CODES CORRECTEURS - TD 1

NICOLAS GUÈS - ANNÉE 2025

Exercice 1 : Corps finis et extensions

On fixe R un anneau. On rappelle que la *caractéristique* $\mathrm{car}R$ de R est définie comme l'unique entier positif n tel que $n\mathbb{Z} = \ker(\mathbb{Z} \to R)$ qui envoie k sur $k \cdot 1_R$.

(1) Montrer que si R est intègre, alors $\mathrm{car}R$ est un nombre premier ou est égale à 0. Donner un exemple pour chacun de ces cas.

(2) **Construction de $\mathbb{F}_4$.** Considérons l'anneau $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1)$. Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$. Compter les éléments de $\mathbb{F}_4$ et construire sa table de multiplication. En déduire que c'est un corps fini.

(3) Montrer en utilisant la caractéristique que tout corps fini K est un espace vectoriel sur $\mathbb{F}_p$ où $p = \mathrm{car}K$. En déduire que son cardinal est une puissance de p.

Exercice 2 : Matrices génératrices et matrices de contrôle

(1) Soit C le code donné par l'application

$$\mathbb{F}_2^3 \to \mathbb{F}_2^4$$

$$(x_1, x_2, x_3) \mapsto (x_1 + x_2, x_2 + x_3, x_1 + x_3, x_1 + x_2 + x_3).$$

Donner la matrice génératrice de ce code. En déduire une matrice de contrôle H.En utilisant le cours, en déduire la distance d du code. Donner un exemple explicite qui montre que ce code ne détecte pas toutes les erreurs de 1 bit.

(2) On se place dans un corps fini K arbitraire. On considère un code linéaire $\phi : K^k \to K^n$ de matrice génératrice M. La plupart du temps, les matrices génératrices sont sous forme *systématique*, à savoir $M = (I_k|A)$ par blocs où A est une matrice de taille $(k, n-k)$. Pour une telle matrice, montrer que $H = (-A^t|I_{n-k})$ est une matrice de contrôle.

(3) En déduire une matrice de contrôle pour : le code de parité et le code de répétition $\times 3$. Lire sur la matrice de contrôle leur distance d et retrouver leur capacité de correction d'erreur t. Montrer que c'est cohérent avec la borne du singleton.

(4) Existe-t-il un code $\phi : \mathbf{F}_2^3 \to \mathbf{F}_2^6$ qui corrige toute erreur de 1 bit?

Exercice 3 : Code de Hamming H_3

On considère le code correcteur de Hamming H_3 sur $\mathbb{F}_2$, dont une matrice génératrice est

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(a) Écrire une matrice de contrôle pour ce code.

(b) Que peut-on dire des colonnes de H ? Donner sa distance et sa capacité de correction d'erreur.

(c) Coder à l'aide de G les trois messages suivants : 1100, 1010 et 1111.

(d) Soit $x \in \mathbf{F}_2^4$ et $y = xG \in \mathbf{F}_2^7$. Si une seule erreur se produit lors de la transmission, alors y devient $z = y + e_i$ pour un certain $1 \leq i \leq 7$. Donc

$$zH = yH + e_iH = e_iH.$$

On pourra donc déterminer i à partir de z, et corriger l'erreur, car les colonnes de H sont distinctes. En utilisant cette idée (la méthode des *syndromes*), dire si les messages reçus suivants sont dans le code, ou les corriger sinon :

$$0110111, \quad 0011000, \quad 0101010.$$