L3 Calcul Formel
Université de Lorraine

TP 4 : Codes correcteurs

Clément Dell'Aiera

1 Codes correcteurs

Nos deux protagonistes préférés, Alice (A) et Bob (B) ont réussi les TP 2 et 3. Ils savent donc trouver de très grands entiers premiers (TP 3) et s'en servir pour coder et décoder leurs messages (TP 2). Ils prennent toutefois conscience que leur canal de transmission est bruité ! De façon aléatoire, un voire plusieurs bits de la transmission peuvent être altérés. Pour remédier à ce problème, ils décident d'utiliser la théorie des codes correcteurs.

A et B utilisent toujours un alphabet $\mathcal{A}$ à q éléments. Nous supposerons que $\mathcal{A} = \mathbb{F}_q$ est le corps à q éléments, qui s'évalue en Sage grâce à $A = GF(q)$. Un mot sera un élément x de $\mathcal{A}^n$, qui est un espace vectoriel de dimension n. On muni l'ensemble des mots de la distance de Hamming

$$d(x, y) = Card\{j \in [1, n] : x_j \neq y_j\}$$

et on définit le poids d'un élément comme

$$w(x) = Card\{j \in [1, n] : x_j \neq 0\}.$$

Définition 1.
- Un code $\mathcal{C}$ est un sous ensemble non vide de $\mathcal{A}^n$ qui possède au moins 2 éléments distincts.
- Un code linéaire est un code $\mathcal{C}$ qui est un sous-espace vectoriel de $\mathcal{A}^n$.
- Un code est binaire si $\mathcal{A} = \mathbb{F}_2$, ternaire si $\mathcal{A} = \mathbb{F}_3$.
- La distance d'un code $\mathcal{C}$ est définie comme

$$d(\mathcal{C}) = \min_{x \neq y \in \mathcal{C}} d(x, y).$$

- On définit $t(\mathcal{C})$ comme le nombre maximal d'erreurs qui sont corrigés par le code.

Voici quelques questions d'ordre théorique (i.e. à résoudre avec un crayon).

1. Montrer que $t(\mathcal{C}) = E[\frac{d(\mathcal{C})-1}{2}]$, et $d(\mathcal{C}) = 2t(\mathcal{C}) + 1$ ou $2t(\mathcal{C}) + 2$.
2. Si moins de $d(\mathcal{C}) - 1$ erreurs sont commises, on peut détecter la présence d'erreur(s). Pourquoi ?

3. Montrer que si t erreurs ont été commises lors de la transmission d'un message m, telles que $2t+1 \leq d(\mathcal{C})$, alors il existe un unique $x \in \mathcal{C}$ tel que $d(x,m) \leq d(\mathcal{C})$.

A un code linéaire $\mathcal{C}$, on associe
- Une matrice vérificatrice $H \in \mathfrak{M}_{n-k,n}(\mathcal{A})$ de rang $n-k$ dont les lignes forment une base des formes linéaires s'annulant sur $\mathcal{C}$.
- Une matrice génératrice $G \in \mathfrak{M}_{k,n}(\mathcal{A})$ de rang k dont les lignes forment une base de $\mathcal{C}$.

On a donc $GH^T = 0$ et $HG^T = 0$. De plus $\mathcal{C}$ est le noyau de H. Si A envoie le message $x \in \mathcal{C}$ à B, que ce dernier reçoit y, on suppose qu'une seule erreur a été commise. Comment B peut-il tester la présence d'erreur et, le cas échéant, retrouver x ? On note $e = y - x$ l'erreur commise.

B calcule Hy.
Si $Hy = 0$, $y \in \mathcal{C}$ et $y = x$.
Sinon, $Hy \neq 0$ et, comme une seule erreur a été commise, il existe un unique j tel que He_j soit proportionnel à Hy, i.e. $\exists! j, \exists a \in \mathcal{A}, Hy = aHe_j = H(ae_j)$.
Alors $x = y - ae_j$.

1. Implémenter une fonction **Test** qui prend en entrée un message bruité ainsi qu'une matrice vérificatrice associée à un code $\mathcal{C}$; et retourne $True$ si le message appartient au code défini par H, $False$ sinon.
2. Implémenter une fonction **Code** qui prend en entrée un message à envoyer ainsi qu'une matrice vérificatrice associée à un code $\mathcal{C}$; et retourne le message codé.
3. Implémenter une fonction **Bruit** qui prend en entrée un message non bruité et le bruite. On prendra pour cela un bit du message au hasard que l'on inverse ($0 \mapsto 1$ et $1 \mapsto 0$).
4. Implémenter une fonction qui, étant donné un code et un message reçu, vérifie s'il y a une erreur, et le cas échéant, corrige l'erreur. La fonction doit retourner le message corrigé. En cas d'erreur, en plus du message corrigé, la fonction afficher un message du type "Erreur detectée sur le bit numéro j" avec j la position de l'erreur.
5. Combien le code de Hamming $H(4,3)$ contient-t-il de mots ? Calculer sa distance, sa capacité de détection et de correction.

2 Construction du polynôme générateur

Polynôme cyclotomique
Entrée : $n \in \mathbb{N}^*$
Sortie : Φ_n

1. Déterminer la décomposition en facteur premier de $n = p_1^{\alpha_1}...p_k^{\alpha_k}$
2. $m = p_1 p_2 ... p_k$
3. $P_0 = X - 1$
4. Pour $j = 1, .., k$ faire $P_j \leftarrow P_{j-1}(X^{p_j})//P_{j-1}(X)$
5. Retourner $P_k X^{n/m}$

Cantor-Zassenhaus
Entrée : $P \in \mathbb{F}_2[X]$ unitaire sans facteur carré ayant tous des facteurs irréductibles de même degré d, $deg\ P = n > 0$.
Sortie : Un facteur non trivial de P, ou $False$.

1. Choisir $Q \in \mathbb{F}_2[X]$ au hasard de degré $< n$.
2. $g = pgcd(P, Q)$
3. Si $g = 1$, alors retourner g
4. $a = T_d(Q) \pmod P$
5. $g \leftarrow pgcd(a - 1, P)$
6. Si $g \neq 1$ et $g \neq P$, retourner g, sinon retouner $False$