1.3 Exercices TD 1

Exercice 1.1.

1) Établir que

$$\forall\, v, w \in \{0,1\}^m,\ d_H(v,w) = H(v+w) \leq H(v) + H(w).$$

2) En déduire que

$$\forall\, u, v, w \in \{0,1\}^m,\ d_H(u,v) = d_H(u+w, v+w) \text{ et } d_H(u,v) = d_H(w, u+v+w).$$

3) Vérifier que d_H est bien une distance sur $\{0,1\}^m$.

4) Représenter dans l'espace à 3 dimensions l'ensemble $L = \{0,1\}^3$. À quoi correspondent les arêtes du volume obtenu ? Où se situent les mots distants de 2 au sens de la distance de Hamming ? Combien il y a t-il de couples de tels mots ?

Exercice 1.2.

Cet exercice propose entre autre une démonstration du théorème 1.1. On considère donc un code $\mathcal{C}$ avec correction suivant la méthode du maximum de vraisemblance et on note $k = \lfloor(\delta(\mathcal{C}) - 1)/2\rfloor$.

On note $w \in \mathcal{C}(\{0,1\}^m)$ le mot émis et $\tilde{w}$ le mot reçu, tels que $d_H(w, \tilde{w}) \leq k$. Soient $\widehat{w_1}, \widehat{w_2} \in \mathcal{C}(\{0,1\}^m)$ vérifiant la propriété

$$\forall\, v \in \mathcal{C}(\{0,1\}^m),\ d_H(\widehat{w_1}, \tilde{w}) = d_H(\widehat{w_2}, \tilde{w}) \leq d_H(v, \tilde{w}). \tag{1.11}$$

1) Montrer que $d_H(\widehat{w_1}, \widehat{w_2}) \leq 2k$.

2) En déduire que $\widehat{w_1} = \widehat{w_2}$.

3) En déduire que la méthode du maximum de vraisemblance donnée par l'équation (1.6) du cours est bien définie. Cela suffit-il à démontrer le théorème 1.1 ?

4) Démontrer le théorème 1.1.

5) Que peut-on dire quand

$$\left\lfloor \frac{\delta(\mathcal{C}) - 1}{2} \right\rfloor \ < \ k \ \leq \ \delta(\mathcal{C}) - 1 \ ?$$

Donner deux exemples de mots codés illustrant deux situations problématiques différentes.

Exercice 1.3.

On considère l'application $\mathcal{C}$ de $\{0,1\} \mapsto \{0,1\}^2$ définie par $\mathcal{C}(0) = 00$, $\mathcal{C}(1) = 11$.

1) Pourquoi cette application est-elle un code ? Quel est l'ensemble des mots du code ?

2) Déterminer sa redondance, son rendement et sa distance minimale.

3) Que peut-on dire sur la capacité de ce code à détecter les erreurs de transmission ?

4) Que peut-on dire sur la capacité de ce code à corriger les erreurs de transmission ?

5) On modélise le bruit du canal de transmission de la manière suivante, appelée *schéma de Bernoulli* : la probabilité p que le bit d'un mot de code soit mal transmis est identique pour tout bit et tout mot et les erreurs sur les bits sont indépendantes les unes des autres. En outre, on suppose que les mots source sont équiprobables. L'expérience aléatoire consiste à appliquer le code à un mot source, à transmettre le mot de code dans le canal bruité et à observer le mot reçu.

Déterminer l'ensemble des résultats possibles de l'expérience, appelé *univers*

$$\Omega = \{e_1, e_2, \ldots, e_N\},$$

les éléments $(e_i)_{i\in[\![1,N]\!]}$ étant les évènements élémentaires. Calculer les probabilités $(P(e_i))_{i\in[\![1,N]\!]}$ de ces évènements élémentaires.

6) On note D l'évènement "un mot reçu est détecté erroné" et E l'évènement "un mot reçu est erroné". Déterminer ces évènements ainsi que l'évènement $D \cap E$ comme parties de Ω et en déduire leur probabilité.

7) Exprimer en fonction de p la probabilité qu'un mot reçu erroné soit effectivement détecté comme étant erroné. Tracer le graphe de la fonction obtenue.

Exercice 1.4.

Soit $t \in \mathbb{N}$, $t \geq 2$. Un *code de répétition* $\mathcal{C} = \mathcal{C}_{tm,m}$ consiste à répéter t fois le mot à transmettre. Ainsi, si $u \in \{0,1\}^m$ est le mot source, le mot transmis est $w = u^t$. On a donc $n = tm$.

1) Quel est le rendement d'un code de répétition ?

2) Montrer que la distance minimale $\delta(\mathcal{C})$ vérifie $\delta(\mathcal{C}) \geq t$.

3) Déterminer la valeur $\delta(\mathcal{C})$.

4) Donner t pour que le code de répétition soit un 2-détecteur.

5) Comment le décodeur d'un tel code peut-il détecter au plus 2 erreurs ?

6) Donner t pour que le code de répétition soit un 2-correcteur.

7) Comment le décodeur d'un tel code peut-il corriger au plus 2 erreurs ?

8) Le canal de transmission est modélisé suivant le *schéma de Bernoulli* : la probabilité p que le bit d'un mot de code soit mal transmis est identique pour tout bit et tout mot et les erreurs sur les bits sont indépendantes les unes des autres. On suppose maintenant que le mot source est réduit à un bit : $m = 1$. En utilisant la variable aléatoire X du nombre de bits erronés dans un mot reçu, déterminer en fonction de t et de p la probabilité p_{de} qu'un mot reçu erroné soit effectivement détecté erroné.

9) Application numérique : calculer la probabilité p_{de} dans le cas où $t = 3$ et $p = 0.1$.

10) Pour ces mêmes valeurs numériques, quelle est la probabilité p_{me} qu'un mot reçu erroné soit mal décodé ?

Exercice 1.5.

1) Quelle est la capacité de correction maximale que l'on puisse obtenir avec un code $\mathcal{C}_{5,2}$?

2) Construire un code possédant une telle capacité de correction.

3) Quelle est la plus petite longueur n possible pour qu'un code $\mathcal{C}_{n,4}$ possède une capacité de correction d'une erreur ? Que peut-on alors dire d'un tel code ?

4) On cherche maintenant à encoder 4 mots binaires avec une capacité de correction de 2 erreurs. Quelle est la distance minimale d'un tel code ?

5) Quelle est la longueur minimale d'un tel code ?