } H(v) - H(u) = \mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v] \big).}$$

- Remarquons alors :

$$[X \leqslant Y] \cap [u < Y \leqslant v] \ \subset \ [X \leqslant v] \cap [u < Y \leqslant v]$$

Démontrons cette inclusion.

Soit $\omega \in \Omega$. Supposons $\omega \in [X \leqslant Y] \cap [u < Y \leqslant v]$.

On en déduit	$\omega \in [X \leqslant Y]$ et $\omega \in [u < Y \leqslant v]$.
Autrement dit	$X(\omega) \leqslant Y(\omega)$ et $u < Y(\omega) \leqslant v$.
En particulier	$X(\omega) \leqslant Y(\omega) \leqslant v$, ce qui s'écrit : $\omega \in [X \leqslant v]$.
Finalement	$\omega \in [X \leqslant v] \cap [u < Y \leqslant v]$.

$$\boxed{[X \leqslant Y] \cap [u < Y \leqslant v] \ \subset \ [X \leqslant v] \cap [u < Y \leqslant v]}$$

En particulier, par croissance de l'application $\mathbb{P}$, on obtient :

$$\mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v] \big) \ \leqslant \ \mathbb{P}\big([X \leqslant v] \cap [u < Y \leqslant v] \big)$$

- On a alors :

$$\begin{aligned} H(v) - H(u) &= \mathbb{P}\big([X \leqslant Y] \cap [u < Y \leqslant v] \big) \\ &\leqslant \mathbb{P}\big([X \leqslant v] \cap [u < Y \leqslant v] \big) \\ &= \mathbb{P}\big([X \leqslant v] \big) \times \mathbb{P}\big([u < Y \leqslant v] \big) && \textit{(car les v.a.r. } X \textit{ et } Y \textit{ sont indépendantes)} \\ &= F_X(v) \times \big(F_Y(v) - F_Y(u) \big) \end{aligned}$$

$$\boxed{\text{En divisant par } v - u > 0 \text{, on obtient bien : } \dfrac{H(v) - H(u)}{v - u} \leqslant F_X(v) \ \dfrac{F_Y(v) - F_Y(u)}{v - u}.}$$

- On raisonne de même pour l'inégalité de gauche. On établit initialement l'égalité :

$$[X \leqslant u] \cap [u < Y \leqslant v] \ \subset \ [X \leqslant Y] \cap [u < Y \leqslant v]$$

Soit $\omega \in \Omega$. Supposons $\omega \in [X \leqslant u] \cap [u < Y \leqslant v]$.

On en déduit	$\omega \in [X \leqslant u]$ et $[u < Y \leqslant v]$.
Autrement dit	$X(\omega) \leqslant u$ et $u < Y(\omega) \leqslant v$.
En particulier	$X(\omega) \leqslant u < Y(\omega)$, ce qui démontre : $\omega \in [X \leqslant Y]$.
Finalement	$\omega \in [X \leqslant Y] \cap [u < Y \leqslant v]$.

On conclut alors, par un raisonnement similaire au précédent :

$$\boxed{F_X(u) \ \dfrac{F_Y(v) - F_Y(u)}{v - u} \ \leqslant \ \dfrac{H(v) - H(u)}{v - u}.}$$

Commentaire

- Cette question peut sembler difficile car elle demande de nouveau une prise d'initiative importante. En particulier, il peut paraître difficile de penser à établir les inclusions entre événements qui permettent d'obtenir le résultat final. Il est conseillé d'opérer par rétro-ingénierie : on part du résultat final pour essayer d'en déduire le résultat intermédiaire qui permettra de conclure. Pour ce faire, on commence généralement par opérer par équivalence afin de pouvoir écrire le résultat final sous une forme plus simple. Par exemple, ici, on pouvait procéder comme suit :

$$F_X(u)\ \frac{F_Y(v)-F_Y(u)}{v-u} \ \leqslant\ \frac{H(v)-H(u)}{v-u}$$

$$\Leftrightarrow\ F_X(u)\ \big(F_Y(v)-F_Y(u)\big) \ \leqslant\ H(v)-H(u) \qquad \textit{(car } v-u>0\textit{)}$$

$$\Leftrightarrow\ \mathbb{P}\big(\,[X\leqslant u]\,\big)\ \mathbb{P}\big(\,[u<Y\leqslant v]\,\big) \ \leqslant\ H(v)-H(u) \qquad \textit{(par définition de } F_X \textit{ et propriété du cours)}$$

$$\Leftrightarrow\ \mathbb{P}\big(\,[X\leqslant u]\,\big)\ \mathbb{P}\big(\,[u<Y\leqslant v]\,\big) \ \leqslant\ \mathbb{P}\big(\,[X\leqslant Y]\cap[u<X\leqslant v]\,\big)$$

$$\Leftrightarrow\ \mathbb{P}\big(\,[X\leqslant u]\cap[u<Y\leqslant v]\,\big) \ \leqslant\ \mathbb{P}\big(\,[X\leqslant Y]\cap[u<X\leqslant v]\,\big) \qquad \textit{(car } X \textit{ et } Y \textit{ sont indépendantes)}$$

  Une inégalité entre probabilité est généralement obtenue par une inclusion entre événements. Il doit donc être naturel de penser à établir une telle inclusion. Notons enfin que l'on perd ici l'équivalence : l'inclusion entre événements **suffit** à démontrer l'inégalité entre probabilités.

- Au passage, soulignons de nouveau l'importance du triptyque :

intersection / indépendance / produit

  Lorsqu'une égalité (ou inégalité) à démontrer comporte un produit de probabilités, il est naturel de penser que ce produit est obtenu comme probabilité d'une intersection d'événements.

- La difficulté d'un sujet se mesure en grande partie à la manière dont chaque question est découpée en sous-questions. Moins il y a de sous-questions, plus le candidat doit prendre des initiatives. Ainsi, un sujet de type `TOP3` proposera un découpage en sous-questions bien moins détaillé qu'un sujet `TOP5`. Le même thème amène à un traitement différent lorsqu'il est abordé dans un sujet du `TOP3` ou du `TOP5`. En guise d'illustration, on peut noter que la propriété qu'il s'agit de démontrer dans cette **Partie I**, à savoir :

$$\mathbb{P}\big(\,[X\leqslant Y]\,\big) \ =\ \int_0^{+\infty} F_X(t)\, f_Y(t)\ dt$$

  (sous les hypothèses de l'énoncé)

  est aussi utilisée (elle est admise) dans l'exercice 1 de l'énoncé `EML 2019`. □

b) En déduire que pour tout $x\in\mathbb{R}_+$, H est dérivable en x et : $H'(x)=F_X(x)\,f_Y(x)$.

Démonstration.

- La fonction f_Y est continue sur l'intervalle $[0,+\infty[$.
  On en déduit que la fonction F_Y est de classe $\mathcal{C}^1$ sur cet intervalle.

En particulier, F_Y est dérivable en tout point de $\mathbb{R}_+$.

  On en déduit que pour tout $x_0\in\mathbb{R}_+$: $\lim\limits_{x\to x_0} \dfrac{F_Y(x)-F_Y(x_0)}{x-x_0} = F_Y'(x_0) = f_Y(x_0)$.

- Soit $x_0 \in \mathbb{R}_+$. Rappelons tout d'abord, que d'après la question précédente, pour tout $x > x_0$:

$$F_X(x_0)\ \frac{F_Y(x) - F_Y(x_0)}{x - x_0} \ \leqslant\ \frac{H(x) - H(x_0)}{x - x_0} \ \leqslant\ F_X(x)\ \frac{F_Y(x) - F_Y(x_0)}{x - x_0}$$

(résultat de la question précédente avec $v = x$ et $u = x_0$)

On a :

$\times$ $\lim\limits_{\substack{x \to x_0 \\ x > x_0}} F_X(x_0) = F_X(x_0)$,

et $\lim\limits_{\substack{x \to x_0 \\ x > x_0}} \dfrac{F_Y(x) - F_Y(x_0)}{x - x_0} = F_Y'(x_0) = f_Y(x_0)$ car F_Y est dérivable en x_0.

$\times$ $\lim\limits_{\substack{x \to x_0 \\ x > x_0}} F_X(x) = F_X(x_0)$ car F_X est continue (à droite) en x_0,

et $\lim\limits_{\substack{x \to x_0 \\ x > x_0}} \dfrac{F_Y(x) - F_Y(x_0)}{x - x_0} = F_Y'(x_0) = f_Y(x_0)$ car F_Y est dérivable en x_0.

On en déduit, par théorème d'encadrement que la fonction H admet une limite à droite en x_0, donnée par :

$$\lim_{\substack{x \to x_0 \\ x > x_0}} \frac{H(x) - H(x_0)}{x - x_0} \ =\ H_d'(x_0) \ =\ F_X(x_0)\ f_Y(x_0)$$

En utilisant de nouveau le résultat de la question précédente, on obtient, pour tout $x < x_0$:

$$F_X(x)\ \frac{F_Y(x_0) - F_Y(x)}{x_0 - x} \ \leqslant\ \frac{H(x_0) - H(x)}{x_0 - x} \ \leqslant\ F_X(x_0)\ \frac{F_Y(x_0) - F_Y(x)}{x_0 - x}$$

(résultat de la question précédente avec $v = x_0$ et $u = x$)

Ce qui s'écrit (en multipliant chaque quotient par $\frac{-1}{-1}$) :

$$F_X(x)\ \frac{F_Y(x) - F_Y(x_0)}{x - x_0} \ \leqslant\ \frac{H(x) - H(x_0)}{x - x_0} \ \leqslant\ F_X(x_0)\ \frac{F_Y(x) - F_Y(_0)}{x - x_0}$$

On en déduit alors, en utilisant de nouveau par le théorème d'encadrement, que la fonction H admet une limite à gauche en x_0, donnée par :

$$\lim_{\substack{x \to x_0 \\ x < x_0}} \frac{H(x) - H(x_0)}{x - x_0} \ =\ H_g'(x_0) \ =\ F_X(x_0)\ f_Y(x_0)$$

- Finalement, la fonction H est dérivable à droite et à gauche en x_0. De plus :

$$H_g'(x_0) \ =\ F_X(x_0)\ f_Y(x_0) \ =\ H_d'(x_0)$$

$\boxed{\text{Ainsi, pour tout } x_0 \in \mathbb{R}_+, \text{ la fonction } H \text{ est dérivable en } x_0 \text{ et } H'(x_0) = F_X(x_0)\ f_Y(x_0).}$ $\square$

c) En conclure que pour tout x réel positif : $H(x) = \displaystyle\int_0^x F_X(t)\, f_Y(t)\ dt$.

Démonstration.
Dans les questions précédentes, on a établi que la fonction H :

× est dérivable sur $\mathbb{R}_+$,

× admet pour dérivée sur $\mathbb{R}_+$ la fonction $h : t \mapsto F_X(t)\, f_Y(t)$,

× vérifie : $H(0) = 0$.

On en déduit que la fonction H est la primitive sur $\mathbb{R}_+$ et qui s'annule en 0 de la fonction h.

En conclusion, la fonction H est telle que :

$$\forall x \in \mathbb{R}_+,\ H(x) = \int_0^x h(t)\ dt = \int_0^x F_X(t)\, f_Y(t)\ dt.$$

Commentaire

On est confronté ici à une question bilan qui consiste simplement à rappeler puis utiliser certains résultats précédents. Ces résultats étant fournis par l'énoncé, cette question peut être traitée même si les questions précédentes ne l'ont pas été. Il faut s'habituer à repérer ces questions qui permettent de prendre facilement des points. □

3. Démontrer : $\mathbb{P}(\,[X \leqslant Y]\,) = \displaystyle\int_0^{+\infty} F_X(t)\, f_Y(t)\ dt$.

Démonstration.
Il suffit de remarquer :

$$\begin{array}{rcll} \mathbb{P}\big(\,[X \leqslant Y]\,\big) & = & \displaystyle\lim_{x\to+\infty} H(x) & \textit{(d'après la question } \textbf{\textit{1.}}\textit{)} \\ & = & \displaystyle\lim_{x\to+\infty} \int_0^x F_X(t)\, f_Y(t)\ dt & \textit{(d'après la question } \textbf{\textit{2.c)}}\textit{)} \\ & = & \displaystyle\int_0^{+\infty} F_X(t)\, f_Y(t)\ dt & \end{array}$$

Rappelons que l'on a démontré, en question ***1.***, que la fonction $x \mapsto \displaystyle\int_0^x F_X(t)\, f_Y(t)\ dt$ admet une limite finie en $+\infty$ (égale à $\mathbb{P}\big(\,[X \leqslant Y]\,\big)$). Cela signifie, par définition, que l'intégrale impropre $\displaystyle\int_0^{+\infty} F_X(t)\, f_Y(t)\ dt$ est convergente. Cela justifie la dernière égalité.

$$\boxed{\mathbb{P}(\,[X \leqslant Y]\,) = \int_0^{+\infty} F_X(t)\, f_Y(t)\ dt}$$

Commentaire

- Il s'agit là encore d'une question bilan qui ne présente pas de difficulté particulière. Cela démontre au passage qu'il n'y a pas forcément de progression croissante de la difficulté des questions dans les énoncés des épreuves de concours. En conséquence, même si on ne parvient pas à traiter plusieurs questions d'affilée, il ne faut pas pour autant passer toute la **Partie I**. Il faut au contraire s'atteler à essayer de traiter les questions qui suivent, ce qui permettra à terme de tomber sur une question dont la résolution est plus simple.

Commentaire

- Dans l'épreuve `EML 2019`, on admet l'égalité :

$$\mathbb{P}\big(\,[X \leqslant Y]\,\big) = \int_0^{+\infty} F_X(t)\, f_Y(t)\; dt$$

Il est par contre demandé de justifier la convergence de cette intégrale à l'aide d'un théorème de comparaison. Rappelons cette démonstration :

× $\forall t \in [0, +\infty[,\ 0 \ \leqslant\ F_X(t)\, f_Y(t) \ \leqslant\ f_Y(t)$

En effet, pour tout $t \in [0, +\infty[$, $0 \ \leqslant\ F_X(t) \ \leqslant\ 1$ et l'inégalité souhaitée est alors obtenue par multiplication par $f_Y(t) \geqslant 0$.

× l'intégrale $\displaystyle\int_0^{+\infty} f_Y(t)\; dt$ est convergente (et vaut 1) en tant que moment d'ordre 0 de la v.a.r. Y. En effet, comme Y est à valeurs positives, f_Y est nulle en dehors de $[0, +\infty[$ et :

$$\mathbb{E}(Y^0) \ = \ \int_{-\infty}^{+\infty} f_Y(t)\; dt \ = \ \int_0^{+\infty} f_Y(t)\; dt$$

Ainsi, par critère de comparaison d'intégrales généralisées de fonctions continues positives, l'intégrale impropre $\displaystyle\int_0^{+\infty} F_X(t)\, f_Y(t)\; dt$ est convergente.

- On pouvait aussi opérer à l'aide d'un équivalent. En effet, comme : $\lim\limits_{t \to +\infty} F_X(t) = 1$, on a :

$$F_X(t)\, f_Y(t) \underset{t \to +\infty}{\sim} f_Y(t)$$

□

4. En utilisant la fonction $K : x \mapsto \mathbb{P}(\,[X < Y] \cap [Y \leqslant x]\,)$, on montrerait de même et nous l'admettrons :

$$\mathbb{P}(\,[X < Y]\,) \ = \ \int_0^{+\infty} F_X(t)\, f_Y(t)\; dt \ = \ \mathbb{P}(\,[X \leqslant Y]\,)$$

Que peut-on en déduire pour $\mathbb{P}(\,[X = Y]\,)$?

Démonstration.

- Remarquons tout d'abord :

$$[X \leqslant Y] \ = \ [X < Y] \cup [X = Y]$$

- On en déduit :

$$\begin{array}{rcll} \mathbb{P}\big(\,[X \leqslant Y]\,\big) & = & \mathbb{P}\big(\,[X < Y] \cup [X = Y]\,\big) & \\ & = & \mathbb{P}\big(\,[X < Y]\,\big) + \mathbb{P}\big(\,[X = Y]\,\big) & \textit{(car les événements } [X < Y] \\ & & & \textit{et } [X = Y] \textit{ sont incompatibles)} \end{array}$$

$$\boxed{\text{Ainsi : } \mathbb{P}\big(\,[X = Y]\,\big) = \mathbb{P}\big(\,[X \leqslant Y]\,\big) - \mathbb{P}\big(\,[X < Y]\,\big) = 0.}$$

□

5. *Application aux lois exponentielles*
On suppose que U et V sont deux variables aléatoires indépendantes suivant des lois exponentielles de paramètres respectifs λ et μ, réels strictement positifs.
Soit θ un réel positif ou nul.

a) Déterminer la fonction de répartition de la variable aléatoire $X = U - \theta$.

Démonstration.

- Notons $h_\theta : x \mapsto x - \theta$ de sorte que $X = h_\theta(U)$.
Comme $U \hookrightarrow \mathcal{E}(\lambda)$, on **considère** $X(\Omega) = [0, +\infty[$. On en déduit :

$$\begin{array}{rcll} X(\Omega) & = & \big(h_\theta(U)\big)(\Omega) & \\ & = & h_\theta\big(U(\Omega)\big) & \\ & = & h_\theta\big([0,+\infty[\big) & \\ & = & [h_\theta(0), \lim\limits_{x\to+\infty} h_\theta(x)[& \textit{(car la fonction } h_\theta \textit{ est continue et strictement croissante sur } [0,+\infty[\textit{)} \\ & = & [-\theta, +\infty[& \end{array}$$

$$\boxed{\text{Et ainsi : } X(\Omega) = [-\theta, +\infty[.}$$

- Soit $x \in \mathbb{R}$. Deux cas se présentent :
  - × si $x < -\theta$, alors $[X \leqslant x] = \varnothing$ car $X(\Omega) = [-\theta, +\infty[$. Donc :
$$F_X(x) = \mathbb{P}\big(\,[X \leqslant x]\,\big) = \mathbb{P}(\varnothing) = 0$$
  - × si $x \geqslant -\theta$, alors :
$$\begin{array}{rcll} F_X(x) & = & \mathbb{P}\big(\,[X \leqslant x]\,\big) & \\ & = & \mathbb{P}\big(\,[U - \theta \leqslant x]\,\big) & \\ & = & \mathbb{P}\big(\,[U \leqslant x + \theta]\,\big) & \\ & = & 1 - \exp\big(-\lambda\,(x+\theta)\big) & \textit{(car } X \hookrightarrow \mathcal{E}(\lambda) \textit{ et } x+\theta \geqslant 0\textit{)} \end{array}$$

$$\boxed{\text{On obtient finalement : } F_X : x \mapsto \left\{ \begin{array}{cl} 0 & \text{si } x < -\theta \\ 1 - \mathrm{e}^{-\lambda\,\theta}\,\mathrm{e}^{-\lambda\,x} & \text{si } x \geqslant -\theta \end{array} \right. .}$$

Commentaire

- Cette question consiste à déterminer la loi de Y, transformée de la v.a.r. X. Ce type de question est extrêmement fréquent dans les sujets traitant de v.a.r. à densité. Leur résolution ne présente aucune difficulté majeure. Il s'agit simplement de se référer à la rédaction usuelle.
- En particulier, il faut savoir déterminer la loi d'une transformée affine, du carré et de la partie entière d'une v.a.r. à densité X. Cela fait partie du bagage culturel mathématique nécessaire avant d'affronter les écrits de concours.
- Il faut ajouter à ce bagage la détermination de la loi du minimum et du maximum de v.a.r. à densité indépendantes. Il suffit une nouvelle fois de mettre en place la rédaction usuelle associée à ce type de questions.

Commentaire

- Profitons-en pour faire un point sur la notation $X(\Omega)$.
  Rappelons qu'une v.a.r. X est une application $X : \Omega \to \mathbb{R}$.
  Comme la notation le suggère, $X(\Omega)$ est l'image de Ω par l'application X.
  Ainsi, $X(\Omega)$ n'est rien d'autre que l'ensemble des valeurs prises par la v.a.r. X :
  $$\begin{array}{rcl} X(\Omega) & = & \{X(\omega) \mid \omega \in \Omega\} \\ & = & \{x \in \mathbb{R} \mid \exists \omega \in \Omega,\ X(\omega) = x\} \end{array}$$
  Il faut bien noter que dans cette définition aucune application probabilité $\mathbb{P}$ n'apparaît.
- Il est toujours correct d'écrire : $X(\Omega) \subseteq \ ]-\infty, +\infty[$.
  En effet, cette propriété signifie que toute v.a.r. X est à valeurs dans $\mathbb{R}$, ce qui est toujours le cas par définition de la notion de variable aléatoire réelle.
- Dans le cas des v.a.r. discrètes, il est d'usage relativement courant de confondre :
  - × l'ensemble des valeurs possibles de la v.a.r. X (*i.e.* l'ensemble $X(\Omega)$),
  - × l'ensemble $\{x \in \mathbb{R} \mid \mathbb{P}\big([X = x]\big) \neq 0\}$, ensemble des valeurs que X prend avec probabilité non nulle. Si X est une v.a.r. discrète, cet ensemble est appelé support de X et est noté $\mathrm{Supp}(X)$.
- Dans le cas des v.a.r. à densité, la détermination de l'ensemble image est plus technique. Dans certains sujets, l'ensemble image des v.a.r. étudiées sera précisé (« On considère une v.a.r. à valeurs strictement positives »). Si ce n'est pas le cas :
  - × si X suit une loi usuelle, on peut se référer à l'ensemble image donné en cours. Par exemple, si $X \hookrightarrow \mathcal{U}([0,1])$, on se permet d'écrire :

    « Comme $X \hookrightarrow \mathcal{U}([0,1])$, on **considère** : $X(\Omega) = [0,1]$. »

  - × si X ne suit pas une loi usuelle, on étudie l'ensemble : $I = \{x \in \mathbb{R} \mid f_X(x) > 0\}$.
    On se permet alors d'écrire :

    « Dans la suite, on **considère** : $X(\Omega) = I$. »

  En **décrétant** la valeur de $X(\Omega)$, on ne commet pas une erreur mais on décide d'ajouter une hypothèse qui ne fait pas partie de l'énoncé. Cette audace permet de travailler avec un ensemble image connu, ce qui permet de structurer certaines démonstrations (l'ensemble image étant connu, on se rappelle que la fonction de répartition, par exemple, s'obtient par une disjonction de cas).

□

b) En déduire que pour tout $\theta \geqslant 0$:
$$\mathbb{P}(\,[U - \theta \leqslant V]\,) \ = \ 1 - \frac{\mu}{\lambda + \mu}\, \mathrm{e}^{-\lambda\,\theta}$$

Démonstration.

- Remarquons tout d'abord que la v.a.r. $X = U - \theta$ est une v.a.r. à densité en tant que transformée affine d'une v.a.r. à densité.
- Ainsi, on a :
  - × les v.a.r. X et V sont à densité.
  - × les v.a.r. $X = U - \theta$ et V sont indépendantes d'après le lemme des coalitions et car U et V le sont.

× comme $V \hookrightarrow \mathcal{E}(\mu)$, on peut considérer $V(\Omega) = [0, +\infty[$.
Autrement dit, on considère que la v.a.r. V est à valeurs positives.

× une densité f_V de la v.a.r. V est donnée par :

$$f_V : t \mapsto \begin{cases} 0 & \text{si } t < 0 \\ \mu\, \mathrm{e}^{-\mu\, t} & \text{si } t \geqslant 0 \end{cases}$$

Et ainsi : $f_V|_{[0,+\infty[} : t \mapsto \mu\, \mathrm{e}^{-\mu\, t}$ est une fonction continue sur $[0, +\infty[$.

On est dans le cadre d'application du résultat démontré en question ***4***.

Commentaire

- Comme précisé dans la question précédente, on se permet de considérer $V(\Omega) = [0, +\infty[$. En réalité, pour toute v.a.r. qui suit une loi exponentielle, cette propriété n'est vérifiée que presque sûrement (avec probabilité 1). Autrement dit, on a toujours, sans hypothèse supplémentaire : $\mathbb{P}\big([V \geqslant 0]\big) = 1$. Il est à noter que c'est l'énoncé qui nous amène à considérer $V(\Omega) = [0, +\infty[$. En effet, cette hypothèse est nécessaire pour se placer dans le cadre d'application du résultat démontré en question ***4***. Il aurait donc été préférable que l'énoncé précise que V est une v.a.r. à valeurs positives, en début de question ***5***.
- Comme signalé au-dessus, il est primordial de savoir déterminer la transformée affine d'une v.a.r. à densité. Ici, on ne demande pas explicitement d'obtenir une densité de la v.a.r. X. On utilise ici le résultat du cours qui affime que la transformée affine d'une v.a.r. à densité est une v.a.r. à densité. On peut aussi démontrer que X est une v.a.r. à densité en établissant que F_X est :
  × continue sur $\mathbb{R}$,
  × de classe $\mathcal{C}^1$ sur $\mathbb{R}$ sauf (éventuellement) en un nombre fini de points.

- On a alors :

$$\begin{aligned}
\mathbb{P}\big([U - \theta \leqslant V]\big) &= \mathbb{P}\big([X \leqslant V]\big) \\
&= \int_0^{+\infty} F_X(t)\, f_V(t)\; dt \\
&= \int_0^{+\infty} \big(1 - \mathrm{e}^{-\lambda\,\theta}\ \mathrm{e}^{-\lambda\, t}\big)\ \mu\, \mathrm{e}^{-\mu\, t}\; dt \\
&= \int_0^{+\infty} \mu\, \mathrm{e}^{-\mu\, t}\; dt - \int_0^{+\infty} \mathrm{e}^{-\lambda\,\theta}\ \mathrm{e}^{-\lambda t}\ \mu\, \mathrm{e}^{-\mu\, t}\; dt && \textit{(par linéarité de l'intégration, les intégrales en présence étant convergentes)} \\
&= \mathbb{E}\big(V^0\big) - \mathrm{e}^{-\lambda\,\theta}\ \mu \int_0^{+\infty} \mathrm{e}^{-\lambda\, t}\ \mathrm{e}^{-\mu\, t}\; dt \\
&= 1 - \mathrm{e}^{-\lambda\,\theta}\ \mu\ \frac{1}{\lambda + \mu} \int_0^{+\infty} (\lambda + \mu)\ \mathrm{e}^{-(\lambda+\mu)\, t}\; dt \\
&= 1 - \frac{\mu}{\lambda + \mu}\ \mathrm{e}^{-\lambda\,\theta}\ \mathbb{E}\big(W^0\big) && \textit{(où } W \textit{ est une v.a.r. de loi } \mathcal{E}(\lambda+\mu)\textit{)}
\end{aligned}$$

$$\boxed{\text{Finalement, on obtient bien : } \mathbb{P}\big([U - \theta \leqslant V]\big) = 1 - \frac{\mu}{\lambda + \mu}\ \mathrm{e}^{-\lambda\,\theta}.}$$

Commentaire

- Détaillons l'obtention de l'égalité : $\displaystyle\int_0^{+\infty} \mu\,\mathrm{e}^{-\mu\,t}\,dt = \mathbb{E}\big(V^0\big)$.

$$\begin{aligned}
\int_0^{+\infty} \mu\,\mathrm{e}^{-\mu\,t}\,dt &= \int_0^{+\infty} f_V(t)\,dt \\
&= \int_{-\infty}^{+\infty} f_V(t)\,dt \qquad \textit{(car } f_V \textit{ est nulle en dehors de } [0,+\infty[\textit{)} \\
&= \int_{-\infty}^{+\infty} t^0\,f_V(t)\,dt \\
&= \mathbb{E}(V^0) \quad (=1)
\end{aligned}$$

- Notons que l'on pourrait exploiter le fait que f_V est une densité pour obtenir :

$$\int_{-\infty}^{+\infty} f_V(t)\,dt \ = \ 1$$

Ce n'est cependant pas le choix fait dans ce corrigé, car il faut s'habituer à reconnaître les moments d'ordre 1 et 2 d'une v.a.r. de loi exponentielle. Plus précisément :

$$\int_0^{+\infty} t\,\mu\,\mathrm{e}^{-\mu\,t}\,dt \ = \ \mathbb{E}(V) \ = \ \frac{1}{\mu}$$

$$\int_0^{+\infty} t^2\,\mu\,\mathrm{e}^{-\mu\,t}\,dt \ = \ \mathbb{E}(V^2) \ = \ \mathbb{V}(V) + \big(\mathbb{E}(V)\big)^2 \ = \ \frac{2}{\mu^2}$$

On traite ici le moment d'ordre 0 de la même manière que l'on traiterait les moments d'ordre 1 et 2.

Inégalité de Boole

6. On considère $(B_k)_{k\in\mathbb{N}^*}$ une famille d'événements d'un espace probabilisé.

a) Montrer par récurrence sur $n \in \mathbb{N}^*$: $\mathbb{P}\left(\bigcup\limits_{k=1}^{n} B_k\right) \leqslant \sum\limits_{k=1}^{n} \mathbb{P}(B_k)$.

Démonstration.

Démontrons par récurrence : $\forall n \in \mathbb{N}^*$, $\mathcal{P}(n)$, où $\mathcal{P}(n)$: $\mathbb{P}\left(\bigcup\limits_{k=1}^{n} B_k\right) \leqslant \sum\limits_{k=1}^{n} \mathbb{P}(B_k)$.

▸ **Initialisation** :

- D'une part : $\mathbb{P}\left(\bigcup\limits_{k=1}^{1} B_k\right) = \mathbb{P}\left(B_1\right)$.
- D'autre part : $\sum\limits_{k=1}^{1} \mathbb{P}(B_k) = \mathbb{P}(B_1)$.

On a bien : $\mathbb{P}\left(B_1\right) \leqslant \mathbb{P}\left(B_1\right)$. D'où $\mathcal{P}(1)$.

- **Hérédité** : soit $n \in \mathbb{N}^*$.
  Supposons $\mathcal{P}(n)$ et démontrons $\mathcal{P}(n+1)$ $\left(i.e. : \mathbb{P}\left(\bigcup\limits_{k=1}^{n+1} B_k\right) \leqslant \sum\limits_{k=1}^{n+1} \mathbb{P}(B_k)\right)$.

$$\begin{array}{rcll}
\mathbb{P}\left(\bigcup\limits_{k=1}^{n+1} B_k\right) & = & \mathbb{P}\left(\left(\bigcup\limits_{k=1}^{n} B_k\right) \cup B_{n+1}\right) & \\
& = & \mathbb{P}\left(\bigcup\limits_{k=1}^{n} B_k\right) + \mathbb{P}(B_{n+1}) - \mathbb{P}\left(\left(\bigcup\limits_{k=1}^{n} B_k\right) \cap B_{n+1}\right) & \textit{(d'après la formule du crible)} \\
& \leqslant & \sum\limits_{k=1}^{n} \mathbb{P}(B_k) + \mathbb{P}(B_{n+1}) - \mathbb{P}\left(\left(\bigcup\limits_{k=1}^{n} B_k\right) \cap B_{n+1}\right) & \textit{(par hypothèse de récurrence)} \\
& \leqslant & \sum\limits_{k=1}^{n} \mathbb{P}(B_k) + \mathbb{P}(B_{n+1}) &
\end{array}$$

  D'où $\mathcal{P}(n+1)$.

$$\boxed{\text{Par principe de récurrence : } \forall n \in \mathbb{N}^*, \ \mathbb{P}\left(\bigcup\limits_{k=1}^{n} B_k\right) \leqslant \sum\limits_{k=1}^{n} \mathbb{P}(B_k).}$$

□

b) On suppose que la série $\sum\limits_{k \geqslant 1} \mathbb{P}(B_k)$ converge. Démontrer :

$$\mathbb{P}\left(\bigcup\limits_{k=1}^{+\infty} B_k\right) \leqslant \sum\limits_{k=1}^{+\infty} \mathbb{P}(B_k)$$

Démonstration.

- Tout d'abord, par le théorème de la limite monotone : $\mathbb{P}\left(\bigcup\limits_{k=1}^{+\infty} B_k\right) = \lim\limits_{N \to +\infty} \mathbb{P}\left(\bigcup\limits_{k=1}^{N} B_k\right)$.
- Comme la série $\sum\limits_{k \geqslant 1} \mathbb{P}(B_k)$ est supposée convergente, on obtient, par passage à la limite dans l'inégalité de la question précédente :

$$\lim_{N \to +\infty} \mathbb{P}\left(\bigcup\limits_{k=1}^{N} B_k\right) \leqslant \lim_{N \to +\infty} \sum\limits_{k=1}^{N} \mathbb{P}(B_k) = \sum\limits_{k=1}^{+\infty} \mathbb{P}(B_k)$$

$$\boxed{\mathbb{P}\left(\bigcup\limits_{k=1}^{+\infty} B_k\right) \leqslant \sum\limits_{k=1}^{+\infty} \mathbb{P}(B_k)}$$

□

Partie II - Une compétition entre deux groupes

Dans toute la suite du sujet, on désigne par p un réel de l'intervalle $]0,1[$ et on pose $q = 1 - p$.
On modélise une compétition entre deux groupes d'individus A et B avec les règles suivantes.

- Le groupe A doit résoudre une suite de problèmes $(P_k)_{k \geqslant 1}$ dans l'ordre des indices. Au temps $t = 0$, le groupe commence la résolution du problème P_1, ce qui lui prend un temps représenté par la variable aléatoire X_1. Une fois P_1 résolu, le groupe aborde immédiatement le problème P_2, et on note X_2 le temps consacré à la résolution de P_2 par le groupe A, et ainsi de suite.
  Pour tout $k \in \mathbb{N}^*$, on note X_k la variable aléatoire donnant le temps consacré à la résolution du problème P_k par le groupe A.
- De même, le groupe B doit résoudre dans l'ordre une suite de problèmes $(Q_k)_{k \geqslant 1}$; la résolution du premier problème Q_1 commence au temps $t = 0$ et on note, pour tout $k \in \mathbb{N}^*$, Y_k la variable aléatoire donnant le temps consacré par le groupe B à la résolution du problème Q_k.
- À ce jeu est associé un espace probabilisé $(\Omega, \mathscr{A}, \mathbb{P})$ sur lequel sont définies les suites de variables aléatoires $(X_k)_{k \geqslant 1}$ et $(Y_k)_{k \geqslant 1}$, et on fait les hypothèses suivantes :
  - × pour tout $k \in \mathbb{N}^*$, X_k suit la loi exponentielle de paramètre p, notée $\mathcal{E}(p)$, et Y_k suit la loi exponentielle $\mathcal{E}(q)$;
  - × pour tout $k \in \mathbb{N}^*$, les variables aléatoires $X_1, \ldots, X_k, Y_1, \ldots, Y_k$ sont indépendantes.
- On établit alors la liste de tous les problèmes résolus *dans l'ordre où ils le sont par les deux groupes*. En cas de simultanéité temporelle de la résolution par les deux groupes d'un de leurs problèmes, on placera d'abord le problème résolu par A dans la liste puis celui résolu par B.
  Pour tout $n \in \mathbb{N}^*$, on note U_n la variable aléatoire de Bernoulli associée à l'événement « le $n^{\text{ème}}$ problème placé dans la liste est un problème résolu par le groupe A ».
  Par exemple, si la liste des cinq premiers problèmes résolus est $(P_1, P_2, Q_1, P_3, Q_2)$, alors $U_1 = 1$, $U_2 = 1$, $U_3 = 0$, $U_4 = 1$ et $U_5 = 0$.
- Pour tout $n \geqslant 0$, on note aussi S_n la variable aléatoire donnant le nombre de problèmes qui ont été résolus par A présents dans la liste des n premiers problèmes résolus. En particulier, S_0 vaut toujours 0.

Commentaire

- Lorsque l'on propose un problème à un groupe, il paraît étonnant de considérer que le temps de résolution de celui-ci puisse être considéré comme aléatoire. On peut au contraire penser que le temps de résolution est entièrement déterministe car il ne dépend que de la composition du groupe, des qualités de raisonnement de ses membres et de leurs connaissances. Ce n'est pas pour autant que la modélisation de l'énoncé n'a pas de sens. En réalité, l'aléa se situe dans le choix aléatoire réalisé pour décider des problèmes qui seront proposés au fur et à mesure aux groupes. Il est alors pertinent de considérer les temps de résolution comme aléatoires.
- On l'a déjà signalé en remarque : une v.a.r. X est une **application** de Ω dans $\mathbb{R}$. Ainsi :
  - × lorsque l'on note $X = 5$, cela signifie que la v.a.r. X est la v.a.r. constante égale à 5 (la propriété : $\forall \omega \in \Omega,\ X(\omega) = 5$ est vérifiée).
  - × lorsqu'on écrit « la v.a.r. X prend la valeur 5 lorsque ... » signifie qu'il **existe** (au moins) un tirage $\omega \in \Omega$ pour lequel $X(\omega) = 5$.

  Malheureusement, cet énoncé ne fait pas de différence entre ces deux expressions. C'est tout à fait malheureux car cela revient à confondre les symboles $\forall$ et $\exists$. Il aurait été plus sage d'écrire :

  « Si la liste des cinq premiers problèmes résolus est $(P_1, P_2, Q_1, P_3, Q_2)$, alors U_1 prend la valeur 1, U_2 prend la valeur 1, U_3 prend la valeur 0, U_4 prend la valeur 1 et U_5 prend la valeur 0. »

  On comprend néanmoins que cette présentation a été écartée pour des raisons de lisibilité.

7. *a)* Que représente la variable aléatoire $\sum\limits_{k=1}^{n} X_k$?

Démonstration.
Pour tout $k \in \mathbb{N}^*$, la v.a.r. X_k représente le temps de résolution du $k^{\text{ème}}$ problème P_k par le groupe A.

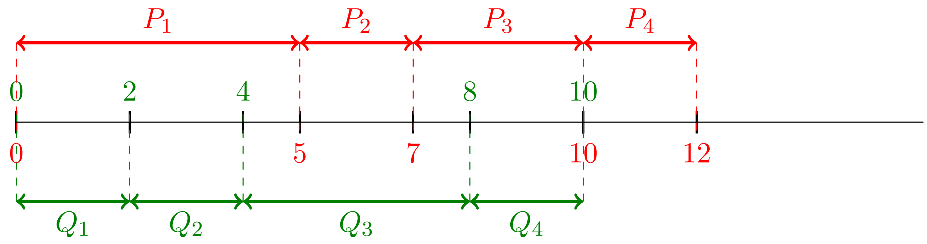
> Ainsi, la v.a.r. $\sum\limits_{k=1}^{n} X_k$ prend pour valeur le temps pris par le groupe A pour résoudre les n premiers problèmes fournis.

□

b) On suppose que $X_1 = 5$, $X_2 = 2$, $X_3 = 3$, $X_4 = 2$, $Y_1 = 2$, $Y_2 = 2$, $Y_3 = 4$ et $Y_4 = 2$.
Déterminer U_1, ..., U_7.
Peut-on aussi en déduire la valeur de U_8 ?

Démonstration.

- On présente ci-dessous la frise chronologique représentant les temps de résolution des 4 premiers problèmes donnés à chacun des groupes :



- Ainsi, :
  - × au bout de 2 unités de temps, un 1^{er} problème est résolu. Il s'agit de Q_1.
  - × il faut attendre 2 unités de temps supplémentaires pour la résolution d'un nouveau problème, le $2^{\text{ème}}$ résolu. Il s'agit de Q_2.
  - × il faut attendre 1 unité de temps supplémentaire pour la résolution d'un nouveau problème, le $3^{\text{ème}}$ résolu. Il s'agit de P_1.
  - × il faut attendre 2 unités de temps supplémentaires pour la résolution d'un nouveau problème, le $4^{\text{ème}}$ résolu. Il s'agit de P_2.
  - × il faut attendre 1 unité de temps supplémentaire pour la résolution d'un nouveau problème, le $5^{\text{ème}}$ résolu. Il s'agit de Q_3.
  - × il faut attendre 2 unités de temps supplémentaires pour la résolution d'un nouveau problème. À cette date, P_3 et Q_4 sont résolus simultanément. Dans ce cas, comme l'indique l'énoncé, on considère que P_3 est le $6^{\text{ème}}$ problème résolu et Q_4 est le $7^{\text{ème}}$.
  - × on ne peut déterminer le $8^{\text{ème}}$ problème résolu. En effet :
    - ▶ soit le groupe B met strictement moins de 2 unités de temps à résoudre le problème Q_5 alors c'est ce problème qui est le $8^{\text{ème}}$ problème résolu.
    - ▶ soit le groupe B met plus de 2 unités de temps à résoudre le problème Q_5 alors c'est le problème P_4 qui est le $8^{\text{ème}}$ problème résolu.

> On en déduit que la liste des 7 premiers problèmes résolus est $(Q_1, Q_2, P_1, P_2, Q_3)$. Les valeurs de U_1, ..., U_7 correspondant à la liste précédente sont respectivement : 0, 0, 1, 1, 0, 1, 0.

> On ne peut pas obtenir la valeur de U_8 dans l'exemple fourni par l'énoncé.

□

c) Compléter le script **Scilab** suivant pour qu'il simule le jeu et, pour n, p donnés, affiche la liste des valeurs U_1, U_2, ..., U_n :

```
1  p = input('p = ')
2  n = input('n = ')
3  q = 1 - p
4  U = zeros(1, n)
5  sommeX = grand(1, 1, 'exp', 1/p)
6  sommeY = grand(1, 1, 'exp', 1/q)
7  mini = min(sommeX, sommeY)
8  for k = 1:n
9      if sommeX == ... then
10         U(k) = ...
11         sommeX = sommeX + grand(1, 1, 'exp', 1/p)
12     else
13         sommeY = ...
14     end
15     mini = min(sommeX, sommeY)
16 end
17 ...
```

Démonstration.
Détaillons les différents éléments présents dans ce script.

- **Début du programme**
  - En lignes 1 et 2, on stocke dans les variables `p` et `n`, une valeur pour p et n à l'aide d'une interface de dialogue avec l'utilisateur :

```
1  p = input('p = ')
2  n = input('n = ')
```

  - En ligne 3, on définit la variable `q` qui stocke la valeur de q.

```
3  q = 1 - p
```

  - Les lignes suivantes servent à initialiser les variables qui seront mises à jour dans la structure itérative à suivre.

```
4  U = zeros(1, n)
5  sommeX = grand(1, 1, 'exp', 1/p)
6  sommeY = grand(1, 1, 'exp', 1/q)
7  mini = min(sommeX, sommeY)
```

En ligne 4, on crée une matrice de taille $1 \times n$ intialement remplie de 0. Elle est destinée à contenir les valeurs des simulations des v.a.r. $U_1, \ldots, U_n$.

En lignes 5 et 6, on initialise les variables `sommeX` et `sommeY`. Comme leurs noms l'indiquent, elles sont destinées à contenir les valeurs successives des simulations des suites $(R_n)_{n \in \mathbb{N}^*}$ et $(T_n)_{n \in \mathbb{N}^*}$ (on note, pour tout $n \in \mathbb{N}^*$, $R_n = \sum\limits_{k=1}^{n} X_k$ et $T_n = \sum\limits_{k=1}^{n} Y_k$).
Plus précisément, l'instruction `grand(1, 1, 'exp', 1/p)` sert à simuler la v.a.r. $R_1 = X_1$ (en ligne 5) et la v.a.r. $T_1 = Y_1$ (en ligne 6). Les variables `sommeX` et `sommeY` contiennent donc initialement le temps pris pour chaque groupe pour résoudre le premier problème fourni.

En ligne 7, on définit une variable `mini` visiblement destinée à contenir le minimum des variables `sommeX` et `sommeY`.

- **Structure itérative**
  Avant d'entrer dans le 1[er] tour de boucle, les variables `sommeX` et `sommeY` contiennent le temps mis par chaque groupe pour résoudre les problèmes qu'on leur a fournis alors que 2 problèmes ont été fournis en tout (ce sont les problèmes en cours). La variable `U` ne contient alors pas encore de simulation des variables U_1, ..., U_n.

  On peut généraliser ces constatations à chaque tour. Plus précisément, pour tout $k \in \mathbb{N}^*$, avant l'entrée dans le $k^{\text{ème}}$ tour de boucle :

  × les variables `sommeX` et `sommeY` contiennent le temps mis par chaque groupe pour résoudre les problèmes qu'on leur a fournis alors que $k+1$ problèmes ont été fournis en tout.

  × la variable `mini` contient le minimum des deux variables précédentes.

  × les $k-1$ premiers coefficients de la matrice ligne `U` contiennent les simulations des v.a.r. U_1, ..., U_{k-1}.

  On entre alors dans le $k^{\text{ème}}$ tour de boucle :

  × **Structure conditionnelle**
  On repère tout d'abord quel groupe en a fini avec la résolution de son problème en cours. On cherche donc quelle variable entre `sommeX` et `sommeY` contient la plus petite valeur. Pour ce faire, on teste si `sommeX` contient cette plus petite valeur :

```
9      if sommeX == mini then
```

  ► Si c'est le cas, c'est que le groupe A a résolu son problème en cours alors que le groupe B est encore en phase de résolution du sien. Cela signifie que le $k^{\text{ème}}$ problème résolu l'a été par le groupe A. Ainsi, la v.a.r. U_k prend la valeur 1, ce qui se traduit par la mise à jour de `U(k)`, $k^{\text{ème}}$ coefficient de la matrice `U`.

```
10         U(k) = 1
```

  Enfin, on fournit au groupe A un nouveau problème ce qui est simulé par l'ajout du temps de résolution de ce nouveau problème à la variable d'accumulation `sommeX`.

```
11         sommeX = sommeX + grand(1, 1, 'exp', 1/p)
```

  ► Si ce n'est pas le cas, c'est que le groupe B a résolu son problème en cours alors que le groupe A est encore en phase de résolution du sien. Cela signifie que le $k^{\text{ème}}$ problème résolu l'a été par le groupe B. Ainsi, la v.a.r. U_k prend la valeur 0 et on doit fournir à B un nouveau problème. Cela se traduit informatiquement comme suit :

```
12     else
13         U(k) = 0
14         sommeY = sommeY + grand(1, 1, 'exp', 1/q)
15     end
```

  En réalité, la ligne 13 est inutile. En effet, la variable `U` est affectée initialement à une matrice ligne remplie de 0. Ainsi, son $k^{\text{ème}}$ coefficient est déjà 0 et il est donc inutile de le mettre à jour.

  × L'une des deux variables `sommeX` ou `sommeY` ayant été modifiée, on doit mettre à jour la variable `mini` en sortie de structure conditionnelle.

```
15     mini = min(sommeX, sommeY)
```

Ces mises à jour ayant été faites, on est assurés, qu'à l'issue de ce $k^{\text{ème}}$ tour de boucle (et donc avant l'entrée dans le $(k+1)^{\text{ème}}$ tour de boucle :

× les variables `sommeX` et `sommeY` contiennent le temps mis par chaque groupe pour résoudre les problèmes qu'on leur a fournis alors que $(k+1)+1 = k+2$ problèmes ont été fournis en tout (on a fourni un problème supplémentaire lors de l'exécution du $k^{\text{ème}}$ tour de boucle).

× la variable `mini` contient le minimum des deux variables précédentes.

× les $(k-1)+1 = k$ premiers coefficients de la matrice ligne `U` contiennent les simulations des v.a.r. $U_1, \ldots, U_k$ (on a mis à jour `U(k)` lors de l'exécution du $k^{\text{ème}}$ tour de boucle).

- **Fin du programme**
  À l'issue de cette boucle, c'est-à-dire à l'issue du $n^{\text{ème}}$ tour, on est alors assuré que les n premiers coefficients de la matrice ligne `U` contiennent les simulations des v.a.r. $U_1, \ldots, U_n$. On renvoie cette valeur.

```
disp(U)
```

Commentaire

- L'énoncé nous incite à écrire des scripts avec des dialogues utilisateurs et des affichages. Cependant, il pourrait être pertinent pour cette question de présenter le résultat sous forme de fonction. On rappelle qu'une fonction permet de réaliser un calcul dont le résultat est réutilisable par un autre programme. C'est d'ailleurs une des bases de la programmation de mener une réflexion sur le découpage en sous-fonctions du projet que l'on souhaite coder.
- Afin de permettre une bonne compréhension des mécanismes en jeu, on a détaillé la réponse à cette question. Cependant, compléter correctement le programme **Scilab** démontre la bonne compréhension de la simulation demandée et permet certainement d'obtenir tous les points alloués à cette question.
  On procédera de même dans les autres questions **Scilab**.
- On a démontré dans cette question que si une propriété décrivant le contenu des variables `sommeX`, `sommeY`, `mini` et `U` était vérifiée au rang $k-1$ (avant le $k^{\text{ème}}$ tour de boucle) alors elle l'était encore au rang k (à l'issue du $k^{\text{ème}}$ tour de boucle et donc avant le $(k+1)^{\text{ème}}$ tour de boucle).
  Cette propriété est ce qu'on appelle un **invariant de boucle**. Elle permet de s'assurer que la fonction implémentée est correcte et notamment qu'à l'issue du dernier tour de boucle la variable `U` contient bien les simulations des v.a.r. $U_1, \ldots, U_n$. □

d) Quelle(s) instruction(s) faut-il ajouter pour afficher la valeur de S_n ?

Démonstration.

- Par définition, pour tout $n \in \mathbb{N}^*$, S_n est la v.a.r. qui prend pour valeur le nombre de problèmes résolus par A dans la liste des n premiers problèmes résolus.
- Autrement dit, S_n est le nombre de v.a.r. $U_1, \ldots, U_n$ qui ont pris la valeur 1 au cours de l'expérience. Ces v.a.r. prenant uniquement la valeur 0 ou 1, on peut alors en conclure :

$$\forall n \in \mathbb{N}^*, \ S_n \ = \ \sum_{k=1}^{n} U_k$$

- Dans le programme précédent, on a créé une variable informatique `U`, matrice ligne de taille $1 \times n$ destinée à contenir la simulation des v.a.r. $U_1, \ldots, U_n$. Il suffit de sommer tous les coefficients de cette matrice pour obtenir la simulation de la v.a.r. S_n. L'affichage est alors réalisé par la fonction `disp`.

```
disp(sum(U))
```

Commentaire

- L'énoncé n'oblige pas à traiter cette question en n'utilisant qu'une seule instruction. Par exemple, il est tout à fait possible de simuler cette v.a.r. S_n à l'aide d'une variable informatique `S` mise à jour par une structure itérative.
- Plus précisément, on pouvait écrire le programme suivant à l'issue du précédent :

```
1 S = 0
2 for k = 1:n
3     S = S + U(k)
4 end
5 disp(S)
```

En réalité, le calcul de `S` peut s'insérer dans la structure itérative déjà présente dans le programme précédent :

× la ligne 1 peut s'insérer entre la ligne 7 et 8 du programme précédent.

× la ligne 3 peut s'insérer entre la ligne 15 et 16 du programme précédent.

× la ligne 4 peut s'insérer en dernière ligne du programme précédent. □

8. *Loi de U_n*

Dans cette question, on démontre par récurrence sur $n \geqslant 1$: $\mathbb{P}([U_n = 1]) = p$.

a) Démontrer : $\mathbb{P}([U_1 = 1]) = \mathbb{P}([X_1 \leqslant Y_1]) = p$.

Démonstration.

- On remarque tout d'abord :

L'événement $[U_1 = 1]$ est réalisé

$\Leftrightarrow$ Le premier problème résolu l'a été par le groupe A (ou par A et B simultanément)

$\Leftrightarrow$ Le temps de résolution du problème P_1 (proposé au groupe A) est inférieur ou égal au temps de résolution du problème Q_1 (proposé au groupe B)

$\Leftrightarrow$ La v.a.r. X_1 prend une valeur plus faible que la v.a.r. Y_1

$\Leftrightarrow$ L'événement $[X_1 \leqslant Y_1]$ est réalisé

$$\boxed{\text{Ainsi : } [U_1 = 1] = [X_1 \leqslant Y_1].}$$

- Les v.a.r. X_1 et Y_1 vérifient les hypothèses de la question ***5.*** de la **Partie I**.
Plus précisément, ce sont deux v.a.r. indépendantes suivant des lois exponentielles de paramètres respectifs $\lambda = p > 0$ et $\mu = q > 0$.
On peut alors appliquer le résultat pour $U = X_1$, $V = Y_1$ et $\theta = 0 \geqslant 0$. On obtient :

$$\begin{aligned}
\mathbb{P}\big([X_1 - 0 \leqslant Y_1]\big) &= 1 - \frac{q}{p+q}\,\mathrm{e}^{-p\times 0} \\
&= 1 - q && \textit{(car } p+q = 1 \textit{ et } e^0 = 1\textit{)} \\
&= p && \textit{(car } p+q = 1\textit{)}
\end{aligned}$$

$$\boxed{\text{Finalement : } \mathbb{P}\big([U_1 = 1]\big) = \mathbb{P}\big([X_1 \leqslant Y_1]\big) = p.}$$

□

b) (i) Démontrer, pour tout réel $x < 0$: $\mathbb{P}_{[U_1=1]}(\,[Y_1 - X_1 \leqslant x]\,) = 0$.

Démonstration.
Soit $x < 0$.

- Tout d'abord :

$$\begin{array}{rcll} \mathbb{P}_{[U_1=1]}\big(\,[Y_1 - X_1 \leqslant x]\,\big) & = & \dfrac{\mathbb{P}\big([U_1 = 1] \cap [Y_1 - X_1 \leqslant x]\,\big)}{\mathbb{P}\big([U_1 = 1]\big)} & \\ & = & \dfrac{\mathbb{P}\big(\,[X_1 \leqslant Y_1] \cap [Y_1 \leqslant X_1 + x]\,\big)}{\mathbb{P}\big([U_1 = 1]\big)} & \textit{(d'après la démonstration de la question précédente)} \\ & = & \dfrac{\mathbb{P}\big(\varnothing\big)}{\mathbb{P}\big([U_1 = 1]\big)} \ = \ 0 & (*) \end{array}$$

- Il reste à démontrer : $[X_1 \leqslant Y_1] \cap [Y_1 \leqslant X_1 + x] = \varnothing$.
  Supposons que l'événement $[X_1 \leqslant Y_1] \cap [Y_1 \leqslant X_1 + x]$ est réalisé. Alors :
  - × l'événement $[X_1 \leqslant Y_1]$ est réalisé.
    Ainsi, la v.a.r. X_1 prend une valeur plus petite que celle prise par Y_1.
  - × l'événement $[Y_1 \leqslant X_1 + x]$ est réalisé.
    Ainsi, la v.a.r. Y_1 prend une valeur plus petite que celle prise par $X_1 + x$.

  On en déduit, par transitivité que X_1 prend une valeur plus petite que celle prise par X_1+x.
  C'est impossible car $x < 0$.

$$\boxed{\text{Finalement, on a bien : } \forall x < 0,\ \mathbb{P}_{[U_1=1]}\big(\,[Y_1 - X_1 \leqslant x]\,\big) = 0.}$$

□

(ii) Soit x un réel positif ou nul.
Établir : $\mathbb{P}_{[U_1=1]}\big(\,[Y_1 - X_1 \leqslant x]\,\big) = \dfrac{1}{p}\ \mathbb{P}\big(\,[X_1 \leqslant Y_1 \leqslant X_1 + x]\,\big)$,
puis calculer $\mathbb{P}_{[U_1=1]}(\,[Y_1 - X_1 \leqslant x]\,)$.

Démonstration.
Soit $x \geqslant 0$.

- En reprenant la question précédente, on obtient :

$$\begin{array}{rcll} \mathbb{P}_{[U_1=1]}\big(\,[Y_1 - X_1 \leqslant x]\,\big) & = & \dfrac{\mathbb{P}\big(\,[X_1 \leqslant Y_1] \cap [Y_1 \leqslant X_1 + x]\,\big)}{\mathbb{P}\big([U_1 = 1]\big)} & \\ & = & \dfrac{1}{p}\ \mathbb{P}\big(\,[X_1 \leqslant Y_1 \leqslant X_1 + x]\,\big) & \textit{(car } \mathbb{P}\big([U_1 = 1]\big) = p \textit{ d'après la question } \textbf{\textit{8.a)}}\textit{)} \end{array}$$

$$\boxed{\forall x \geqslant 0,\ \ \mathbb{P}_{[U_1=1]}\big(\,[Y_1 - X_1 \leqslant x]\,\big) = \dfrac{1}{p}\ \mathbb{P}\big(\,[X_1 \leqslant Y_1 \leqslant X_1 + x]\,\big)}$$

- La famille $\Big(\,[Y_1 \leqslant X_1 + x]\,, [Y_1 > X_1 + x]\,\Big)$ forme un système complet d'événements.
  On en déduit, par la formule des probabilités totales :

$$\mathbb{P}\big(\,[X_1 \leqslant Y_1]\,\big) \ = \ \mathbb{P}\big(\,[X_1 \leqslant Y_1] \cap [Y_1 \leqslant X_1 + x]\,\big) + \mathbb{P}\big(\,[X_1 \leqslant Y_1] \cap [Y_1 > X_1 + x]\,\big)$$

  Comme $[Y_1 > X_1 + x] \subset [X_1 \leqslant Y_1]$ alors : $[X_1 \leqslant Y_1] \cap [Y_1 > X_1 + x] = [Y_1 > X_1 + x]$.

On en déduit, en réordonnant les termes de l'égalité précédente :

$$\begin{array}{rcll}
\mathbb{P}\big([X_1 \leqslant Y_1 \leqslant X_1 + x]\big) & = & \mathbb{P}\big([X_1 \leqslant Y_1]\big) - \mathbb{P}\big([Y_1 > X_1 + x]\big) & \\
& = & \mathbb{P}\big([X_1 \leqslant Y_1]\big) - \big(1 - \mathbb{P}\big([Y_1 \leqslant X_1 + x]\big)\big) & \\
& = & \mathbb{P}\big([X_1 \leqslant Y_1]\big) - \big(1 - \mathbb{P}\big([Y_1 - x \leqslant X_1]\big)\big) & \\
& = & p - \left(\cancel{1} - \left(\cancel{1} - \dfrac{p}{p+q}\mathrm{e}^{-q\,x}\right)\right) & \begin{array}{l}\textit{(en appliquant la question } \textbf{\textit{5.b)}} \\ \textit{avec } U = Y_1,\ \lambda = q,\ V = X_1, \\ \mu = p \textit{ et } \theta = x \geqslant 0\textit{)}\end{array} \\
& = & p - \big(p\ \mathrm{e}^{-q\,x}\big) & \textit{(car } p + q = 1\textit{)} \\
& = & p\ \left(1 - \mathrm{e}^{-q\,x}\right) &
\end{array}$$

$$\boxed{\text{Finalement : } \forall x \geqslant 0,\ \ \mathbb{P}_{[U_1=1]}\big([Y_1 - X_1 \leqslant x]\big) = \frac{1}{p}\ \mathbb{P}\big([X_1 \leqslant Y_1 \leqslant X_1 + x]\big) = 1 - \mathrm{e}^{-q\,x}.}$$

□

c) On peut interpréter ce résultat en disant que la *loi conditionnelle de* $Y_1 - X_1$ *sachant* $[U_1 = 1]$ est une loi exponentielle. Quelle est son paramètre ?
Par analogie, quelle est la loi conditionnelle de $X_1 - Y_1$ sachant $[U_1 = 0]$? (on n'attend pas une démonstration précise mais un argument de bon sens pour justifier le résultat proposé).

Démonstration.

- La loi conditionnelle de $Y_1 - X_1$ sachant $[U_1 = 1]$ est celle d'une v.a.r. Z qui suit la loi exponentielle de paramètre q. En effet :

$$\forall x \in \mathbb{R},\ \mathbb{P}_{[U_1=1]}\big([Y_1 - X_1 \leqslant x]\big) \ = \ F_Z(x) \ = \ \left\{\begin{array}{cl} 0 & \text{si } x < 0 \\ 1 - \mathrm{e}^{-q\,x} & \text{si } x \geqslant 0 \end{array}\right.$$

$$\boxed{\text{La loi conditionnelle de } Y_1 - X_1 \text{ sachant } [U_1 = 1] \text{ est la loi } \mathcal{E}(q).}$$

Commentaire

- Rappelons que la fonction de répartition d'une v.a.r. caractérise sa loi. En particulier, donner la fonction de répartition d'une v.a.r. , c'est donner sa loi.
- Lorsque l'on cherche la loi conditionnelle d'une v.a.r. X sachant un événement A, on cherche la loi de X dans le contexte où l'événement A est réalisé. Se placer dans ce contexte, c'est considérer $\mathbb{P}_A$ en tant qu'application probabilité, en lieu et place de $\mathbb{P}$.
- Si la v.a.r. X est discrète, sa loi conditionnelle sachant l'événement A est la donnée :
  - × de son ensemble image $X(\Omega)$,
  - × des valeurs $\mathbb{P}_A\big([X = x]\big)$ pour tout $x \in X(\Omega)$.
- Si la v.a.r. X est à densité, sa loi conditionnelle sachant l'événement A est la donnée :
  - × de son ensemble image $X(\Omega)$,
  - × de la fonction $x \mapsto \mathbb{P}_A\big([X \leqslant x]\big)$.

  En réalité, cette dernière définition est aussi utilisable dans le cas discret, puisque la fonction fournie dans le deuxième point permet des déterminer les valeurs de la famille $\big(\mathbb{P}_A\big([X = x]\big)\big)_{x \in X(\Omega)}$.

- De manière générale, on a démontré que si U et V sont des v.a.r. indépendantes qui suivent chacune une loi exponentielle de paramètre respectivement $\lambda > 0$ et $\mu > 0$, alors la loi conditionnelle de $V - U$ sachant l'événement $[U \leqslant V]$ est la loi $\mathcal{E}(\mu)$.
  En appliquant ce résultat à $U = Y_1$, $V = X_1$, on démontre que la loi conditionnelle de $X_1 - Y_1$ sachant l'événement $[Y_1 \leqslant X_1]$ est la loi $\mathcal{E}(p)$.
- Pour conclure, il reste à remarquer :

$$\begin{aligned}
\mathbb{P}\big([Y_1 \leqslant X_1]\big) &= \mathbb{P}\big([Y_1 < X_1]\big) && \textit{(d'après la question 4.)} \\
&= \mathbb{P}\Big(\overline{[X_1 \leqslant Y_1]}\Big) \\
&= \mathbb{P}\Big(\overline{[U_1 = 1]}\Big) \\
&= 1 - \mathbb{P}\big([U_1 = 1]\big) \\
&= \mathbb{P}\big([U_1 = 0]\big) && \textit{(car } \big([U_1 = 0], [U_1 = 1]\big) \textit{ est un système complet d'événements)}
\end{aligned}$$

$$\boxed{\text{On peut en conclure que la loi conditionnelle de } X_1 - Y_1 \text{ sachant } [U_1 = 0] \text{ est la loi } \mathcal{E}(p).}$$

Commentaire

- Dans ce qui précède, on démontre : $\mathbb{P}\big([Y_1 \leqslant X_1]\big) = \mathbb{P}\big([U_1 = 0]\big)$. Cela ne démontre pas pour autant que les deux événements $[Y_1 \leqslant X_1]$ et $[U_1 = 0]$ sont égaux.
  Il n'est donc pas démontré que la loi conditionnelle de $X_1 - Y_1$ sachant $[X_1 \leqslant Y_1]$ est la même que la loi conditionnelle de $X_1 - Y_1$ sachant $[U_1 = 0]$. Pour ce faire, il faudrait démontrer que pour tout $x \in \mathbb{R}$, $\mathbb{P}_{[Y_1 \leqslant X_1]}\big([X_1 - Y_1 \leqslant x]\big) = \mathbb{P}_{[U_1=0]}\big([X_1 - Y_1 \leqslant x]\big)$.
- On peut le faire en remarquant que pour tout $x \in \mathbb{R}$:

$$\begin{aligned}
&\mathbb{P}_{[Y_1 \leqslant X_1]}\big([X_1 - Y_1 \leqslant x]\big) \\
= \ & \frac{\mathbb{P}\big([Y_1 \leqslant X_1] \cap [X_1 - Y_1 \leqslant x]\big)}{\mathbb{P}\big([Y_1 \leqslant X_1]\big)} \\
= \ & \frac{\mathbb{P}\big([Y_1 \leqslant X_1 \leqslant Y_1 + x]\big)}{\mathbb{P}\big([U_1 = 0]\big)} \\
= \ & \frac{\mathbb{P}\big([Y_1 < X_1 \leqslant Y_1 + x] \cup [X_1 = Y_1]\big)}{\mathbb{P}\big([U_1 = 0]\big)} \\
= \ & \frac{\mathbb{P}\big([Y_1 < X_1 \leqslant Y_1 + x]\big) + \mathbb{P}\big([X_1 = Y_1]\big)}{\mathbb{P}\big([U_1 = 0]\big)} && \textit{(par incompatibilité des événements)} \\
= \ & \frac{\mathbb{P}\big([Y_1 < X_1 \leqslant Y_1 + x]\big)}{\mathbb{P}\big([U_1 = 0]\big)} && \textit{(car } \mathbb{P}\big([X_1 = Y_1]\big) = 0 \textit{ d'après la question 4.)} \\
= \ & \frac{\mathbb{P}\big([Y_1 < X_1] \cap [X_1 \leqslant Y_1 + x]\big)}{\mathbb{P}\big([U_1 = 0]\big)} \\
= \ & \frac{\mathbb{P}\big([U_1 = 0] \cap [X_1 \leqslant Y_1 + x]\big)}{\mathbb{P}\big([U_1 = 0]\big)} = \mathbb{P}_{[U_1=0]}\big([X_1 - Y_1 \leqslant x]\big)
\end{aligned}$$

- La manière dont est formulée la question n'amène pas à un développement théorique. Celui-ci est donné ci-dessus par rigueur mais n'était certainement pas attendu par le concepteur. □

d) On suppose que $n \in \mathbb{N}^*$ et $\mathbb{P}(\,[U_n = 1]\,) = p$.
Déduire de cette hypothèse et de la question précédente :

$$\mathbb{P}_{[U_1=1]}(\,[U_{n+1} = 1]\,) = p \quad \text{et} \quad \mathbb{P}_{[U_1=0]}(\,[U_{n+1} = 1]\,) = p$$

Démonstration.
Déterminons $\mathbb{P}_{[U_1=1]}\big(\,[U_{n+1} = 1]\,\big)$.

- Si l'événement $[U_1 = 1]$ est réalisé, c'est que le premier problème résolu l'a été par le groupe A. Autrement dit, le premier problème résolu est P_1.
  Il reste à déterminer l'ordre de résolution de tous les autres problèmes.
- Pour ce faire, on peut considérer une nouvelle expérience, notée (E_1), commençant à la date de résolution de P_1. Le premier problème fourni au groupe A après cette date est P_2, le suivant P_3, etc. On peut alors noter pour tout $i \in \mathbb{N}^*$:
  - × $A_i = P_{i+1}$, le $i^{\text{ème}}$ problème posé au groupe A lors de l'expérience (E_1).
  - × $W_i = X_{i+1}$, la v.a.r. qui prend pour valeur le temps de résolution du problème A_i.

  Pour le groupe B, la modélisation est un peu différente car le problème Q_1 est encore en cours de résolution à la date de résolution de P_1. À cette date, le groupe B a déjà réfléchi au problème Q_1 pendant un temps X_1. Ce problème ne sera résolu qu'après ajout d'un temps de résolution $Y_1 - X_1$. On note alors $B_1 = Q_1$ le premier problème proposé au groupe B et $Z_1 = Y_1 - X_1$ le temps de résolution de B_1 dans l'expérience (E_1).
  Par ailleurs, on note, pour tout $i \geqslant 2$:
  - × $B_i = Q_i$, le $i^{\text{ème}}$ problème posé au groupe B lors de l'expérience (E_1).
  - × $Z_i = Y_i$, la v.a.r. qui prend pour valeur le temps de résolution du problème B_i.

  Enfin, pour tout $i \in \mathbb{N}^*$, on note V_i la v.a.r. qui prend pour valeur 1 si, lors de l'expérience (E_1), le $i^{\text{ème}}$ problème placé dans la liste a été résolu par le groupe A et qui prend pour valeur 0 dans le cas contraire.
- Résumons les données de la nouvelle expérience (E_1) :
  - × le groupe A doit résoudre dans l'ordre une suite de problèmes $(A_i)_{i\in\mathbb{N}^*}$.
    On a alors noté $(W_i)_{i\in\mathbb{N}^*}$ la suite dont les v.a.r. prennent pour valeur le temps de résolution de ces problèmes par le groupe A.
  - × le groupe B doit résoudre dans l'ordre une suite de problèmes $(B_i)_{i\in\mathbb{N}^*}$.
    On a alors noté $(Z_i)_{i\in\mathbb{N}^*}$ la suite dont les v.a.r. prennent pour valeur le temps de résolution de ces problèmes par le groupe B.
  - × à ce jeu est associé un espace probabilisé $(\Omega, \mathscr{A}, \mathbb{P}_{[U_1=1]})$.
    On peut alors remarquer (démonstration à suivre $(*)$) :
    - ▶ pour tout $i \in \mathbb{N}^*$, W_i suit la loi $\mathcal{E}(p)$ et Z_i suit la loi $\mathcal{E}(q)$.
    - ▶ pour tout $i \in \mathbb{N}^*$, les v.a.r. $W_1, \dots, W_i, Z_1, \dots, Z_i$ sont indépendantes.
- L'expérience (E_1) ayant précisément les mêmes hypothèses que l'expérience de l'énoncé, on peut en conclure :

(probabilité de $[V_n = 1]$ dans l'espace probabilisé associé à (E_1))

$$\begin{array}{ccc} \mathbb{P}_{[U_1=1]}\big(\,[V_n = 1]\,\big) & = & \mathbb{P}\big(\,[U_n = 1]\,\big) \\ \parallel & & \parallel \\ \mathbb{P}_{[U_1=1]}\big(\,[U_{n+1} = 1]\,\big) & & p \end{array}$$

(probabilité de $[U_n = 1]$ dans l'espace probabilisé associé à l'expérience de l'énoncé)

$$\boxed{\mathbb{P}_{[U_1=1]}\big(\,[U_{n+1} = 1]\,\big) = p}$$

- Il reste à démontrer $(*)$:
  - soit $i \in \mathbb{N}^*$. Par définition, $W_i = X_{i+1}$.
    Soit $x \in \mathbb{R}$. On a :

$$\begin{array}{rcl} \mathbb{P}_{[U_1=1]}\big([W_i \leqslant x]\big) & = & \mathbb{P}_{[U_1=1]}\big([X_{i+1} \leqslant x]\big) \\ & = & \mathbb{P}_{[X_1 \leqslant Y_1]}\big([X_{i+1} \leqslant x]\big) \\ & = & \dfrac{\mathbb{P}\big([X_1 - Y_1 \leqslant 0] \cap [X_{i+1} \leqslant x]\big)}{\mathbb{P}\big([X_1 \leqslant Y_1]\big)} \\ & = & \dfrac{\cancel{\mathbb{P}\big([X_1 - Y_1 \leqslant 0]\big)} \times \mathbb{P}\big([X_{i+1} \leqslant x]\big)}{\cancel{\mathbb{P}\big([X_1 \leqslant Y_1]\big)}} \quad \textit{(car les v.a.r. } X_1 - Y_1 \textit{ et } X_{i+1} \textit{ sont indépendantes par le lemme des coalitions)} \\ & = & \mathbb{P}\big([X_{i+1} \leqslant x]\big) \end{array}$$

    Ainsi, la loi de W_i, dans l'espace probabilisé $(\Omega, \mathscr{A}, \mathbb{P}_{[U_1=1]})$ est la loi de la v.a.r. X_i.

$$\boxed{\forall i \in \mathbb{N}^*,\ W_i \hookrightarrow \mathcal{E}(p)}$$

    Par ailleurs, par définition : $Z_1 = Y_1 - X_1$ et : $\forall i \geqslant 2$, $Z_i = Y_i$.

    En question ***8.c)***, on a démontré que la loi conditionnelle de Z_1 sachant $[U_1 = 1]$ est la loi $\mathcal{E}(q)$. Autrement dit, la loi de Z_1 dans l'espace probabilisé $(\Omega, \mathscr{A}, \mathbb{P}_{[U_1=1]})$ est la loi $\mathcal{E}(q)$.
    Enfin, pour tout $i \geqslant 2$ et tout $x \in \mathbb{R}$, on démontre comme au-dessus :

$$\mathbb{P}_{[U_1=1]}\big([Z_i \leqslant x]\big) \ = \ \mathbb{P}\big([Y_i \leqslant x]\big)$$

$$\boxed{\forall i \in \mathbb{N}^*,\ Z_i \hookrightarrow \mathcal{E}(q)}$$

  - pour tout $i \in \mathbb{N}^*$, les v.a.r. $W_1 = X_2, \ldots, W_i = X_{i+1}$, $Z_1 = Y_1 - X_1$, $Z_2 = Y_2, \ldots, Z_i = Y_i$ sont indépendantes d'après le lemme des coalitions et car, par hypothèse de l'énoncé, les v.a.r. $X_1, \ldots, X_i$, $Y_1, \ldots, Y_i$ sont indépendantes.
- La démonstration de : $\mathbb{P}_{[U_1=0]}\big([U_{n+1} = 1]\big) = p$ est en tout point similaire à ce qui précède.
  On se place dans le contexte où le premier problème résolu l'est par le groupe B.
  Mathématiquement, cela revient à considérer l'espace probabilisé $(\Omega, \mathscr{A}, \mathbb{P}_{[U_1=0]})$.
  On s'intéresse alors à la nouvelle expérience (E_0) obtenue en considérant les suites de v.a.r. et de problèmes suivants :
  × $W_1 = X_1 - Y_1$ et $A_1 = P_1$ et : $\forall i \geqslant 2$, $W_i = X_i$ et $A_i = P_i$.
  × $\forall i \in \mathbb{N}^*$, $Z_i = Y_{i+1}$ et $B_i = Q_{i+1}$.
  × pour tout $i \in \mathbb{N}^*$, V_i est la v.a.r. qui prend pour valeur 1 si le $i^{\text{ème}}$ problème de l'expérience a été résolu par le groupe A et, qui prend pour valeur 0 dans le cas contraire.

  La nouvelle expérience (E_0) a précisément les mêmes hypothèses que celles de l'énoncé. Ainsi :

(probabilité de $[V_n = 1]$ dans l'espace probabilisé associé à (E_0))

$$\begin{array}{ccc} \mathbb{P}_{[U_1=0]}\big([V_n = 1]\big) & = & \mathbb{P}\big([U_n = 1]\big) \\ \shortparallel & & \shortparallel \\ \mathbb{P}_{[U_1=0]}\big([U_{n+1} = 1]\big) & & p \end{array}$$

(probabilité de $[U_n = 1]$ dans l'espace probabilisé associé à l'expérience de l'énoncé)

$$\boxed{\mathbb{P}_{[U_1=0]}\big([U_{n+1} = 1]\big) = p}$$

Commentaire

- Si chaque étape de la démonstration est à portée d'un bon élève de classe ECE, la prise d'initiative est beaucoup trop importante pour espérer qu'un élève en vienne à bout. Cette question n'a donc pas le rôle discriminant qu'ont généralement les questions de concours : classer les élèves selon qu'ils ont traité de manière satisfaisante ou non la question.

La présence d'une telle question permet de comprendre la stratégie à adopter lors des concours :

- il est essentiel de savoir repérer les questions les plus difficiles. Elles permettent de discriminer les candidats puisqu'il faut avoir du recul pour juger du niveau d'une question.
- il faut aborder ces questions en ayant en tête que le correcteur sera plus indulgent pour les candidats qui s'y aventurent. Cependant, il ne faut pas perdre du temps à essayer de les traiter jusqu'au bout : le nombre de points alloués ne sera certainement pas à la hauteur du temps investi pour traiter une telle question.

Il ne faut donc pas hésiter à passer les questions les plus difficiles et aller chercher les points où ils sont, à savoir sur les questions plus abordables du sujet.

☐

e) Conclure.

Démonstration.
Il s'agit de démontrer par récurrence : $\forall n \in \mathbb{N}^*$, $\mathcal{P}(n)$ où $\mathcal{P}(n)$: $\mathbb{P}\big([U_n = 1]\big) = p$.

- **Initialisation** :
  D'après la question ***8.a)*** : $\mathbb{P}\big([U_1 = 1]\big) = p$.
  D'où $\mathcal{P}(1)$.
- **Hérédité** : soit $n \in \mathbb{N}^*$.
  Supposons $\mathcal{P}(n)$ et démontrons $\mathcal{P}(n+1)$ (*i.e.* $\mathbb{P}\big([U_{n+1} = 1]\big) = p$).

  Par hypothèse de récurrence, $\mathbb{P}\big([U_n = 1]\big) = p$.
  On peut donc en conclure, d'après la question précédente :

$$\mathbb{P}_{[U_1=1]}([U_{n+1} = 1]) = p \quad \text{et} \quad \mathbb{P}_{[U_1=0]}([U_{n+1} = 1]) = p$$

  La famille $\big([U_1 = 0], [U_1 = 1]\big)$ forme un système complet d'événements.
  On en déduit, par la formule des probabilités totales :

$$\begin{aligned}
\mathbb{P}\big([U_{n+1} = 1]\big) &= \mathbb{P}\big([U_1 = 1] \cap [U_{n+1} = 1]\big) + \mathbb{P}\big([U_1 = 0] \cap [U_{n+1} = 1]\big) \\
&= \mathbb{P}\big([U_1 = 1]\big) \times \mathbb{P}_{[U_1=1]}\big([U_{n+1} = 1]\big) + \mathbb{P}\big([U_1 = 0]\big) \times \mathbb{P}_{[U_1=0]}\big([U_{n+1} = 1]\big) \\
&= p \times p + (1-p) \times p \\
&= \cancel{p^2} + (p - \cancel{p^2})
\end{aligned}$$

  D'où $\mathcal{P}(n+1)$.

$$\boxed{\text{Par principe de récurrence : } \forall n \in \mathbb{N}^*, \mathcal{P}(n).}$$

☐

9. On montrerait aussi par récurrence, et nous l'admettrons, que pour tout $n \in \mathbb{N}^*$, les variables aléatoires $U_1, \ldots, U_n$ sont mutuellement indépendantes.
En déduire la loi de S_n.

Démonstration.

- On a démontré en question ***7.b)*** que, pour tout $n \in \mathbb{N}^*$: $S_n = \sum\limits_{k=1}^{n} U_k$.

- Par ailleurs, par définition, pour tout $k \in \mathbb{N}^*$: $U_k(\Omega) = \{0, 1\}$.
  Ainsi, toutes les v.a.r. de la suite $(U_k)_{k\in\mathbb{N}^*}$ suivent une loi de Bernoulli.
  Or, d'après la question précédente :

$$\forall k \in \mathbb{N}^*, \ \mathbb{P}\big([U_k = 1] \big) = p$$

$$\boxed{\forall k \in \mathbb{N}^*, \ U_k \hookrightarrow \mathcal{B}(p) = \mathcal{B}(1, p).}$$

- Les v.a.r. $U_1, \ldots, U_n$ étant mutuellement indépendantes, on peut conclure, par stabilité par somme des lois binomiales : $\sum\limits_{k=1}^{n} U_k \hookrightarrow \mathcal{B}(1 + \ldots + 1, p)$.

$$\boxed{\forall n \in \mathbb{N}^*, \ \sum_{k=1}^{n} U_k \hookrightarrow \mathcal{B}(n, p).}$$

□

Soit $r \in \mathbb{N}$, on s'intéresse, dans les questions qui suivent, à la probabilité a_r de l'événement :

A_r : « il existe un $n \geqslant r$ tel que, lorsque n problèmes en tout ont été résolus, le groupe A en a résolu r de plus que le groupe B »

10. a) Justifier : $a_0 = 1$.

Démonstration.

- L'événement A_0 est réalisé si et seulement si il existe un entier $n \geqslant 0$ tel que, lorsque n problèmes en tout ont été résolus, le groupe A n'en a résolu aucun de plus que le groupe B.
- Autrement dit, l'événement A_0 est réalisé si et seulement si il existe un moment du jeu au cours duquel le groupe A et le groupe B ont résolu autant de problèmes.
  C'est le cas au tout début de l'expérience : lorsqu'aucun problème n'a été résolu, le groupe A n'a aucune avance sur le groupe B.
- On en conclut que l'événement A_0 est réalisé.

$$\boxed{\text{Ainsi : } A_0 = \Omega \text{ et } \mathbb{P}(A_0) = \mathbb{P}(\Omega) = 1.}$$

□

b) Démontrer, pour tout $r \geqslant 1$:

$$\mathbb{P}_{[U_1=1]}(A_r) = \mathbb{P}(A_{r-1}) \quad \text{et} \quad \mathbb{P}_{[U_1=0]}(A_r) = \mathbb{P}(A_{r+1})$$

Démonstration.
Soit $r \in \mathbb{N}^*$.

- L'événement A_r est réalisé si et seulement si il existe un entier $n \geqslant r$ tel que, lorsque n problèmes en tout ont été résolus, le groupe A en a résolu r de plus que le groupe B.
  Autrement dit, l'événement A_r est réalisé si et seulement si il existe un moment du jeu au cours duquel le groupe A possède une avance de r problèmes sur le groupe B.
- Si l'événement $[U_1 = 1]$ est réalisé, c'est que le premier problème résolu, l'a été par le groupe A. Le groupe A a donc un problème d'avance sur le groupe B au moment où 1 seul problème a été résolu. Dans ce cas, A_r est réalisé si et seulement si, en poursuivant l'expérience, le groupe A parvient à prendre une avance supplémentaire de $r - 1$ problèmes. Cela se produit avec probabilité $\mathbb{P}(A_{r-1})$.

$$\boxed{\text{Finalement : } \forall r \in \mathbb{N}^*, \ \mathbb{P}_{[U_1=1]}(A_r) = \mathbb{P}(A_{r-1}).}$$

- De manière similaire, si l'événement $[U_1 = 0]$ est réalisé, c'est que le premier problème résolu, l'a été par le groupe B. Le groupe B a donc un problème d'avance sur le groupe A au moment où 1 seul problème a été résolu. Dans ce cas, A_r est réalisé si, en poursuivant l'expérience, le groupe A parvient à prendre une avance supplémentaire de $r+1$ problèmes.
  Cela se produit avec probabilité $\mathbb{P}(A_{r+1})$.

$$\boxed{\text{Finalement : } \forall r \in \mathbb{N}^*,\ \mathbb{P}_{[U_1=0]}(A_r) = \mathbb{P}(A_{r+1}).}$$

□

c) En déduire, pour tout $r \geqslant 1$: $a_{r+1} = \dfrac{1}{q}\, a_r - \dfrac{p}{q}\, a_{r-1}$.

Démonstration.
Soit $r \in \mathbb{N}^*$.

- La famille $\big([U_1 = 0], [U_1 = 1]\big)$ est un système complet d'événements.
  On en déduit, par la formule des probabilités totales :

$$\begin{array}{cll} & \mathbb{P}(A_r) & \\ = & \mathbb{P}\big([U_1 = 0] \cap A_r\big) + \mathbb{P}\big([U_1 = 1] \cap A_r\big) & \\ = & \mathbb{P}\big([U_1 = 0]\big) \times \mathbb{P}_{[U_1=0]}\big(A_r\big) + \mathbb{P}\big([U_1 = 1]\big) \times \mathbb{P}_{[U_1=1]}\big(A_r\big) & \textit{(avec } \mathbb{P}\big([U_1 = 0]\big) = 1 - p \neq 0 \\ & & \textit{et } \mathbb{P}\big([U_1 = 1]\big) = p \neq 0\textit{)} \\ = & (1-p) \times \mathbb{P}\big(A_{r+1}\big) + p \times \mathbb{P}\big(A_{r-1}\big) & \textit{(d'après la question précédente)} \\ = & q \times a_{r+1} + p \times a_{r-1} & \end{array}$$

- En réordonnant les termes de l'égalité précédente, on obtient :

$$\begin{array}{lrcl} & q \times a_{r+1} & = & a_r - p \times a_{r-1} \\ \text{donc} & a_{r+1} & = & \dfrac{1}{q}\, a_r - \dfrac{p}{q}\, a_{r-1} \end{array}$$

$$\boxed{\text{On a bien : } \forall r \in \mathbb{N}^*,\ a_{r+1} = \dfrac{1}{q}\, a_r - \dfrac{p}{q}\, a_{r-1}.}$$

□

d) En remarquant que $1 - 4pq = (1-2p)^2$, donner une expression de a_r en fonction de p, q, r et de deux constantes que l'on introduira.

Démonstration.

- Remarquons tout d'abord :

$$\begin{array}{rcl} 1 - 4\,p\,q & = & 1 - 4\,p\,(1-p) \\ & = & 1 - (4\,p - 4\,p^2) \\ & = & 1 - 4\,p + 4\,p^2 \\ & = & (1 - 2\,p)^2 \end{array}$$

$$\boxed{1 - 4\,p\,q = (1 - 2\,p)^2}$$

- La suite $(a_r)_{r \in \mathbb{N}}$ vérifie : $\forall r \in \mathbb{N},\ a_{r+2} = \dfrac{1}{q}\, a_{r+1} - \dfrac{p}{q}\, a_r$.
  C'est donc une suite récurrente linéaire d'ordre 2.

– L'équation caractéristique associée à la suite $(a_r)_{r\in\mathbb{N}}$ est : $x^2 = \frac{1}{q}\,x - \frac{p}{q}$.
Notons P le polynôme : $P(X) = X^2 - \frac{1}{q}\,X + \frac{p}{q}$.
Ce polynôme admet pour discriminant :

$$\Delta \;=\; \left(-\frac{1}{q}\right)^2 - 4\times 1\times\left(\frac{p}{q}\right) \;=\; \frac{1}{q^2} - \frac{4p}{q} \;=\; \frac{1-4\,pq}{q^2} \;=\; \frac{(1-2\,p)^2}{q^2} \;=\; \left(\frac{1-2\,p}{q}\right)^2$$

Comme $\Delta \geqslant 0$, ce polynôme admet deux racines (éventuellement égales) :

$$x_+ \;=\; \frac{-\left(-\frac{1}{q}\right)+\sqrt{\Delta}}{2} \;=\; \frac{\frac{1}{q}+\frac{|1-2p|}{q}}{2} \;=\; \frac{1+|1-2p|}{2\,q}$$

$$\text{et} \quad x_- \;=\; \frac{-\left(-\frac{1}{q}\right)-\sqrt{\Delta}}{2} \;=\; \frac{\frac{1}{q}-\frac{|1-2p|}{q}}{2} \;=\; \frac{1-|1-2p|}{2\,q}$$

Remarquons alors :

× si $p > \frac{1}{2}$ $(\Delta > 0)$ alors $1-2\,p \leqslant 0$ et $|1-2p| = -(1-2\,p) = -1+2\,p$. Ainsi :

$$x_+ = \frac{\cancel{1}-\cancel{1}+2\,p}{2\,q} = \frac{p}{q} \qquad \text{et} \qquad x_- = \frac{1+1-2\,p}{2\,q} = \frac{2\,(1-p)}{2\,q} = 1$$

× si $p < \frac{1}{2}$ $(\Delta > 0)$ alors $1-2\,p > 0$ et $|1-2p| = 1-2\,p$. Ainsi :

$$x_+ = \frac{1+1-2\,p}{2\,q} = \frac{2\,(1-p)}{2\,q} = 1 \qquad \text{et} \qquad x_- = \frac{\cancel{1}-\cancel{1}+2\,p}{2\,q} = \frac{p}{q}$$

× si $p = \frac{1}{2}$ $(\Delta = 0)$ alors :

$$x_+ = x_- = \frac{1}{2\,q} = \frac{1}{2\,(1-p)} = \frac{1}{2\,\frac{1}{2}} = 1$$

$$\boxed{\begin{array}{c}\text{Ainsi, si } p \neq \frac{1}{2},\ P \text{ possède deux racines distinctes : } 1 \text{ et } \frac{p}{q}.\\ \text{Et si } p = \frac{1}{2},\ P \text{ possède une racine double : } 1.\end{array}}$$

Commentaire

- On pouvait aussi remarquer que le réel 1 est racine de P puisque :

$$P(1) = 1 - \frac{1}{q} + \frac{p}{q} = \frac{q-1+p}{q} = \frac{(p+q)-1}{q} = 0$$

  Ainsi, on peut factoriser le polynôme P comme suit :

$$P(X) = (X-1)\left(X - \frac{p}{q}\right)$$

  On retrouve alors que la $2^{\text{ème}}$ racine de P est $\frac{p}{q}$.
- La formulation de l'énoncé (qui demande de démontrer au préalable : $1-4p\,q = (1-2\,p)^2$), nous incite à rédiger en passant par le calcul du discriminant de P.
  Cela a du sens car la racine 1 n'est peut-être pas si évidente.

– Deux cas se présentent alors :

▸ si $\Delta = 0$, c'est-à-dire si $p = \frac{1}{2}$, la formule explicite de $(a_r)_{r\in\mathbb{N}}$ est donnée par :

$$\forall r \in \mathbb{N},\ a_r = \lambda \times (1)^r + \mu \times r \times (1)^r = \lambda + \mu\ r$$

$$\boxed{\text{Si } p = \tfrac{1}{2} : \forall r \in \mathbb{N},\ a_r = \lambda + \mu\ r.}$$

▸ si $\Delta > 0$, c'est-à-dire si $p \neq \frac{1}{2}$, la formule explicite de $(a_r)_{r\in\mathbb{N}}$ est donnée par :

$$\forall r \in \mathbb{N},\ a_r = \lambda \times (1)^r + \mu \times \left(\frac{p}{q}\right)^r = \lambda + \mu \times \left(\frac{p}{q}\right)^r$$

$$\boxed{\text{Si } p \neq \tfrac{1}{2} : \forall r \in \mathbb{N},\ a_r = \lambda + \mu\ \left(\tfrac{p}{q}\right)^r.}$$

□

11. Le cas $p \geqslant \dfrac{1}{2}$.

Montrer que, dans les cas $p = \dfrac{1}{2}$ et $p > \dfrac{1}{2}$, la suite $(a_r)_{r\in\mathbb{N}}$ est constante et égale à 1.

Démonstration.

Deux cas se présentent.

- Si $p = \frac{1}{2}$ alors, d'après la question précédente :

$$\forall r \in \mathbb{N},\ a_r = \lambda + \mu\ r$$

Démontrons alors : $\mu = 0$. On procède par l'absurde.

Supposons : $\mu \neq 0$. Alors :

× si $\mu > 0$, $\lim\limits_{r\to+\infty} a_r \ = \ \lim\limits_{r\to+\infty} (\lambda + \mu\ r) \ = \ +\infty$

× si $\mu < 0$, $\lim\limits_{r\to+\infty} a_r \ = \ \lim\limits_{r\to+\infty} (\lambda + \mu\ r) \ = \ -\infty$

Or, la suite $(a_r)_{r\in\mathbb{N}}$ est bornée :

$$\forall r \in \mathbb{N},\quad 0 \ \leqslant \ \underset{\displaystyle a_r}{\underset{\shortparallel}{\mathbb{P}(A_r)}} \ \leqslant \ 1$$

On en déduit que si $(a_r)_{r\in\mathbb{N}}$ admet une limite, celle-ci est forcément finie.
C'est impossible lorsque $\mu \neq 0$, d'après ce qui précède.

$$\boxed{\text{Ainsi, si } p = \tfrac{1}{2}, \text{ alors } \mu = 0 \text{ et : } \forall r \in \mathbb{N},\ a_r = \lambda.}$$

La valeur de λ est obtenue en considérant $r = 0$. On obtient : $\lambda = a_0 = 1$ (d'après ***10.a)***).

$$\boxed{\text{Ainsi, si } p = \tfrac{1}{2} : \forall r \in \mathbb{N},\ a_r = 1.}$$

- Si $p > \frac{1}{2}$ alors, d'après la question précédente :

$$\forall r \in \mathbb{N},\ a_r = \lambda + \mu \times \left(\frac{p}{q}\right)^r$$

Remarquons tout d'abord :

$$\begin{array}{lll} \text{Comme } p > \frac{1}{2} & \text{alors} & q < \frac{1}{2} \\[2mm] & \text{donc} & \frac{1}{q} > 2 \\[2mm] & \text{donc} & \frac{p}{q} > 1 \end{array}$$

Démontrons alors : $\mu = 0$. On procède par l'absurde.

Supposons : $\mu \neq 0$. Alors :

× si $\mu > 0$, comme $\frac{p}{q} > 1$ alors : $\lim\limits_{r \to +\infty} a_r = \lim\limits_{r \to +\infty} \left(\lambda + \mu \times \left(\frac{p}{q}\right)^r\right) = +\infty$

× si $\mu < 0$, , comme $\frac{p}{q} > 1$ alors : $\lim\limits_{r \to +\infty} a_r = \lim\limits_{r \to +\infty} \left(\lambda + \mu \times \left(\frac{p}{q}\right)^r\right) = -\infty$

Comme précisé, dans le point précédent, ceci est impossible car la suite $(a_r)_{r\in\mathbb{N}}$ est bornée.

$$\boxed{\text{On en conclut, comme au point précédent, } \mu = 0 \text{ et : } \forall r \in \mathbb{N},\ a_r = \lambda = 1.}$$

□

12. Le cas $p < \dfrac{1}{2}$.

a) Soit k un entier naturel.

(i) Établir : $A_{2k} = \bigcup\limits_{i \geqslant k} [S_{2i} = i + k]$.

Démonstration.

- Rappelons tout d'abord que, pour tout $n \in \mathbb{N}$, S_n prend pour valeur le nombre de problèmes résolus par A lorsque n problèmes en tout ont été résolus.
- Remarquons alors :

L'événement A_{2k} est réalisé

$\Leftrightarrow$ Il existe un entier $n \geqslant 2k$ tel que, lorsque n problèmes en tout ont été résolus, le groupe A en a résolu $2k$ de plus que le groupe B

$\Leftrightarrow$ Il existe un moment du jeu au cours duquel le groupe A possède une avance de $2k$ problèmes sur le groupe B

$\Leftrightarrow$ Il existe un entier $j \in \mathbb{N}$ tel que
× B a résolu j problèmes
× A a résolu $j + 2k$ problèmes

alors que $j + (j + 2k) = 2j + 2k$ problèmes ont été résolus en tout

$\Leftrightarrow$ Il existe $j \in \mathbb{N}$ tel que, lorsque $2j + 2k$ problèmes en tout ont été résolus, $j + 2k$ l'ont été par le groupe A

$\Leftrightarrow$ Il existe $j \in \mathbb{N}$ tel que, S_{2j+2k} prend pour valeur $j + 2k$

$\Leftrightarrow$ Il existe $j \in \mathbb{N}$ tel que, $[S_{2j+2k} = j + 2k]$ est réalisé

$\Leftrightarrow$ L'événement $\bigcup\limits_{j \in \mathbb{N}} [S_{2j+2k} = j + 2k]$ est réalisé

On en déduit :

$$\begin{aligned} A_{2k} &= \bigcup_{j=0}^{+\infty} [S_{2j+2k} = j + 2k] \\ &= \bigcup_{i=k}^{+\infty} [S_{2i} = i + k] \qquad \textit{(avec le changement d'indice } i = j + k\textit{)} \end{aligned}$$

$$\boxed{A_{2k} = \bigcup_{i=k}^{+\infty} [S_{2i} = i + k]}$$

□

(ii) Montrer que pour tout $i \geqslant k$, on a : $\mathbb{P}(\,[S_{2i} = i+k]\,) = \dbinom{2i}{i+k} p^{i+k}\, q^{i-k}$.

Démonstration.
Soit $i \geqslant k$.

- D'après la question ***9.***, $S_{2i} \hookrightarrow \mathcal{B}\,(2i, p)$. Ainsi :

$$\forall j \in [\![0, 2i]\!],\ \mathbb{P}\big(\,[S_{2i} = j]\,\big) = \binom{2i}{j} p^j\, q^{2i-j}$$

- Comme $k \in [\![0, i]\!]$, alors on peut appliquer cette égalité en $j = i + k \in [\![0, 2i]\!]$. On obtient :

$$\mathbb{P}\big(\,[S_{2i} = i+k]\,\big) \ = \ \binom{2i}{i+k} p^{i+k}\, q^{2i-(i+k)} \ = \ \binom{2i}{i+k} p^{i+k}\, q^{i-k}$$

$$\boxed{\forall i \geqslant k,\ \mathbb{P}\big(\,[S_{2i} = i+k]\,\big) \ = \ \binom{2i}{i+k} p^{i+k}\, q^{i-k}}$$

□

(iii) Après avoir donné la valeur de la somme $\sum\limits_{j=0}^{2i} \dbinom{2i}{j}$, démontrer :

$$\forall i \geqslant k,\ \binom{2i}{i+k} \leqslant 4^i$$

Démonstration.

- Tout d'abord :

$$\begin{array}{rcll} \sum\limits_{j=0}^{2i} \dbinom{2i}{j} & = & \sum\limits_{j=0}^{2i} \dbinom{2i}{j} 1^j \times 1^{2i-j} & \\ & = & (1+1)^{2i} & \textit{(par la formule du binôme de Newton)} \\ & = & 2^{2i} \ = \ \left(2^2\right)^i \ = \ 4^i & \end{array}$$

$$\boxed{\sum_{j=0}^{2i} \binom{2i}{j} = 4^i}$$

- Tous les termes cette somme étant positifs, on en déduit :

$$\binom{2i}{i+k} \ \leqslant \ \left(\sum_{j=0}^{i+k-1} \binom{2i}{j}\right) + \binom{2i}{i+k} + \left(\sum_{j=i+k+1}^{2i} \binom{2i}{j}\right) \ = \ \sum_{j=0}^{2i} \binom{2i}{j} \ = \ 4^i$$

$$\boxed{\text{Ainsi : } \forall i \geqslant k,\ \binom{2i}{i+k} \ \leqslant \ 4^i.}$$

□

(iv) En déduire l'inégalité :

$$\sum_{i=k}^{+\infty} \mathbb{P}(\,[S_{2i}=k+i]\,) \ \leqslant\ \left(\frac{p}{q}\right)^k \ \frac{(4pq)^k}{1-4pq}$$

Démonstration.

- Tout d'abord, pour tout $i \geqslant k$:

$$\begin{aligned} \mathbb{P}\big(\,[S_{2i}=k+i]\,\big) &= \binom{2i}{i+k}\, p^{i+k}\, q^{i-k} && \textit{(d'après la question } \textbf{\textit{12.a)(ii)}}\textit{)} \\ &= p^k\, q^{-k} \binom{2i}{i+k}\, p^i\, q^i \\ &= \left(\frac{p}{q}\right)^k \binom{2i}{i+k}\, p^i\, q^i \\ &\leqslant \left(\frac{p}{q}\right)^k 4^i\, p^i\, q^i \ = \ \left(\frac{p}{q}\right)^k \big(4\,p\,q\big)^i \end{aligned}$$

$$\boxed{\forall i \geqslant k,\ \mathbb{P}\big(\,[S_{2i}=k+i]\,\big) \ \leqslant\ \left(\frac{p}{q}\right)^k \big(4\,p\,q\big)^i \quad (*)}$$

- La série $\sum\limits_{i} \big(4\,p\,q\big)^i$ est une série géométrique de raison $4\,p\,q$. Or :

$$4\,p\,q \ = \ 4\,p\,(1-p) \ \leqslant\ 4 \times \frac{1}{4} \qquad \textit{(d'après l'inégalité classique obtenue par l'étude de la fonction polynomiale } x \mapsto x\,(1-x)\textit{)}$$

  Notons que l'égalité n'a lieu que si $p=\frac{1}{2}$, ce qui est exclu (on traite le cas $p<\frac{1}{2}$ dans cette question ***12.***). Comme de plus $p \neq 0$ et $q \neq 0$, on en conclut : $4\,p\,q \in \,]0,1[$.
  Ainsi, la série $\sum\limits_{i} \big(4\,p\,q\big)^i$ est convergente.
  On en déduit alors, par l'inégalité $(*)$ et par critère de comparaison des séries à termes positifs, que la série $\sum\limits_{i \geqslant k} \mathbb{P}\big(\,[S_{2i}=k+i]\,\big)$ est aussi convergente.

- Ainsi, en sommant les inégalités $(*)$ on obtient :

$$\begin{aligned} \sum_{i=k}^{+\infty} \mathbb{P}\big(\,[S_{2i}=k+i]\,\big) &\leqslant \sum_{i=k}^{+\infty} \left(\frac{p}{q}\right)^k \big(4\,p\,q\big)^i \\ &= \left(\frac{p}{q}\right)^k \sum_{i=k}^{+\infty} \big(4\,p\,q\big)^i \\ &= \left(\frac{p}{q}\right)^k \sum_{i=0}^{+\infty} \big(4\,p\,q\big)^{i+k} && \textit{(par décalage d'indice)} \\ &= \left(\frac{p}{q}\right)^k \big(4\,p\,q\big)^k \sum_{i=0}^{+\infty} \big(4\,p\,q\big)^i \\ &= \left(\frac{p}{q}\right)^k \big(4\,p\,q\big)^k \frac{1}{1-4\,p\,q} \end{aligned}$$

$$\boxed{\sum_{i=k}^{+\infty} \mathbb{P}(\,[S_{2i}=k+i]\,) \ \leqslant\ \left(\frac{p}{q}\right)^k \ \frac{(4pq)^k}{1-4pq}}$$

□

b) Montrer en utilisant l'inégalité de Boole (voir question ***6.***) que si $p < \dfrac{1}{2}$, alors : $\displaystyle\lim_{k\to+\infty} a_{2k} = 0$.

Démonstration.

- D'après la question ***12.a)(i)***, pour tout $k \in \mathbb{N}$:

$$A_{2k} \ = \ \bigcup_{i=k}^{+\infty} [S_{2i} = i+k]$$

- La série $\sum\limits_{i\geqslant k} \mathbb{P}([S_{2i} = i+k])$ est convergente d'après la question précédente.
  On en déduit, par l'inégalité de Boole (question ***6.b)***) :

$$\begin{aligned} \mathbb{P}\left(\bigcup_{i=k}^{+\infty} [S_{2i} = i+k]\right) \ &\leqslant \ \sum_{i=k}^{+\infty} \mathbb{P}\big(\,[S_{2i} = i+k]\,\big) \\ &\leqslant \ \left(\frac{p}{q}\right)^k \ \frac{(4pq)^k}{1-4pq} \qquad \textit{(d'après la question précédente)} \end{aligned}$$

- On en conclut :

$$0 \ \leqslant \ \mathbb{P}(A_{2k}) \ \leqslant \ \left(\frac{p}{q}\right)^k \ \frac{(4pq)^k}{1-4pq}$$

  Or :
  × $\displaystyle\lim_{k\to+\infty} 0 = 0$,
  × $\displaystyle\lim_{k\to+\infty} \left(\frac{p}{q}\right)^k \ \frac{(4pq)^k}{1-4pq} = 0$ car
    ▸ $\displaystyle\lim_{k\to+\infty} (4pq)^k = 0$ car $4pq \in \,]0,1[$ (d'après la question précédente)
    ▸ $\displaystyle\lim_{k\to+\infty} \left(\frac{p}{q}\right)^k = 0$ car $\frac{p}{q} \in \,]0,1[$ (par une méthode similaire à la question ***11.***)

  Ainsi, par théorème d'encadrement, la suite $(a_{2k})_{k\in\mathbb{N}}$ est convergente, de limite nulle. □

c) Conclure en utilisant la question ***10.d)***, que si $p < \dfrac{1}{2}$, alors : $\forall r \in \mathbb{N},\ a_r = \left(\dfrac{p}{q}\right)^r$.

Démonstration.

- En question ***10.d)***, on a démontré : $\forall r \in \mathbb{N},\ a_r = \lambda + \mu\ \left(\frac{p}{q}\right)^r$.
  Ainsi, pour tout $k \in \mathbb{N}$, en appliquant l'égalité précédente à $r = 2k \in \mathbb{N}$, on obtient :

$$a_{2k} = \lambda + \mu\ \left(\frac{p}{q}\right)^{2k}$$

- Or, comme vu dans la question précédente : $\displaystyle\lim_{k\to+\infty} \left(\frac{p}{q}\right)^{2k} = 0$.
  On en déduit : $\displaystyle\lim_{k\to+\infty} a_{2k} = \lambda$.

  Par unicité de la limite, on en déduit $\lambda = 0$ et : $\forall r \in \mathbb{N},\ a_r = \mu\ \left(\dfrac{p}{q}\right)^r$.

- Enfin, en appliquant cette égalité en $r = 0$, on obtient : $a_0 = \mu$.

  Comme $a_0 = 1$, on a bien : $\forall r \in \mathbb{N},\ a_r = \left(\dfrac{p}{q}\right)^r$. □

On a ainsi établi dans les questions ***11.*** et ***12.*** :

$$\forall r \in \mathbb{N}, \quad a_r = \begin{cases} \left(\dfrac{p}{q}\right)^r & \text{si } p < \dfrac{1}{2} \\ 1 & \text{si } p \geqslant \dfrac{1}{2} \end{cases}$$

Ce résultat pourra être admis et utilisé dans la suite du sujet.

Partie III - La *blockchain* et la stratégie de la *double dépense*

On utilise, dans cette partie, les notations et résultats de la partie **II**.

Soit n un entier supérieur ou égal à 1.

La *blockchain* est formée d'une suite de blocs, chacun associé à plusieurs transactions. Elle contient l'historique de toutes les transactions effectuées depuis la création du *bitcoin*.

Avant d'être placé dans la *blockchain*, un nouveau bloc doit être validé. Cette validation nécessite la mise en oeuvre d'une grande puissance de calcul pour résoudre un problème dépendant fortement du contenu du bloc et des blocs qui le précèdent.

Les individus qui valident les blocs sont appelés mineurs.

Il est possible qu'à un instant donné, coexistent sur le réseau deux *blockchains*, valides et différentes. Dans ce cas, le réseau choisira celle qui comporte le plus de blocs et l'autre sera abandonnée.

Par prudence, lorsqu'un bloc est validé, il est recommandé d'attendre que $n-1$ blocs le suivant soient aussi validés pour considérer que les transactions incluses dans le bloc soient honnêtes.

Un groupe de mineurs mal intentionnés, noté A, peut essayer de dépenser deux fois les mêmes *bitcoins* en procédant ainsi :

- le groupe A demande la validation de l'achat d'un bien d'un montant de s *bitcoins* qu'il a en sa possession.
- lorsque le bloc K incluant cette transaction est proposé à la validation sur le réseau, A modifie ce bloc en K', qu'il ne diffuse pas, en remplaçant l'achat par une vente des s *bitcoins* en euros à son profit par exemple. Il se met alors à la validation de ce nouveau bloc et crée ainsi une deuxième instance de la *blockchain* qu'il continue à développer sans la diffuser.
- lorsque le groupe B, représentant l'ensemble des autres mineurs du réseau, a validé K ainsi que les $n-1$ blocs suivants, le vendeur du bien considère que la transaction est valide et fournit le bien.
- le groupe A attend alors d'avoir une *blockchain* plus longue que celle de B, qui est publique, pour la diffuser donc invalider la *blockchain* publique et l'achat du bien. Le crédit en *bitcoins* du vendeur du bien est alors annulé.

On reprend et on complète la modélisation de la partie précédente pour déterminer la probabilité que la stratégie de la *double dépense* réussisse et le choix de n pour que cette probabilité soit faible.

Une première phase du jeu, décrit dans la partie **II**, s'achève à l'instant aléatoire t où le problème Q_n est ajouté à la liste des problèmes résolus.

Le groupe de mineurs A est ensuite déclaré vainqueur s'il se trouve un instant $t' \geqslant t$ où le nombre de problèmes résolus par A dans la liste des problèmes résolus depuis le début du jeu, est strictement supérieur au nombre de ceux résolus par B dans cette même liste. On note G_n cet événement.

On détermine, dans cette partie, la probabilité de G_n en fonction de n et de p.

13. On s'intéresse tout d'abord à la loi de la variable aléatoire T_n égale au nombre de problèmes résolus par le groupe A lorsque l'on place Q_n dans la liste des problèmes résolus.

a) Démontrer, pour tout $k \in \mathbb{N}$: $[T_n = k] = [S_{n+k-1} = k] \cap [U_{n+k} = 0]$.

Démonstration.
Soit $k \in \mathbb{N}$.

	L'événement $[S_{n+k-1} = k] \cap [U_{n+k} = 0]$ est réalisé		
$\Leftrightarrow$	L'événement $[S_{n+k-1} = k]$ est réalisé	ET	l'événement $[U_{n+k} = 0]$ est réalisé
$\Leftrightarrow$	Dans les $n + k - 1$ premiers problèmes résolus, k l'ont été par le groupe A	ET	le $(n + k)^{\text{ème}}$ problème a été résolu par le groupe B
$\Leftrightarrow$	Sur les $n + k - 1$ premiers problèmes, k ont été résolus par le groupe A, et $n - 1$ l'ont été par le groupe B	ET	le problème suivant (le $(n + k)^{\text{ème}}$) a été résolu par le groupe B (qui a donc résolu n problèmes en tout sur les $n + k$ premiers)
$\Leftrightarrow$	Sur les $n + k - 1$ premiers problèmes, k ont été résolus par le groupe A	ET	Q_n est le $(n + k)^{\text{ème}}$ problème résolu
$\Leftrightarrow$	Lorsque Q_n apparaît dans la liste des problèmes résolus (c'est le $(n + k)^{\text{ème}}$ résolu), k problèmes ont été résolus par le groupe A		
$\Leftrightarrow$	L'événement $[T_n(\omega) = k]$ est réalisé		

$$\boxed{\text{On en déduit : } [T_n = k] = [S_{n+k-1} = k] \cap [U_{n+k} = 0].}$$

□

b) En déduire : $\mathbb{P}(\,[T_n = k]\,) = \binom{n+k-1}{k} p^k\, q^n$.

Démonstration.
Soit $k \in \mathbb{N}$.

- D'après la question précédente :

$$\mathbb{P}([T_n = k]) \;=\; \mathbb{P}([S_{n+k-1} = k] \cap [U_{n+k} = 0])$$

- Or, d'après la question ***9.*** : $S_{n+k-1} = \sum\limits_{i=1}^{n+k-1} U_i$.
  Ainsi, par lemme des coalitions, les v.a.r. S_{n+k-1} et U_{n+k} sont indépendantes.
- On en déduit :

$$\begin{aligned}
\mathbb{P}([T_n = k]) &= \mathbb{P}([S_{n+k-1} = k]) \times \mathbb{P}([U_{n+k} = 0]) \\
&= \binom{n+k-1}{k} p^k\, q^{(n+\cancel{k}-1)-\cancel{k}} \times q \qquad \textit{(d'après les questions \textbf{8.} et \textbf{9.})} \\
&= \binom{n+k-1}{k} p^k\, q^n
\end{aligned}$$

$$\boxed{\forall k \in \mathbb{N},\ \mathbb{P}(\,[T_n = k]\,) = \binom{n+k-1}{k} p^k\, q^n}$$

□

14. a) En utilisant la formule des probabilités totales, établir :

$$\mathbb{P}(G_n) \;=\; \mathbb{P}(\,[T_n \geqslant n+1]\,) + \sum_{k=0}^{n} \mathbb{P}(\,[T_n = k]\,)\, a_{n+1-k}$$

Démonstration.

- Le famille $\big(\,[T_n = k]\,\big)_{k\in\mathbb{N}}$ forme un système complet d'événements.
Par formule des probabilités totales :

$$\begin{aligned} \mathbb{P}(G_n) &= \sum_{k=0}^{+\infty} \mathbb{P}([T_n = k] \cap G_n) \\ &= \sum_{k=0}^{+\infty} \mathbb{P}([T_n = k])\, \mathbb{P}_{[T_n=k]}(G_n) \quad \textit{(car : } \forall k \in \mathbb{N},\ \mathbb{P}([T_n = k]) \neq 0\textit{)} \end{aligned}$$

- Soit $k \in \mathbb{N}$.
Si l'événement $[T_n = k]$ est réalisé, c'est que, lorsque Q_n est résolu par le groupe B, le groupe A a déjà résolu k problèmes. Deux cas se présentent alors :
  - × si $k \in [\![0, n]\!]$, alors l'événement G_n est réalisé si et seulement s'il existe un instant $t' \geqslant t$ où le nombre de problèmes résolus par le groupe A est strictement supérieur au nombre de problèmes résolus par le groupe B
(on rappelle que t est l'instant où le problème Q_n est résolu par le groupe B)

    Comme l'événement $[T_n = k]$ est réalisé, à l'instant t :
    - le groupe A a résolu k problèmes ($k \in [\![0, n]\!]$)
    - le groupe B a résolu n problèmes.

    Le groupe A a donc $n-k$ problèmes de retard sur le groupe B. L'événement G_n est donc réalisé si et seulement s'il existe $t' \geqslant t$ où le groupe A a résolu $n-k+1$ problèmes de plus que le groupe B, c'est-à-dire si et seulement si l'événement A_{n-k+1} est réalisé.

    $$\boxed{\text{On en déduit : } \mathbb{P}_{[T_n=k]}(G_n) \;=\; \mathbb{P}(A_{n-k+1}) \;=\; a_{n-k+1}.}$$

  - × si $k \in [\![n+1, +\infty[\![$, alors l'événement G_n est toujours réalisé. En effet, à l'instant T où le problème Q_n est résolu par le groupe B :
    - le groupe A a résolu k problèmes ($k > n$)
    - le groupe B a résolu n problèmes.

    $$\boxed{\text{On en déduit : } \mathbb{P}_{[T_n=k]}(G_n) = 1.}$$

- On en conclut :

$$\begin{aligned} \mathbb{P}(G_n) &= \sum_{k=0}^{n} \mathbb{P}([T_n = k])\, \mathbb{P}_{[T_n=k]}(G_n) + \sum_{k=n+1}^{+\infty} \mathbb{P}([T_n = k])\, \mathbb{P}_{[T_n=k]}(G_n) \\ &= \sum_{k=0}^{n} \mathbb{P}([T_n = k])\, a_{n+1-k} + \sum_{k=n+1}^{+\infty} \mathbb{P}([T_n = k]) \\ &= \sum_{k=0}^{n} \mathbb{P}([T_n = k])\, a_{n+1-k} + \mathbb{P}([T_n \geqslant n+1]) \end{aligned}$$

$$\boxed{\text{Finalement : } \mathbb{P}(G_n) \;=\; \mathbb{P}(\,[T_n \geqslant n+1]\,) + \sum_{k=0}^{n} \mathbb{P}(\,[T_n = k]\,)\, a_{n+1-k}.}$$

□

b) Dans le cas où $p \geqslant \dfrac{1}{2}$, en déduire : $\mathbb{P}(G_n) = 1$.

Démonstration.
Supposons : $p \geqslant \dfrac{1}{2}$.

- Soit $k \in [\![0, n]\!]$. Comme $n - k + 1 \in \mathbb{N}$, d'après le résultat établi en fin de **Partie II** :

$$a_{n+1-k} \ = \ 1$$

Commentaire

- Citer les hypothèses d'un théorème avant son utilisation est **indispensable**. Lorsque ce théorème n'est pas un résultat du cours mais un résultat démontré dans un sujet de concours, ce réflexe doit perdurer.
- On utilise par exemple dans cette question un résultat démontré dans la partie précédente. On n'omettra donc en aucun cas de vérifier que l'on est placé dans le bon cadre d'application de cette propriété (ici $r = n + 1 - k \in \mathbb{N}$).

- On obtient, d'après la question précédente :

$$\begin{aligned}
\mathbb{P}(G_n) &= \sum_{k=0}^{n} \mathbb{P}([T_n = k]) \times 1 + \mathbb{P}([T_n \geqslant n+1]) \\
&= \sum_{k=0}^{n} \mathbb{P}([T_n = k]) + \sum_{k=n+1}^{+\infty} \mathbb{P}([T_n = k]) \\
&= \sum_{k=0}^{+\infty} \mathbb{P}([T_n = k]) \\
&= 1 && \textit{(car } \big([T_n = k] \big)_{k\in\mathbb{N}} \textit{ forme un système complet d'événements)}
\end{aligned}$$

$$\boxed{\mathbb{P}(G_n) = 1}$$

□

c) De même lorsque $p < \dfrac{1}{2}$, démontrer :

$$\mathbb{P}(G_n) \ = \ 1 - \sum_{k=0}^{n} \binom{n+k-1}{k} \left(p^k\, q^n - p^{n+1}\, q^{k-1}\right)$$

Démonstration.
Supposons : $p < \dfrac{1}{2}$.

- Tout d'abord, d'après la question ***14.a)*** :

$$\mathbb{P}(G_n) \ = \ \mathbb{P}([T_n \geqslant n+1]) + \sum_{k=0}^{n} \mathbb{P}([T_n = k])\, a_{n+1-k}$$

- De plus :

$$\begin{aligned}
\mathbb{P}([T_n \geqslant n+1]) &= 1 - \mathbb{P}([T_n < n+1]) \\
&= 1 - \mathbb{P}([T_n \leqslant n]) && \textit{(car } T_n \textit{ est à valeurs entières)} \\
&= 1 - \sum_{k=0}^{n} \mathbb{P}([T_n = k])
\end{aligned}$$

- On obtient :

$$\begin{array}{rcl}
\mathbb{P}(G_n) & = & 1 - \sum\limits_{k=0}^{n} \mathbb{P}([T_n = k]) + \sum\limits_{k=0}^{n} \mathbb{P}([T_n = k])\, a_{n+1-k} \\
& = & 1 - \sum\limits_{k=0}^{n} \mathbb{P}([T_n = k])\, (1 - a_{n+1-k}) \\
& = & 1 - \sum\limits_{k=0}^{n} \mathbb{P}([T_n = k]) \left(1 - \left(\dfrac{p}{q}\right)^{n+1-k}\right) \qquad \textit{(d'après le résultat de fin de } \textbf{Partie II}\textit{, car } n+1-k \in \mathbb{N}\textit{)} \\
& = & 1 - \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} p^k\, q^n \left(1 - \dfrac{p^{n+1-k}}{q^{n+1-k}}\right) \qquad \textit{(d'après } \textbf{\textit{13.b)}}\textit{)} \\
& = & 1 - \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} \left(p^k\, q^n - \dfrac{p^{n+1}}{q^{1-k}}\right)
\end{array}$$

$$\boxed{\text{Finalement : } \mathbb{P}(G_n) = 1 - \sum_{k=0}^{n} \binom{n+k-1}{k} \left(p^k\, q^n - p^{n+1}\, q^{k-1}\right).}$$

□

15. *Une meilleure expression de* $\mathbb{P}(G_n)$ *lorsque* $p < \dfrac{1}{2}$

Pour tout $x \in [0,1]$ et $n \in \mathbb{N}^*$, on pose :

$$u_n(x) \ = \ (1-x)^n \sum_{k=0}^{n} \binom{n+k-1}{k} x^k$$

a) Vérifier que pour tout $n \in \mathbb{N}^*$: $\mathbb{P}(G_n) = 1 - u_n(p) + \dfrac{p}{q}\, u_n(q)$.

Démonstration.
Soit $n \in \mathbb{N}^*$.

$$\begin{array}{rl}
& 1 - u_n(p) + \dfrac{p}{q}\, u_n(q) \\
= & 1 - (1-p)^n \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} p^k + \dfrac{p}{q}\, (1-q)^n \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} q^k \\
= & 1 - q^n \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} p^k + \dfrac{p}{q}\, p^n \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} q^k \\
= & 1 - \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} p^k\, q^n + \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} p^{n+1}\, q^{k-1} \\
= & 1 - \sum\limits_{k=0}^{n} \dbinom{n+k-1}{k} \left(p^k\, q^n - p^{n+1}\, q^{k-1}\right) \\
= & \mathbb{P}(G_n) \qquad \textit{d'après } \textbf{\textit{14.c)}}
\end{array}$$

$$\boxed{\forall n \in \mathbb{N}^*,\ \mathbb{P}(G_n) = 1 - u_n(p) + \frac{p}{q}\, u_n(q)}$$

□

b) Pour tout $x \in [0,1]$ et $n \in \mathbb{N}^*$, établir la relation :

$$u_{n+1}(x) \; = \; u_n(x) + (1-x)^n \, x^{n+1} \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} \, x \right)$$

Démonstration.
Soit $x \in [0,1]$. Soit $n \in \mathbb{N}^*$.

- Tout d'abord :

$$\begin{aligned}
& u_{n+1}(x) \\
= \; & (1-x)^{n+1} \sum_{k=0}^{n+1} \binom{(n+\cancel{1}) + k - \cancel{1}}{k} \, x^k \\
= \; & (1-x)\,(1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k \\
= \; & (1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k - x\,(1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k \\
= \; & (1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k - x\,(1-x)^n \left(\sum_{k=0}^{n} \binom{n+k}{k} \, x^k + \binom{2n+1}{n+1} \, x^{n+1} \right) \\
= \; & (1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k - x\,(1-x)^n \sum_{k=0}^{n} \binom{n+k}{k} \, x^k - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} \, x \qquad (*)
\end{aligned}$$

- Simplifions légèrement le $2^{\text{ème}}$ terme de la somme $(*)$ ci-dessus.

$$\begin{aligned}
x\,(1-x)^n \sum_{k=0}^{n} \binom{n+k}{k} \, x^k \; &= \; (1-x)^n \sum_{k=0}^{n} \binom{n+k}{k} \, x^{k+1} \\
&= \; (1-x)^n \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} \, x^k \qquad \textit{(par décalage d'indice)}
\end{aligned}$$

- Rassemblons maintenant les 2 premiers termes de $(*)$.

$$\begin{aligned}
& (1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k - (1-x)^n \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} \, x^k \\
= \; & (1-x)^n \left(\sum_{k=0}^{n+1} \binom{n+k}{k} \, x^k - \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} \, x^k \right) \\
= \; & (1-x)^n \left(\binom{n}{0} \, x^0 + \sum_{k=1}^{n+1} \binom{n+k}{k} \, x^k - \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} \, x^k \right) \\
= \; & (1-x)^n \left(1 + \sum_{k=1}^{n+1} \left(\binom{n+k}{k} - \binom{n+k-1}{k-1} \right) x^k \right) \\
= \; & (1-x)^n \left(1 + \sum_{k=1}^{n+1} \binom{n+k-1}{k} \, x^k \right) \qquad \textit{(par triangle de Pascal)} \\
= \; & (1-x)^n \sum_{k=0}^{n+1} \binom{n+k-1}{k} \, x^k
\end{aligned}$$

- On en déduit :

$$\begin{aligned}
& u_{n+1}(x) \\
= \ & (1-x)^n \sum_{k=0}^{n+1} \binom{n+k-1}{k} x^k - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} x \\
= \ & (1-x)^n \left(\sum_{k=0}^{n} \binom{n+k-1}{k} x^k + \binom{2n}{n+1} x^{n+1} \right) - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} x \\
= \ & (1-x)^n \sum_{k=0}^{n} \binom{n+k-1}{k} x^k + x^{n+1}\,(1-x)^{,} \binom{2n}{n+1} - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} x \\
= \ & u_n(x) + x^{n+1}\,(1-x)^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} x \right)
\end{aligned}$$

$$\boxed{\forall x \in [0,1],\ \forall n \in \mathbb{N}^*,\ u_{n+1}(x) = u_n(x) + x^{n+1}\,(1-x)^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} x \right)}$$

□

c) En déduire, pour tout $n \in \mathbb{N}^*$:

$$\mathbb{P}(G_{n+1}) \ = \ \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right)\ (pq)^{n+1} \binom{2n+1}{n+1}$$

Démonstration.
Soit $n \in \mathbb{N}^*$.

$$\begin{aligned}
& \mathbb{P}(G_{n+1}) \\
= \ & 1 - u_{n+1}(p) + \frac{p}{q}\ u_{n+1}(q) && \textit{(d'après } \textbf{15.a)}\textit{)} \\
= \ & 1 - \left(u_n(p) + p^{n+1}\, q^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} p \right) \right) + \frac{p}{q} \left(u_n(q) + q^{n+1}\, p^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} q \right) \right) \\
& && \textit{(d'après la question précédente)} \\
= \ & \left(1 - u_n(p) + \frac{p}{q}\ u_n(q) \right) - p^{n+1}\, q^n \left(\cancel{\binom{2n}{n+1}} - \binom{2n+1}{n+1} p \right) + p^{n+1}\, q^n \left(\cancel{\binom{2n}{n+1}} - \binom{2n+1}{n+1} q \right) \\
= \ & \mathbb{P}(G_n) - p^{n+1}\, q^n \binom{2n+1}{n+1} (q-p) && \textit{(d'après } \textbf{15.a)}\textit{)} \\
= \ & \mathbb{P}(G_n) - p^{n+1}\, q^{n+1}\ \frac{1}{q} \binom{2n+1}{n+1} (q-p) \\
= \ & \mathbb{P}(G_n) - (p\,q)^{n+1} \binom{2n+1}{n+1} \left(1 - \frac{p}{q}\right)
\end{aligned}$$

$$\boxed{\forall n \in \mathbb{N}^*,\ \mathbb{P}(G_{n+1}) \ = \ \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right)\ (pq)^{n+1} \binom{2n+1}{n+1}}$$

□

d) Montrer par récurrence, pour tout $n \in \mathbb{N}^*$:

$$\mathbb{P}(G_n) \ = \ \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n} \binom{2k-1}{k} (pq)^k$$

Démonstration.
Démontrons par récurrence : $\forall n \in \mathbb{N}^*, \mathcal{P}(n)$ où $\mathcal{P}(n) : \mathbb{P}(G_n) \ = \ \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n} \binom{2k-1}{k} (pq)^k$.

▸ **Initialisation** :

- D'une part, d'après ***14.c)*** :

$$\begin{aligned} \mathbb{P}(G_1) &= 1 - \sum_{k=0}^{1} \binom{\cancel{1} + k - \cancel{1}}{k} (p^k\, q - p^2\, q^{k-1}) \\ &= 1 - \left(\left(p^0\, q - \frac{p^2}{q}\right) + (p\, q - p^2\, q^0) \right) \\ &= (1-q) + \frac{p^2}{q} - p\, q + p^2 \\ &= p + \frac{p^2}{q} - p\, q + p^2 \end{aligned}$$

- D'autre part :

$$\begin{aligned} \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{1} \binom{2k-1}{k} (p\, q)^k &= \frac{p}{q} - \left(1 - \frac{p}{q}\right) \binom{1}{1} (p\, q)^1 \\ &= \frac{p}{q} - p\, q \left(1 - \frac{p}{q}\right) \\ &= \frac{p}{q} - p\, q + p^2 \end{aligned}$$

- Vérifions alors : $p + \frac{p^2}{q} - p\, q + p^2 = \frac{p}{q} - p\, q + p^2$.

$$\begin{aligned} p + \frac{p^2}{q} - \cancel{p\, q} + \cancel{p^2} - \left(\frac{p}{q} - \cancel{p\, q} + \cancel{p^2}\right) &= p + \frac{p^2}{q} - \frac{p}{q} \\ &= p \left(1 + \frac{p}{q} - \frac{1}{q}\right) \\ &= p\ \frac{q+p-1}{q} \\ &= p\ \frac{1-1}{q} \ = \ 0 \qquad (\textit{car } p+q=1) \end{aligned}$$

On a ainsi bien démontré :

$$\mathbb{P}(G_1) \ = \ \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{1} \binom{2k-1}{k} (p\, q)^k$$

D'où $\mathcal{P}(1)$.

▸ **Hérédité** : soit $n \in \mathbb{N}^*$.
Supposons $\mathcal{P}(n)$ et démontrons $\mathcal{P}(n+1)$ (*i.e.* $\mathbb{P}(G_{n+1}) = \dfrac{p}{q} - \left(1 - \dfrac{p}{q}\right) \sum\limits_{k=1}^{n+1} \dbinom{2k-1}{k} (pq)^k$).

$$\begin{aligned}
& \mathbb{P}(G_{n+1}) \\
= \ & \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right) (p\,q)^{n+1} \binom{2n+1}{n+1} && \textit{(d'après } \textbf{\textit{15.c)}}\textit{)} \\
= \ & \left(\frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n} \binom{2k-1}{k} (p\,q)^k\right) - \left(1 - \frac{p}{q}\right) (p\,q)^{n+1} \binom{2n+1}{n+1} && \textit{(par hypothèse de récurrence)} \\
= \ & \frac{p}{q} - \left(1 - \frac{p}{q}\right) \left(\sum_{k=1}^{n} \binom{2k-1}{k} (p\,q)^k + \binom{2n+1}{n+1} (p\,q)^{n+1}\right) \\
= \ & \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n+1} \binom{2k-1}{k} (pq)^k
\end{aligned}$$

D'où $\mathcal{P}(n+1)$.

$$\boxed{\text{Par principe de récurrence : } \forall n \in \mathbb{N}^*,\ \mathbb{P}(G_n) = \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n} \binom{2k-1}{k} (pq)^k.}$$ □

16. *Application à la sécurisation des transactions*
Connaissant $p < \dfrac{1}{2}$, on cherche à limiter le risque que la stratégie mise en place par le groupe de mineurs A réussisse.

a) Après avoir établi la formule $\dbinom{n}{k} = \dfrac{n}{k} \dbinom{n-1}{k-1}$ lorsque $k \in [\![1, n]\!]$, écrire une fonction **Scilab** qui calcule les coefficients binomiaux.

Démonstration.
Soit $k \in [\![1, n]\!]$.

- Tout d'abord :

$$k \binom{n}{k} = k \ \frac{n!}{k!\ (n-k)!} = \frac{n!}{(k-1)!\ (n-k)!}$$

- Par ailleurs :

$$n \binom{n-1}{k-1} = n \ \frac{(n-1)!}{(k-1)!\ ((n-\cancel{1}) - (k-\cancel{1}))!} = \frac{n!}{(k-1)!\ (n-k)!}$$

Ainsi : $k \dbinom{n}{k} = n \dbinom{n-1}{k-1}$.

$$\boxed{\text{D'où : } \forall k \in [\![1, n]\!],\ \binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}.}$$

Commentaire

La relation sur les coefficients binomiaux peut aussi se faire par dénombrement.
Pour ce faire, on considère un ensemble E à n éléments.
(on peut penser à une pièce qui contient n individus)
On souhaite alors construire une partie P à k éléments de cet ensemble contenant un élément distingué *(on peut penser à choisir dans la pièce un groupe de k individus dans lequel figure un représentant de ces individus)*.
Pour ce faire, on peut procéder de deux manières :

1) On choisit d'abord la partie à k éléments de E : $\binom{n}{k}$ possibilités.
On distingue ensuite un élément de cet ensemble P : $\binom{k}{1} = k$ possibilités.
(on choisit d'abord les k individus et on élit ensuite un représentant de ces individus)
Ainsi, il y a $k \binom{n}{k}$ manières de construire P.

2) On choisit d'abord, dans E, l'élément à distinguer : $\binom{n}{1} = n$ possibilités.
On choisit ensuite $k-1$ éléments dans E qui, pour former P, en y ajoutant l'élément précédent : $\binom{n-1}{k-1}$ possibilités.
(on choisit d'abord le représentant puis on lui adjoint un groupe de $k-1$ individus)
Ainsi, il y a $n \binom{n-1}{k-1}$ manières de construire P.

On retrouve ainsi le résultat.

- En itérant la formule précédente, on obtient :

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1} = \frac{n}{k} \frac{n-1}{k-1} \binom{n-2}{k-2} = \cdots = \frac{n\,(n-1)\cdots(n-k+1)}{k\,(k-1)\cdots 1}$$

(cette formule se démontre rigoureusement par récurrence)

- On propose alors la fonction **Scilab** suivante.

```
function c = CoeffBin(k, n)
    c = 1
    for i = 1:k
        c = c * (n - i + 1) / i
    end
endfunction
```

Détaillons les éléments de ce script.

- **Début de la fonction**
On commence par préciser la structure de la fonction :
  × cette fonction se nomme `CoeffBin`,
  × elle prend en paramètre les variables `k` et `n`,
  × elle admet pour variable de sortie la variable `c`.

```
function c = CoeffBin(k, n)
```

On initialise ensuite la variable `c` à 1 (choix naturel d'initialisation lorsqu'on souhaite coder un produit puisque 1 est l'élément neutre de l'opérateur produit).

```
    c = 1
```

- **Structure itérative**

Les lignes 3 à 5 consistent à mettre à jour la variable `c` pour qu'elle contienne la quantité $\binom{n}{k}$.
Or, d'après ce qui précède :

$$\binom{n}{k} = \frac{n\,(n-1)\,\cdots\,(n-k+1)}{k\,(k-1)\,\cdots\,1} = \frac{\prod\limits_{i=1}^{k}(n-i+1)}{\prod\limits_{i=1}^{k} i} = \prod_{i=1}^{k} \frac{n-i+1}{i}$$

Pour cela, on utilise alors une structure conditionnelle (boucle for) :

```
3     for i = 1:k
4         c = c ⋆ (n - i + 1) / i
5     end
```

- **Fin de la fonction**

À l'issue de cette boucle, la variable `c` contient la quantité $\prod\limits_{i=1}^{k} \frac{n-i+1}{i} = \binom{n}{k}$.

Commentaire

- Afin de permettre une bonne compréhension des mécanismes en jeu, on a détaillé la réponse à cette question. Cependant, proposer un programme **Scilab** correct démontre la bonne de ces mécanismes et permet certainement d'obtenir la majorité des points alloués à cette question. On procèdera de même dans les autres questions **Scilab**.
- Comme expliqué plus haut, on initialise `c` à 1 puisque cette variable doit contenir un produit, et que le réel 1 est l'élément neutre pour l'opérateur produit.
  On rappelle qu'on procède de même avec l'initialisation d'une somme stockée dans une variable `S` : on initialise la variable `S` à 0 car le réel 0 est l'élément neutre pour l'opérateur de sommation.
- On remarque que le programme proposé permet bien d'obtenir : $\binom{n}{0} = 1$.
  En effet, si $\mathtt{k} = 0$, alors :
  1) la variable `c` est initialisée à 1,
  2) la boucle qui suit n'est pas effectuée puisque la matrice `1:0` est une matrice vide,
  3) la fonction renvoie donc bien 1 lorsque `k` vaut 0.
- On pouvait exploiter plus directement la relation : $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.
  On obtient la fonction **Scilab** suivante :

```
function c = CoeffBin(k, n)
    if k==0 then
        c = 1
    else
        c = (n / k) ⋆ CoeffBin(n - 1, k - 1)
    end
endfunction
```

On remarque que la définition de la fonction `CoeffBin` fait appel à elle-même. On dit que la fonction `CoeffBin` est définie de manière *récursive*. Cette manière de coder est ici rendue naturelle par la formule démontrée juste avant.

Commentaire

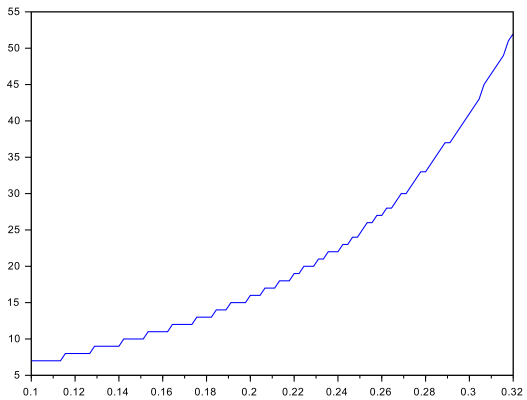
- Par exemple, lorsqu'on effectue l'appel `CoeffBin(2,3)` (pour obtenir la valeur de $\binom{3}{2}$), le calcul s'effectue de la façon suivante :

$$\begin{aligned}\texttt{CoeffBin}(2,3) &= \frac{3}{2} \times \texttt{CoeffBin}(2,1) \\ &= \frac{3}{2} \times \frac{2}{1} \times \texttt{CoeffBin}(1,0) \\ &= \frac{3}{2} \times \frac{2}{1} \times 1 \ = \ \frac{3 \times 2}{2 \times 1} \ = \ \binom{3}{2}\end{aligned}$$

Remarquons que le calcul est certain d'aboutir puisque l'appel `CoeffBin(k,n)` nécessite les appels de `CoeffBin(k-1, n-1)`, puis `CoeffBin(k-2, n-2)`, ..., puis `CoeffBin(1, n-(k-2))`, et enfin `CoeffBin(0, n-(k-1))` (dont on connaît la valeur). $\square$

b) Écrire un script **Scilab** qui détermine n_p, le plus petit entier n tel que $\mathbb{P}(G_n) \leqslant \varepsilon$ pour $p < \frac{1}{2}$ et $\varepsilon > 0$ saisis au clavier par l'utilisateur.

NB : Pour $\varepsilon = 10^{-4} = 0,1\%$ et p variant entre 10% et 32%, on obtient pour la représentation de n_p en fonction de p :



Démonstration.
On rappelle le résultat suivant, obtenu à la question ***15.c)*** pour le cas $p < \frac{1}{2}$:

$$\forall n \in \mathbb{N}^*, \quad \mathbb{P}(G_{n+1}) = \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right) (p\,q)^{n+1} \binom{2n+1}{n+1}$$

On propose alors le script Scilab suivant.

```
p = input(' Entrez la valeur de p : ')
eps = input(' Entrez la valeur de epsilon : ')
q = 1 - p
n = 1
ProbGn = p/q - (1 - p/q) ⋆ p ⋆ q
while ProbGn > eps
    ProbGn = ProbGn - (1 - p/q) ⋆ (p ⋆ q) ^ (n+1) ⋆ CoeffBin(n + 1, 2 ⋆ n + 1)
    n = n + 1
end
disp(n)
```

Détaillons les éléments de ce programme.

- **Début du programme**
  On commence par demander à l'utilisateur d'entrer une valeur pour le paramètre `p` et pour la précision `eps`.

```
1  p = input(' Entrez la valeur de p : ')
2  eps = input(' Entrez la valeur de epsilon : ')
```

  On définit la variable `q`.

```
3  q = 1 - p
```

  La variable `n` est initialisée à 1.
  La variable `ProbGn`, qui contiendra les valeurs successives de la suite $\big(\mathbb{P}(G_n)\big)_{n\in\mathbb{N}^*}$, est initialisée à $\mathbb{P}(G_1)$ (calculée en question ***15.d)***).

```
4  n = 1
5  ProbGn = p/q - (1 - p/q) ⋆ p ⋆ q
```

- **Structure itérative**
  Les lignes 6 à 9 consistent à déterminer le plus petit entier n tel que : $\mathbb{P}(G_n) \leqslant \varepsilon$. On doit donc calculer les valeurs successives de la suite $\big(\mathbb{P}(G_n)\big)$ jusqu'à ce que $\mathbb{P}(G_n) \leqslant \varepsilon$. Autrement dit, on doit calculer ces valeurs successives tant que $\mathbb{P}(G_n) > \varepsilon$. Pour cela, on met en place une structure itérative (boucle while).

```
6  while ProbGn > eps
```

  Tant que $\mathbb{P}(G_n) > \varepsilon$, on calcule $\mathbb{P}(G_{n+1})$ et on stocke toujours cette valeur dans `ProbGn` (on utilise ici la formule de la question ***15.c)***) :

```
7      ProbGn = ProbGn - (1 - p/q) ⋆ (p ⋆ q) ^ (n+1) ⋆ CoeffBin(n + 1, 2 ⋆ n + 1)
```

  On met alors à jour en conséquence la variable `n` : on ajoute 1 pour signaler qu'on a calculé $\mathbb{P}(G_{n+1})$.

```
8      n = n + 1
```

- **Fin du programme**
  À l'issue de cette boucle, la variable `n` contient le plus petit entier n tel que $\mathbb{P}(G_n) \leqslant \varepsilon$.
  On affiche alors enfin la valeur de la variable `n`.

```
10 disp(n)
```

$\square$