TD – Codes de Reed-Solomon

Exercice 1. *Polynômes et corps finis*

1. Calculer $9+6$, $3-8$, 6×4 et $7/2$ dans $\mathbb{F}_{11}$.
2. Soit $F(X) = 11X^3 + 10X^2 + 8X + 4$ un polynôme à coefficient dans $\mathbb{F}_{13}$.
   i. Calculer $F(4)$.
   ii. Montrer que 9 est racine de F.

Exercice 2. *D'autres corps finis*

On peut définir, pour tout n, un corps fini à 2^n éléments. Pour cela, on choisit un polynôme de degré n sur $\mathbb{F}_2$ *irréductible*, c'est-à-dire un polynôme ϕ qu'on ne peut pas écrire comme produit de deux polynômes de degrés plus petits non constants (c'est l'équivalent des nombres premiers). On peut alors montrer que l'ensemble des polynômes *modulo* ϕ est un corps [1] : on peut additionner, soustraire, multiplier et surtout diviser dans cet ensemble. On le note $\mathbb{F}_{2^n}$.

1. On considère $\phi(X) = X^2 + X + 1$. On admet qu'il est irréductible [2].
   i. Soit $\alpha(X) = X + 1$ et $\beta(X) = X$. Calculer $\alpha+\beta$, $\alpha-\beta$ et $\alpha\times\beta$, *modulo* $\phi(X)$.
   ii. Trouver un inverse de X *modulo* ϕ.
2. On se place dans le cadre général où ϕ est un polynôme irréductible de degré n.
   i. Montrer que le corps $\mathbb{F}_{2^n}$ défini par ϕ a bien 2^n éléments distincts.
   ii. Exprimer en terme d'opérations logiques l'addition de deux éléments de ce corps.
   iii. Qu'est-ce qui rend l'utilisation de ce type de corps intéressante ?
3. Un polynôme à coefficients dans $\mathbb{F}_{2^n}$ est un polynôme dont les coefficients sont eux-mêmes des polynômes. Il faut deux variables : on note X celle de $\mathbb{F}_{2^n}$, et Y celle des polynômes à coefficients dans $\mathbb{F}_{2^n}$.
   i. Quel est le degré du polynôme $(X^4+X+1)Y^2 + (X+1)Y + X^5 + X^3 + X$?

   On se place dans $\mathbb{F}_4$, avec le polynôme $\phi = X^2 + X + 1$. On note $F(Y) = (X+1)Y^2 + Y + X$.
   ii. En évaluant F sur chaque point de $\mathbb{F}_4$, trouver toutes ses racines.

Exercice 3. *Propriétés des codes de Reed-Solomon*

Soit $\mathscr{C}$ un code de Reed-Solomon sur $\mathbb{F}_q$, de dimension k et de longueur n, défini par les points d'évaluation $\alpha_1, \ldots, \alpha_n$.

1. Montrer que $\mathscr{C}$ est un code linéaire : si c_1 et c_2 sont deux mots de codes, alors $\alpha c_1 + \beta c_2$ est un mot de codes, pour tous $\alpha, \beta \in \mathbb{F}_q$.
2. On veut calculer la distance minimale de $\mathscr{C}$. Soit m_1 et m_2 deux messages, et $c_1 = \mathrm{RS}(m_1)$ et $c_2 = \mathrm{RS}(m_2)$ les mots de codes correspondant.
   i. Montrer que la distance entre c_1 et c_2 est $n - t$ où $t = \#\{\alpha_i : F_{m_1}(\alpha_i) = F_{m_2}(\alpha_i)\}$.
   ii. En déduire que la distance minimale est $\geq n - k + 1$.
   iii. Montrer que la distance minimale est $\leq n - k + 1$ en exhibant deux mots de $\mathscr{C}$ à distance $n - k + 1$.
   iv. De quelle autre manière aurait-on pu démontrer que la distance minimale est $\leq n - k + 1$?

Exercice 4. *Singleton, le retour*

1. Soit $\mathscr{C}$ un code $(n, k, d)_q$. Montrer qu'on peut le convertir en un code $(n-1, k, d-1)_q$.
2. En déduire la borne de Singleton, par récurrence sur d.

1. Plus généralement, on peut définir de la même façon un corps à p^n éléments pour tout nombre premier p et tout n. Et on peut montrer réciproquement que tout corps fini possède p^n éléments où p est un nombre premier : il n'existe par exemple aucun corps possédant 6 éléments.
2. Une façon de s'en convaincre est d'essayer toutes les possibilités !