Corps finis / Codes correcteurs

Questions de cours

Donner une construction du corps à 9 élements et ses tables de multiplication et d'addition.

Montrer que dans un tableau de nombres entiers à 9 lignes et 8 colonnes on peut toujours sélectionner des lignes dont la somme des éléments colonne à colonne est paire.

Exercice 1. *On considère E un espace vectoriel de dimension n sur $\mathbb{F}_q$. Donner le nombre d'éléments de E. Donner le nombre de droites vectorielles de E.*

Exercice 2. *Montrer que $\mathbb{F}_q$ a un sous-corps de cardinal p un nombre premier. En déduire que $q = p^r$ pour un entier strictement positif r. Montrer que $F : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r}$ définie par $F(x) = x^p$ est un automorphisme de corps vérifiant $F(x) = x$ si et seulement si $x \in \mathbb{F}_p \subset \mathbb{F}_{p^r}$.*

Exercice 3. *On définit, pour $(x, y) \in (\mathbb{F}_q^n)^2$, $d(x, y) = \#\{i \in \{1, \dots, n\} | x_i \neq y_i\}$. Montrer que d est une distance.*

Soit $C \subset \mathbb{F}_q^n$ un sous-espace vectoriel. On note $d_{min}(C) = \min\{d(x, y) | x \neq y, (x, y) \in C \times C\}$ la distance minimal de C. Montrer que $d_{min}(C) = \min\{d(x, 0) | x \neq 0, x \in C\}$.

Soit $\sigma : \mathbb{F}_2^n \to \mathbb{F}_2$ définie par $\sigma(x) = \sum x_i$. Quelle est $d_{min}(\ker \sigma)$?

On dit que C corrige e erreurs si quelque soit $y \in \mathbb{F}_q^n$ $\#\{x \in C | d(y, x) \leq e\} \leq 1$. Montrer que si C corrige e erreurs alors $d_{min}(C) > 2e$.

Soit $C \subset \mathbb{F}_q^n$ un sous-espace vectoriel de dimension k montrer que, quitte à réordonner la base canonique $e_1, \dots e_n$, il existe une base de C de la forme $e_i + \sum_{j=k+1}^{n} *_{i,j} e_j$, $i = 1, \dots, k$. En déduire que $d_{min}(C) \leq n - k + 1$.

Exercice 4. *Soient V un sous-espace vectoriel de $\mathbb{F}_2^n$ et $V^\perp = \{x \in \mathbb{F}_2^{2^n - 1} | \forall y \in V, \sum x_i y_i = 0\}$. Donner un exemple de sous-espace $V \neq \{0\}$ tel que $V \subset V^\perp$. On dit que V est isotrope. Montrer que $(V^\perp)^\perp = V$ Montrer que $\dim V + \dim V^\perp = n$. Donner un exemple de sous-espace de $\mathbb{F}_2^n$ isotrope de dimension maximale.*

1. Codes de Hamming

Exercice 5. *Soit H la matrice dont les colonnes sont tous les vecteurs non nuls de $\mathbb{F}_2^n$. Quel est le format de H ? Montrer que les colonnes de H^T forment une base d'un sous-espace vectoriel V_H de $\mathbb{F}_2^{2^n - 1}$. Soit G une matrice dont les lignes forment une base de $V_H^\perp$. Quel est le format de G ? Montrer que l'on peut choisir H par blocs $\begin{bmatrix} A & Id \end{bmatrix}$ et $G = \begin{bmatrix} Id & A^T \end{bmatrix}$.*

Calculer $\#V_H$ et $\#V_G$. Montrer que la distance minimal de V_H est 2^{n-1}. Montrer que la distance minimal de V_G est 3.

Considérons $Enc : \mathbb{F}_2^{2^n - n - 1} \to \mathbb{F}_2^{2^n - 1}$ définie par $Enc(m) = G^T m$. Montrer que $c = G^T m$ si et seulement si $Hc = 0$. Montrer que si $Hc \neq 0$ il existe un unique e dont les coordonnées sont nulles sauf une tel que $H(c + e) = 0$.

Exercice 6. *Avec les notations de l'exercice précédent et $n = 3$. Donner une matrice de contrôle H et sa matrice génératrice G. On reçoit le message encoder par G :*

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}^T$$

par un canal de transmission susceptible d'altérer une coordonnée. Le message reçu est-il correct ? Si non quel est le message envoyé.

Exercice 7. *Votre voisin pense à un nombre entre 0 et 15. Posez lui 7 questions dont les réponses sont 'oui' ou 'non' pour trouver ce nombre même si il vous ment une fois.*

2. Codes de Reed-Solomon

Exercice 8. *Montrer que si $x_1, \dots, x_n$ sont des éléments d'un corps alors* $\det \left[x_i^j\right]_{\substack{1 \leq i \leq n \\ 0 \leq j \leq n-1}} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$.

Exercice 9. *Montrer que le groupe multiplicatif des inversibles de $\mathbb{F}_q$ est un groupe cyclique. Un générateur de ce groupe s'appelle une racine primitive de $\mathbb{F}_q$.*

Exercice 10. *Soit E_k le sous-espace vectoriel de $\mathbb{F}_{2^n}[X]$ des polynômes de degré inférieur à $k < 2^n - 2$ et α une racine primitive de $\mathbb{F}_{2^n}$. Montrer que l'application $Enc : E_k \to \mathbb{F}_{2^m}^{2^m - 1}$ définie par $Enc(P) = \left[P(\alpha^i)\right]_{0 \leq i \leq 2^m - 2}$ est injective et donner un inverse à droite.*

Notons C le sous espace vectoriel de $\mathbb{F}_{2^m}^{2m-1}$ image de Enc. Montrer $d_{min}(C) = n - k + 1$.

Comment utiliser C pour coder (donner une matrice génératrice) un message, repérer les $\frac{1}{2}(n - k + 1)$ erreurs éventuelles dans le message reçu (donner une matrice de contrôle) et le corriger pour obenir le message envoyé ?