Codes correcteurs d'erreurs : TP

Christophe Ritzenthaler

Quelques codes linéaires généraux

1. Créer le code linéaire binaire de $\mathbb{F}_2^7$ engendré par

$$(1,1,1,0,0,0,0), \quad (1,0,0,1,1,0,0), \quad (0,1,0,1,0,1,0), \quad (1,1,0,1,0,0,1).$$

2. Déterminer les paramètres de ce code. Vérifier que cela est compatible avec les bornes connues.
3. Calculer à la main la matrice systématique, la matrice de contrôle et vérifier le calcul de la distance minimale. Vérifier vos calculs par `Sage`.
4. Soit le mot $(0,1,1,0,1,0,0)$. Est-il dans le code ? Sinon décodez le selon le maximum de vraisemblance, d'abord à la main puis vérifier le résultat par ordinateur.

1. Créer C le code de matrice de contrôle

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

2. Donner une matrice génératrice pour C.
3. Décoder par syndrome $r = (11101)$ et $s = (11011)$.

1. On crée ensuite le code de Hamming sur $\mathbb{F}_2$ de longueur $n = 2^5 - 1$.
2. Vérifier que la distance minimale est 3.

Codes cycliques

Un code linéaire $C \subset \mathbb{F}_2^n$ est dit *cyclique* quand il est stable par l'automorphisme de décalage cyclique

$$\begin{array}{rcl} T : \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ (x_1, \ldots, x_n) & \mapsto & (x_2, \ldots, x_n, x_1) \end{array}$$

On identifie $\mathbb{F}_2^n$ à l'algèbre $\mathbb{F}_2[X]/(X^n - 1)$ par

$$(x_1, \ldots, x_n) \mapsto x_1 X^{n-1} + \cdots + x_{n-1} X + x_n.$$

On désigne ici par la même lettre l'indéterminée X et son image dans le quotient. L'endomorphisme T, modulo cette identification, est l'endomorphisme de multiplication par X. Par définition, un code cyclique est un sous-espace vectoriel stable par multiplication par X, et donc par n'importe quel polynôme en X. Donc, un code linéaire C de longueur n est cyclique

si et seulement si C est un idéal de $\mathbb{F}_2[X]/(X^n-1)$.
L'homorphisme de passage au quotient induit une bijection entre l'ensemble des idéaux de $\mathbb{F}_2[X]/(X^n-1)$ et l'ensemble des idéaux de $\mathbb{F}_2[X]$ qui contiennent (X^n-1). Puisque $\mathbb{F}_2[X]$ est principal, ce sont exactement les idéaux engendrés par les diviseurs (que l'on prend unitaires pour assurer l'unicité) de X^n-1 dans $\mathbb{F}_2[X]$. Le diviseur unitaire g de X^n-1 ainsi associé à un code cyclique C s'appelle le *polynôme générateur* de C. Si $g \neq X^n-1$ (dans le cas contraire C est nul), le code C est engendré (comme espace vectoriel sur $\mathbb{F}_2$) par $g, Xg, ..., X^{n-1-\deg(g)}g$. La dimension de C est dans tous les cas $k = n - \deg(g)$.
Le procédé de codage systématique $\mathbb{F}_2^k \to C$ d'un code cyclique de polynôme générateur g est donné par la division euclidienne par g : le vecteur $(x_1, \ldots, x_k) \in \mathbb{F}_2^k$ est codé par le polynôme $c = c_I - c_R$, où $c_I = x_1X^{n-1} + \ldots + x_kX^{n-k}$, et c_R (de degré $< n-k$) est le reste de la division euclidienne de c_I par g. (Le polynôme c_I porte l'information, et c_R la redondance).
On suppose à partir de maintenant que n est premier avec la caractéristique de $\mathbb{F}_2$, c.-à-d. impair. Cette hypothèse entraîne que le polynôme X^n-1 a n racines distinctes dans son corps de décomposition sur $\mathbb{F}_2$. Notons K ce corps de décomposition, c'est-à-dire le corps engendré par les racines n-ièmes de l'unité sur $\mathbb{F}_2$. On fait le choix d'une racine primitive n-ième de l'unité dans K, que nous noterons α. Le polynôme minimal P de α sur $\mathbb{F}_2$ a pour degré l'ordre r de 2 dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, et ses racines sont $\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^{r-1}}$. On a $K = \mathbb{F}_2[\alpha] = \mathbb{F}_2[X]/P = \mathbb{F}_2^r$. Le polynôme cyclotomique ϕ_n factorise sur $\mathbb{F}_2$ en produit de facteurs irréductibles de degré r (par exemple $\phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ se factorise en $(X^4+X+1)(X^4+X^3+1)$ sur $\mathbb{F}_2$), et P est un de ces facteurs. Le polynôme générateur g va être déterminé par ses racines dans K, qui forment un sous-ensemble de l'ensemble $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ des racines n-ièmes de l'unité (les zéros du code). Soit Σ un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$. Le polynôme $g_\Sigma = \prod_{i\in\Sigma}(X-\alpha^i)$ est un diviseur de X^n-1 à coefficients dans $\mathbb{F}_2$ si et seulement si Σ est stable par multiplication par 2 (se souvenir que $\mathbb{F}_2$ est l'ensemble des éléments de K laissés fixes par l'élévation au carré). En conclusion, on a une bijection entre les codes cycliques de longueur n et les sous-ensembles de $\mathbb{Z}/n\mathbb{Z}$ stables par multiplication par 2. La configuration des racines du polynôme générateur nous renseigne sur la distance minimale du code cyclique.

Proposition 0.1. *Si Σ contient s entiers consécutifs $a+1, a+2, \ldots, a+s$ modulo n, alors le code cyclique de polynôme générateur g_Σ est nul ou a une distance minimum supérieure ou égale à $s+1$.*

La démonstration est une application des propriétés du déterminant de Vandermonde.
On s'intéresse maintenant aux codes suivants.

1. Décomposer $x^{15}-1$ sur $\mathbb{F}_2$. Soit C un code cyclique de longueur 15 sur $\mathbb{F}_2$ de polynôme générateur $g = x^4 + x + 1$. Quelle est la dimension du code ? Quelle est sa distance minimale ? Écrire une matrice de contrôle.
2. Le satellite d'exploration de Jupiter, Galileo, utilise un code cyclique de longueur 255 et de dimension 223. En utilisant la proposition, déterminer quel polynôme générateur a le plus de chance d'avoir une grande distance minimale.