Université de Bordeaux — **Arithmétique – M1MA7W01**
Master 1 CSI — 2013–2014

FEUILLE D'EXERCICES n° 7

Exercice 1 – [Borne de Singleton]
Soit $C \subset (\mathbb{F}_q)^n$ un code linéaire de paramètres (n, k, d).

1) Montrer que les mots (de longueur $n-(d-1)$) obtenus en supprimant les $d-1$ premières coordonées des mots de C sont distincts.

2) En déduire que $n \geqslant k + d - 1$.

3) Plus généralement, si on ne suppose plus C linéaire, mais simplement $C \subset (\mathbb{F}_q)^n$ de distance minimale d, montrer que $\#C \leqslant q^{n-d+1}$.

Exercice 2 – [Borne de Hamming]
Soit $C \subset (\mathbb{F}_q)^n$ un code de distance minimale d. On sait que C est t-correcteur, où $t = \lfloor (d-1)/2 \rfloor$.

1) Montrer qu'une boule de Hamming de rayon t possède $m := \sum_{k=0}^{t} \binom{n}{k} (q-1)^k$ éléments.

2) Montrer que $\#C \leqslant q^n/m$.

Exercice 3 – On définit sur $(\mathbb{F}_q)^n$ le produit

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := \sum_{i=1}^{n} x_i y_i.$$

On définit le code dual $C^\perp$ d'un code linéaire $C \subset (\mathbb{F}_q)^n$ par

$$C^\perp := \{x \in (\mathbb{F}_q)^n \colon x \cdot y = 0 \text{ pour tout } y \in C\}$$

1) Montrer que $C^\perp$ est un code linéaire.

2) Montrer que si C est cyclique, alors $C^\perp$ l'est aussi.

3) Montrer que si C est de dimension k, alors $C^\perp$ est de dimension $n - k$.

4) Montrer que $\left(C^\perp\right)^\perp = C$.

Exercice 4 – Soient C_1 et C_2 deux codes linéaires sur $\mathbb{F}_q$, de paramétres respectifs (n_i, k_i, d_i), pour $i = 1, 2$. On définit

$$C_1 \oplus C_2 = \{(x, y) \in (\mathbb{F}_q)^{n_1} \times (\mathbb{F}_q)^{n_2} \colon x \in C_1, y \in C_2\},$$

ainsi que si $n_1 = n_2 = n$,

$$C_1 * C_2 = \{(x, x + y) \in (\mathbb{F}_q)^{n} \times (\mathbb{F}_q)^{n} \colon x \in C_1, y \in C_2\},$$

1) Montrer que $C_1 \oplus C_2$ est un code linéaire, de paramètres

$$\big(n_1 + n_2, k_1 + k_2, \min(d_1, d_2)\big).$$

2) Montrer que $C_1 * C_2$ est linéaire, de paramètres $\big(2n, k_1 + k_2, \min(2d_1, d_2)\big)$.

Exercice 5 – [Code de Hamming]
Soit $g(X) \in \mathbb{F}_2[X]$ un polynôme primitif (irréductible) de degré m. Il définit un code cyclique $\langle g \rangle$ de longeur $n = 2^m - 1$ dans $\mathbb{F}_2[X]/(X^n - 1)$, vu comme $\mathbb{F}_2$-espace vectoriel de dimension n. On note α la classe de X dans $\mathbb{F}_2[X]/(g)$.

1) Montrer que le code C est constitué des polynômes modulo $X^n - 1$ qui s'annulent en α.

2) Montrer que la dimension de C est $n - m$.

3) On suppose que $m > 1$. Montrer que la distance minimale de C est 3.

4) Écrire la matrice génératrice d'un tel code pour $m = 3$. Écrire une matrice génératrice de son code dual.