

TD 11 : Codes de Reed-Solomon

Exercice 1.*D'autres corps finis*

On définit souvent les codes de Reed-Solomon sur des codes finis à 2^n éléments pour un certain n . Le but de l'exercice est de montrer comment construire un corps de ce type.

1. Pourquoi est-ce intéressant en pratique ?

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 corps¹ : on peut additionner, soustraire, multiplier et surtout diviser dans cet ensemble. On le note \mathbb{F}_{2^n} .

2. On considère $\phi(X) = X^2 + X + 1$. On admet qu'il est irréductible².
 - 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 .

On se place de manière générale dans le corps \mathbb{F}_{2^n} , défini par un polynôme irréductible ϕ de degré n .

3.
 - 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.
4. On veut maintenant exprimer les autres opérations sur ce corps.
 - i. De quelles opérations a-t-on besoin pour effectuer une multiplication de deux éléments du corps ? Quelle est la complexité obtenue ?

Soit $\alpha \in \mathbb{F}_{2^n}$, et U et V des coefficients de Bézout associés à α et ϕ .

- i. Que vaut $U\alpha + V\phi$?
 - ii. En déduire un algorithme de calcul d'inverse dans \mathbb{F}_{2^n} , avec sa complexité.
5. 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 2.*Propriétés des codes de Reed-Solomon*

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

1. Montrer que \mathcal{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 \mathcal{C} , c'est-à-dire la distance minimale entre deux mots de code. Soit m_1 et m_2 deux messages, et $c_1 = \text{RS}(m_1)$ et $c_2 = \text{RS}(m_2)$ 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 \mathcal{C} à distance $n - k + 1$.
 - iv. De quelle autre manière aurait-on pu démontrer que la distance minimale est $\leq n - k + 1$?

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 !