Théorie de l'information et du codage

TD n^{o}9

Quelques exos sur les corps finis

1. Soit F une extension finie de $F(p)$ qui contient tous les zéros de $X^{p^m} - X$. Montrer (i) que $X^{p^m} - X$ a tous ses zéros distincts dans F ; (ii) directement que ces zéros forment un corps.
2. Soit G un groupe commutatif contenant des éléments g et h d'ordres r et s respectivement. (i) Montrer que si $g^n = 1$ alors $r|n$. (ii) Montrer que si $r \vee s = 1$ alors gh a pour ordre rs. (iii) Montrer que si $r = r_1 r_2$ alors g^{r_1} a pour ordre r_2.
3. (i) Montrer que dans tout corps :

$$X^s - 1 | X^r - 1 \Leftrightarrow s|r.$$

(ii) Montrer que $p.g.c.d.\{X^r - 1, X^s - 1\} = X^d - 1$ avec $d = p.g.c.d.\{r, s\}$.

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.

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. Quel est son orthogonal ?
5. Donner une formule récursive pour sa matrice génératrice. Expliciter cette matrice pour $m=3$ et $0 \leq d \leq m$.
6. Quelle est sa distance ?
7. Quel est son code diminué ?
8. Quel est son polynôme énumérateur lorsque $d = 0, 1, m-1$ et m ?