Problème de Mathématiques

Référence pp1609 — Version du 31 décembre 2025

Une information est transmise par l'intermédiaire d'un canal. Ce canal n'est pas complètement fiable : on observe qu'un bit envoyé peut être modifié, c'est-à-dire qu'un 1 (respectivement, un 0) en entrée peut devenir un 0 (respectivement, un 1) en sortie. On dit qu'un tel canal est **bruité**.

On modélise la transmission d'un bit de la manière suivante :

— Le bit envoyé est représenté par une variable aléatoire b suivant une loi de Bernoulli :

$$\mathbf{P}(b = 1) = \alpha, \qquad \mathbf{P}(b = 0) = 1 - \alpha.$$

— La perturbation du signal est aussi modélisée de façon probabiliste : le bit reçu est représenté par une variable aléatoire b' suivant aussi une loi de Bernoulli.

— On note p, la probabilité qu'un 1 en entrée ne soit pas altéré pendant la transmission :

$$p = \mathbf{P}(b' = 1 \mid b = 1). \tag{1}$$

— On note q, la probabilité qu'un 0 en entrée ne soit pas altéré pendant la transmission :

$$q = \mathbf{P}(b' = 0 \mid b = 0). \tag{2}$$

Toutes les variables aléatoires sont définies sur un même espace probabilisé $(\Omega, \mathcal{A}, \mathbf{P})$.

1. Exprimer $1 - p$ et $1 - q$ sous la forme de probabilités conditionnelles analogues à (1) et (2).

2. Un bit est envoyé. Quelle est la probabilité r de recevoir un 1 en sortie ?

3. On reçoit un 1 en sortie. Quelle est la probabilité qu'un 1 ait été envoyé en entrée ?

Soit $n \geqslant 2$, un entier. On envoie n fois le même bit b et on note $b'_1, \dots, b'_n$, les n bits reçus. On note alors X, le nombre de 1 reçus. On remarque que X est une variable aléatoire à valeurs dans $\mathbb{N}$ telle que

$$\mathbf{P}(0 \leqslant X \leqslant n) = 1.$$

4. Soit $0 \leqslant k \leqslant n$, un entier. Exprimer $\mathbf{P}(X = k)$ en fonction de r, n et k.

5. En déduire l'espérance de X en fonction de p, q et α.

6. Soit $0 \leqslant k \leqslant n$, un entier. Calculer la probabilité conditionnelle que le bit 1 ait été envoyé, sachant que le nombre de 1 reçus est égal à k.

On étudie désormais un **canal symétrique** : chaque bit, qu'il soit égal à 0 ou à 1, est altéré avec la même probabilité, c'est-à-dire $p = q$.

On suppose de plus que $1/2 < p < 1$.

7. a. Déterminer, en fonction des paramètres p et α, l'ensemble des valeurs de X pour lesquelles il est plus probable qu'un 1 ait été envoyé plutôt qu'un 0.

7. b. Que devient ce résultat pour $\alpha = 1/2$?

8. On suppose que $\alpha = 1/2$ et on note $f(n)$, la probabilité pour que l'interprétation du signal reçu soit fausse, c'est-à-dire que le bit envoyé ne soit pas le plus probable compte tenu du bit reçu.

8. a. Exprimer la probabilité $f(n)$ en fonction de n et p.

8. b. Écrire en langage Python une fonction `binome` de paramètres $N \in \mathbb{N}$ et $k \in \mathbb{N}$ tels que $0 \leqslant k \leqslant N$, qui retourne le coefficient binomial $\binom{N}{k}$.

8. c. On suppose que $p = 0,95$. Écrire en langage Python une fonction `f` de paramètre $n \in \mathbb{N}$ qui retourne une estimation de $f(n)$.

Solution ❀ Transmission d'une information par un canal imparfait

1. Les événements $[b'=1] \in \mathcal{A}$ et $[b'=0] \in \mathcal{A}$ sont complémentaires l'un de l'autre dans Ω :

$$\Omega = [b'=1] \sqcup [b'=0].$$

Comme $\mathbf{P}_{b=1}$ est une mesure de probabilité sur $(\Omega, \mathcal{A})$, on déduit de (1) que

$$1-p = \mathbf{P}_{[b=1]}([b'=1]^c) = \mathbf{P}(b'=0 \mid b=1)$$

et de même, on déduit de (2) que

$$1-q = \mathbf{P}_{[b=0]}([b'=0]^c) = \mathbf{P}(b'=1 \mid b=0).$$

2. Comme les événements $[b=0]$ et $[b=1]$ constituent un système complet, on déduit de la formule des probabilités totales que la probabilité de recevoir un 1 en sortie est égale à :

$$\mathbf{P}(b'=1) = \mathbf{P}(b'=1 \mid b=0)\,\mathbf{P}(b=0) + \mathbf{P}(b'=1 \mid b=1)\,\mathbf{P}(b=1) = (1-q)(1-\alpha) + p\alpha.$$

3. Les événements $[b=1]$ et $[b'=1]$ n'étant pas négligeables, la formule de Bayes montre que la probabilité (conditionnelle) qu'un 1 ait été envoyé sachant qu'on a reçu un 1 est égale à

$$\mathbf{P}(b=1 \mid b'=1) = \frac{\mathbf{P}(b'=1 \mid b=1)\,\mathbf{P}(b=1)}{\mathbf{P}(b'=1)} = \frac{p\alpha}{(1-q)(1-\alpha)+p\alpha}.$$

4. La fonction X est bien une variable aléatoire sur $(\Omega, \mathcal{A})$ en tant que somme de variables aléatoires :

$$\forall\, \omega \in \Omega, \quad X(\omega) = b'_1(\omega) + \cdots + b'_n(\omega).$$

Mais la modélisation proposée par l'énoncé est *incomplète* : la loi jointe des variables aléatoires

$$b, \quad b'_1, \dots, b'_n$$

n'est pas connue ! *Nous supposerons* donc dans la suite que, conditionnellement aux événements $[b=1]$ et $[b=0]$, les variables aléatoires b'_1, ..., b'_n sont indépendantes et de même loi que b'.

La loi de X sous $\mathbf{P}_{[b=1]}$ est donc la loi d'une somme de n variables aléatoires indépendantes suivant chacune la loi de Bernoulli de paramètre p, c'est-à-dire la loi binomiale $\mathcal{B}(n, p)$.

La loi de X sous $\mathbf{P}_{[b=0]}$ est de même la loi d'une somme de n variables aléatoires indépendantes suivant chacune la loi de Bernoulli de paramètre $1-q$, c'est-à-dire la loi binomiale $\mathcal{B}(n, 1-q)$.

Comme précédemment, on déduit de la formule des probabilités totales appliquée au système complet d'événements $\big([b=1], [b=0]\big)$ que

$$\begin{aligned}\mathbf{P}(X=k) &= \mathbf{P}(X=k \mid b=1)\,\mathbf{P}(b=1) + \mathbf{P}(X=k \mid b=0)\,\mathbf{P}(b=0)\\ &= \alpha\binom{n}{k}p^k(1-p)^{n-k} + (1-\alpha)\binom{n}{k}(1-q)^k q^{n-k}\end{aligned}$$

pour tout entier $0 \leqslant k \leqslant n$.

5. Comme l'espérance de la loi binomiale $\mathcal{B}(n, r)$ est égale à nr, on déduit de ce qui précède que

$$\mathbf{E}(X) = \alpha np + (1-\alpha)n(1-q) = n\,\mathbf{E}(b').$$

6. D'après la formule de Bayes,

$$\mathbf{P}(b=1 \mid X=k) = \frac{\mathbf{P}(X=k \mid b=1)\,\mathbf{P}(b=1)}{\mathbf{P}(X=k)}$$

où le numérateur et le dénominateur ont été calculés à la question précédente.

$$\mathbf{P}(b=1 \mid X=k) = \frac{1}{1+\dfrac{1-\alpha}{\alpha}\Big(\dfrac{1-q}{p}\Big)^k\Big(\dfrac{q}{1-p}\Big)^{n-k}}$$

7. a. Avec $p=q$, l'expression précédente devient

$$\mathbf{P}(b=1 \mid X=k) = \frac{1}{1+\frac{1-\alpha}{\alpha}(1-p)^{2k-n}p^{n-2k}}$$

et comme b est une variable aléatoire qui suit une loi de Bernoulli,

$$\mathbf{P}(b=0 \mid X=k) = 1 - \mathbf{P}(b=1 \mid X=k).$$

On cherche donc les valeurs de l'entier $0 \leqslant k \leqslant n$ pour lesquelles

$$\frac{1}{1+\frac{1-\alpha}{\alpha}(1-p)^{2k-n}p^{n-2k}} > \frac{1}{2},$$

c'est-à-dire

$$\frac{1-\alpha}{\alpha}\Big(\frac{1-p}{p}\Big)^{2k-n} < 1.$$

Comme $1/2 < p < 1$, alors $0 < (1-p)/p < 1$, donc $\ell n[(1-p)/p] < 0$. On déduit donc de l'inégalité précédente qu'il est plus probable qu'un 1 ait été envoyé plutôt qu'un 0 si, et seulement si, X prend une valeur supérieure à

$$\frac{n}{2} + \frac{1}{2} \cdot \frac{\ell n\,\alpha - \ell n(1-\alpha)}{\ell n(1-p) - \ell n\,p}.$$

7. b. Pour $\alpha = 1/2$, il est plus probable qu'un 1 ait été envoyé plutôt qu'un 0 si, et seulement si, X prend une valeur supérieure à $n/2$.

8. a. Ce qui précède conduit à interpréter le signal reçu selon les règles suivantes :
— Si X prend une valeur supérieure à $n/2$, alors on décide que le bit envoyé était égal à 1 ;
— Si X prend une valeur inférieure à $n/2$, alors on décide que le bit envoyé était égal à 0 ;
— Comme l'entier n peut être à peu près librement choisi (tout de même pas trop grand pour ne pas surcharger le canal de transmission !), on peut imposer une valeur impaire à n pour ne pas avoir à décider d'une conduite particulière à tenir dans le cas très particulier où X prendrait la valeur $n/2$.

L'événement qui traduit que l'interprétation est fausse est donc

$$([X < n/2] \cap [b=1]) \sqcup ([X > n/2] \cap [b=0])$$

et sa probabilité est égale à

$$\sum_{0 \leqslant k < n/2} \mathbf{P}(X=k \mid b=1)\,\mathbf{P}(b=1) + \sum_{n/2 < k \leqslant n} \mathbf{P}(X=k \mid b=0)\,\mathbf{P}(b=0)$$

puisque la famille $([X=k])_{0 \leqslant k \leqslant n}$ est un système complet d'événements.

D'après **[4.]**, conditionnellement à $[b=1]$, la loi de X est la loi binomiale $\mathcal{B}(n,p)$ et conditionnellement à $[b=0]$, la loi de X est la loi binomiale $\mathcal{B}(n,[1-p])$ (puisque $q=p$ ici). De plus, ici,

$$\mathbf{P}(b=0) = \mathbf{P}(b=1) = \frac{1}{2}$$

puisque $\alpha = 1/2$. On peut alors déduire de la symétrie des coefficients binomiaux que la probabilité cherchée est égale à

$$\sum_{0 \leqslant k < n/2} \binom{n}{k} p^k (1-p)^{n-k}.$$

> *Cette probabilité est égale à* $\mathbf{P}(Y < n/2)$ *où* Y *est une variable aléatoire suivant la loi binomiale* $\mathcal{B}(n,p)$. *On en déduit sans autre calcul que cette probabilité est d'autant plus proche de* 0 *que* p *est proche de* 1 *et* n *grand.*

8. b. Le plus simple est de procéder par itération en partant du fait que $\binom{n}{0} = 1$ et de la relation

$$\forall\, 0 \leqslant k < n, \quad \binom{n}{k+1} = \frac{n-k}{k+1} \cdot \binom{n}{k}$$

qui nous assure que les calculs s'effectuent tous avec des *entiers* (si on effectue la multiplication par $(n-k)$ *avant* la division par $(k+1)$), aussi petits que possible. Il est aussi utile d'exploiter la symétrie des coefficients binomiaux

$$\forall\, 0 \leqslant k \leqslant n, \quad \binom{n}{k} = \binom{n}{n-k}$$

pour réduire autant que possible le nombre d'opérations à effectuer.

```
def binome(N, k):
    if (k>N-k):
        return binome(N, N-k)
    else:
        b = 1
        for i in range(k):
            b = b*(N-i)//(i+1)
        return b
```

L'utilisation des factorielles

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

est déconseillée : cela conduit à manipuler des facteurs extrêmement grands au numérateur comme au dénominateur et donc à calculer en flottants. *On n'obtient alors qu'une valeur approchée (*très *précise cependant) des coefficients binomiaux.*

Le calcul récursif (à partir de la formule du triangle de Pascal) est inefficace au possible : on effectue $\binom{n}{k}$ appels à la fonction pour calculer $\binom{n}{k}$...

8. c. Le calcul de $f(n)$ ne pose aucune difficulté.

```
def f(n):
    p = 0.95
    N = (n+1)//2
    s = sum(binome(n, k)*p**k*(1-p)**(n-k)
            for k in range(N))
    return s
```

La version suivante est plus économique et effectue aussi peu de multiplications que possible.

```
def f(n):
    p = 0.95
    q = 1-p
    s, b, pk, qnk = 0.0, 1, 1, q**n
    N = (n+1)//2
    for k in range(N):
        s += b*pk*qnk
        pk, qnk = pk*p, qnk/q
        b = b*(n-k)//(k+1)
    return s
```

En pratique, $f(5)$ est de l'ordre de $0,1\%$ et $f(7)$ de l'ordre de $0,02\%$. Il y a donc très peu de chances que la règle de décision choisie au **[8.a.]** conduise à un résultat faux dès $n = 5$. La version optimisée de f est donc d'un intérêt très limité !