Exercices du cours de Théorie de l'Information et Codage

cours 11 du 17 mai 2011.

1. Pour tout entier positif m, on définit $\varphi(m)$ comme le nombre d'entiers positifs $\leq m$ qui sont premiers avec m. (i) Montrer que

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

où les p sont premiers. (ii) Montrer que si $a \wedge m = 1$ alors

$$a^{\varphi(m)} \equiv 1 (\text{mod } m).$$

2. Comme dans le cours, m est l'ordre multiplicatif de q modulo n. (i) Montrer que les racines de $X^n - 1$ forment un sous-groupe cyclique de $F(q^m)^*$. Montrer que les racines de $X^n - 1$ constituent le groupe multiplicatif d'un corps ssi $n = q^m - 1$.

3. Montrer que pour la définition plus générale de polynôme minimal vue en cours, les propriétés (M1)-(M6) sont encore vraies.

4. Montrer que le dual d'un code Reed-Solomon est un un code de Reed-Solomon.

5. Montrer que pour un code de Reed-Solomon de longueur $n = q^m - 1$ et de générateur

$$g(X) = (X - \alpha)(X - \alpha^2) \dots (X - \alpha^{d-1}),$$

étendre chaque mot code $c = c_0 \dots c_{n-1}$ en rajoutant $c_n = -\sum_{i=0}^{n-1} c_i$ produit un code de longueur $n + 1$, dimension $n - d + 1$ et distance minimal $d + 1$.