Théorie de l'information et du codage

TD n^{o}8 – Codes linéaires

Exercice 1 – Codes de Hamming q-aires

L'objet de cet exercice est de généraliser à n'importe quel corps fini $\mathbb{F}_q$ les codes de Hamming binaires ($q = 2$). Soit C un code linéaire de matrice de parité $H \in \mathcal{M}_{m,n}(\mathbb{F}_q)$.

1. Si m est fixé, comment à t-on interêt à choisir n pour que le code soit le plus efficace possible ? Montrer que si C corrige les erreurs uniques, alors nécessairement,

$$n \leq \frac{q^m - 1}{q - 1}.$$

   Lorsque l'égalité est atteinte, C est appelé code de Hamming $q-$aire de paramètre $\left(n = \frac{q^m-1}{q-1}, k = n - m\right)$.

2. Montrer que ces codes sont parfaits. Y a t-il d'autres codes $1-$correcteurs parfaits ?
3. Construire un code de Hamming $(4, 2)$ ternaire, un code de Hamming $(13, 10)$ ternaire, et un code de Hamming $(6, 4)$ $5-$aire. (On donnera les matrices de vérification.)

Exercice 2 – Codes de Hamming augmentés et diminués

Les codes de Hamming sont parfaitement adaptés aux situations ou l'on peut garantir qu'au plus une erreur se produit à chaque transmission. Malheureusement, leurs performances deviennent désastreuses aussitôt que cette condition se trouve violée. Cet exercice met en évidence ce problème, et propose quelques moyens simples d'y remédier.

1. Est-il vrai que, lorsque l'on utilise un code de Hamming et que deux erreurs ou plus se produisent au cours de la transmission, le décodage est toujours incorrect ?
2. À partir d'un code linéaire donné, on peut définir les deux variantes suivantes :
   (a) le code *augmenté* s'obtient en ajoutant au code original un bit de parité globale ;
   (b) le code *diminué* est le sous-code obtenu à partir de l'original en ne conservant que les mots-code dont le poids de Hamming est pair.

   Calculer la dimension et la distance de ces codes en fonction de celles du code original.
3. Montrer que les codes de Hamming augmentés et diminués corrigent toujours les erreurs uniques mais détectent désormais également les erreurs doubles.

Exercice 3 – Débit maximal des codes $t-$correcteurs

1. Montrer que tout code $\mathcal{C}$ binaire $t-$correcteur de longueur n ($2t < n$) vérifie nécessairement :

$$|\mathcal{C}| \sum_{i=0}^{t} \binom{n}{i} \leq 2^n,$$

   et en déduire une borne supérieure sur le débit du code (en bits utiles par symbole émis).

2. On fait maintenant tendre la taille n des mots-code vers l'infini et l'on souhaite pouvoir corriger jusqu'à $t = \lceil \varepsilon n \rceil$ erreurs par mot-code ($0 \leq \varepsilon < \frac{1}{2}$). Que donne alors la borne précédemment obtenue ? On exprimera la réponse à l'aide de la fonction

$$H \colon x \mapsto -x \log_2(x) - (1-x) \log_2(1-x).$$

3. Comment pouvait-on prévoir directement cette limitation théorique sur le débit ? La borne obtenue est-elle atteignable asymptotiquement ?

Exercice 4 – Identité de MacWilliams

Soit $A(X) = \sum_{i=0}^{n} a_i X^i$ le polynôme énumérateur d'un (n,k)-code linéaire binaire $C \subseteq$, et soit $B(X) = \sum_{i=0}^{n} b_i X^i$ le polynôme énumérateur du code orthogonal $C^\perp$. Alors A et B sont liés par l'identité remarquable suivante, due à MacWilliams :

$$B(X) = \frac{1}{2^k} \sum_{i=0}^{n} a_i (1-X)^i (1+X)^{n-i}.$$

1. Démontrer cette identité en calculant de deux manières différentes la quantité :

$$\sum_{x \in C} \sum_{y \in \mathbb{F}_2^n} X^{w(y)} (-1)^{\langle x,y \rangle}.$$

2. Application : calculer le polynôme énumerateur d'un code de Hamming binaire.
3. Généraliser l'identité de MacWilliams à $\mathbb{F}_q$ quelconque.
4. Application : calculer le polynôme énumérateur d'un code de Hamming $q-$aire.

Exercice 5 – Codes de Reed-Muller

Historiquement, le code $RM(5,1)$ a été utilisé par les sondes *Mariner* lancées par la NASA entre 1969 et 1973 pour assurer une transmission correcte des photos numérisées de Mars. Soit $0 \leq d \leq m$ des entiers. Notons $\mathcal{P}_{m,d}$ l'ensemble des polynômes de degré au plus d à m variables sur le corps $\mathbb{F}_2$. On note $v_0, \ldots, v_{M-1}$ les $M = 2^m$ éléments de $\mathbb{F}_2^m$ dans l'ordre lexicographique. À chaque $f \in \mathcal{P}_{m,d}$, on peut alors associer le vecteur $(f(v_0), \ldots, f(v_{M-1})) \in \mathbb{F}_2^M$. L'ensemble des vecteurs de $\mathbb{F}_2^M$ ainsi obtenus est noté $RM(m,d)$: c'est le code de Reed-Muller binaire de longueur 2^m et d'ordre d.

1. Est-ce un code linéaire ?
2. Quelle est sa dimension ?
3. Que sont en fait $RM(m,0)$, $RM(m,m)$, $RM(m,m-1)$?
4. Quelle est sa distance ?
5. Quel est son code diminué ?
6. Quel est son orthogonal ?
7. Donner une formule récursive pour sa matrice génératrice. Expliciter cette matrice pour $m = 3$ et $0 \leq d \leq m$.
8. Quel est son polynôme énumérateur lorsque $d = 0, 1, m-1$ et m ?