TD1 - Mesure de l'information

Exercice 1 (Jeu de cartes)
Un jeu de 32 cartes comporte :

- *8 cartes de coeur* $\heartsuit$,
- *8 cartes de carreau* $\diamondsuit$,
- *8 cartes de pique* ♠,
- *et 8 cartes de trêfle* ♣.

Ces 8 cartes sont, par valeur décroissante, l'as, le roi, la dame, le valet, le 10, le 9, le 8 et le 7. On considère une "main" de 4 cartes tirées au hasard d'un jeu de 32 cartes, ainsi que les évènements suivants :

— E_1 *: la main ne contient aucune carte inférieure au valet,*

— E_2 *: le main ne contient pas de figure (roi, dame, valet),*

— E_3 *: la main contient 4 cartes du même nom.*

— E_4 *: la main contient les 4 as.*

1. *Calculer la quantité d'information propre* $I(E_i)$ *associée à chaque évènement* E_i, $i \in \{1, 2, 3, 4\}$.
2. *Calculer les informations mutuelles* $I(E_1, E_2)$ *et* $I(E_1, E_3)$.
3. *Évaluer approximativement la quantité d'information nécessaire pour spécifier une main de 4 cartes. Comparer cette quantité à l'entropie de la variable aléatoire correspondant au contenu d'une main.*

Exercice 2 (Un problème de météo)
Dans la vallée de la mort :

— *il pleut en moyenne 1 jour sur 100.*

— *la météo prédit 3 jours de pluie sur 100.*

— *chaque fois qu'il pleut, la météo l'a prévu.*

Monsieur Sûr-de-lui prévoit qu'il ne pleut jamais. Est-il justifié de payer cher des investissements météo, alors que Monsieur Sûr-de-lui, qui ne coûte rien et se trompe moins souvent que la météo ?

Exercice 3
Soit un vecteur $(X_1, X_2 \ldots, X_n)$ *de* n *variables aléatoires. Par définition on sait que son entropie est :*

$$H(X_1, X_2 \ldots, X_n) = -\sum p(x_1, \ldots, x_n) \log(p(x_1, \ldots, x_n))$$

1. *(Cas d'indépendance) Montrer que si les variables* $X_1, X_2 \ldots, X_n$ *sont indépendantes, alors :*
$$H(X_1, X_2 \ldots, X_n) = \sum_{i=1}^{n} H(X_i).$$
2. *(Cas général : « règle de chaînage pour l'entropie ») Montrer que :*
$$H(X_1, X_2 \ldots, X_n) = H(X_n|X_1, \ldots, X_{n-1}) + H(X_{n-1}|X_1, \ldots, X_{n-2}) + \cdots + H(X_2|X_1) + H(X_1).$$

Exercice 4

Soit X une variable aléatoire et g une fonction.

1. *En utilisant le règle de chaînage de deux manières différentes, montrer que*

$$H(g(X)) \leq H(X).$$

2. *Dans quelle condition a-t-on l'égalité ?*

Exercice 5 (Pesées)

1. *On considère un ensemble de n pièces d'or. Parmis ces pièces une seule est fausse et a un poids inférieur au poids standard. De plus on dispose d'une balance à deux plateaux permettant de comparer les poids a et b de deux ensembles A et B de pièces posés respectivement sur chacun des plateaux.*
   (a) *Quelle est la quantité d'information nécessaire pour déterminer la fausse pièce ?*
   (b) *On suppose dans cette question que $n = 3k$. Calculer la quantité d'information qu'apporte une pesée quand $|A| = |B| = k$.*
   (c) *En déduire une borne inférieure du nombre moyen m de pesées nécessaires pour déterminer la fausse pièce. Que peut-on dire si n est de la forme 3^i ?*

Exercice 6

Soient X et Y deux variables aléatoires à valeurs dans un groupe $(G, +)$. Soit la variable aléatoire $Z = X + Y$.

1. *Montrer que $H(Z|X) = H(Y|X)$.*
2. *Montrer que si X et Y sont indépendantes alors $H(Y) \leq H(Z)$ et $H(X) \leq H(Z)$ (utiliser la positivité de l'information mutuelle).*
3. *Donner un exemple de deux variables aléatoires X et Y telles que $H(X) > H(Z)$ et $H(Y) > H(Z)$.*

Exercice 7 (Le problème du mot de passe)

Un individu (probablement mal intentionné) cherche à accéder à un service protégé par un mot de passe qu'il ne connaît pas. Soit $\mathcal{M} = \{0, 1\}^m$ l'ensemble des mots de passe possibles. Nous supposons que le système d'authentification est parfait et que la seule possibilité d'action pour l'attaquant consiste à essayer les mots de passe un par un.

On suppose ensuite que le mot de passe est choisi dans $\mathcal{M}$ selon une loi d'entropie $h \leq m$. Nous notons p_i les probabilités des mots de $\mathcal{M}$dans l'ordre décroissant (le mot le plus probable a pour probabilité p_1, le suivant p_2 ...).

1. *Montrer que la meilleure stratégie consiste à tester les mots dans l'ordre des probabilités décroissantes. Exprimez le nombre moyen d'essais, $\mathcal{N}(p)$, en fonction des p_i.*
2. *Soient deux lois de probabilité $p = (p_i)_{i\geq 1}$ et $q = (q_i)_{i\geq 1}$ telles que les suites p_i et q_i soient décroissantes avec $q_i > 0$ pour tout $i \geq 1$ (en revanche p_i peut être nul à partir d'un certain rang).*
   Nous posons $q - i = (1 - \alpha)\alpha^{i-1}$ pour un certain réel $0 < \alpha < 1$. On suppose que les entropie $H(p)$ et $H(q)$ sont bien définies. Montrer que si $H(p) = H(q)$ alors

$$\sum_{i\geq 1} ip_i \geq \sum_{i\geq 1} iq_i.$$

(Indication : on pourra tirer profit de la positivité de la distance de Kullback $D(p||q) \geq 0$)

3. *Calculer l'entropie* $H(q)$ *de la loi* q *en fonction de* α. *Nous noterons* H_α *cette quantité. On rappelle les identités* $\sum_{i\geq 1}\alpha^{i-1} = \frac{1}{1-\alpha}$ *et* $\sum_{i\geq 1}\alpha^{i-1} = \frac{1}{(1-\alpha)^2}$.
4. *En déduire que pour tout réel* $0 < \alpha < 1$ *nous avons* $1 < (1-\alpha)2^{H_\alpha} < e$, *où* e *est la base du logarithme népérien.*
5. *Déduire du résultat précédent que* $\mathcal{N} < c_1 2^h$ *(on s'efforcera de donner une valeur à* c_1*).*