L3 Calcul Formel
Université de Lorraine

TP 4 : Codes correcteurs

Clément Dell'Aiera

1 Code de Hamming

1. Implémenter une fonction **Test** qui prend en entrée un message bruité ainsi qu'une matrice définissant un code BCH ; 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 définissant un code BCH ; et retourne le message codé.
3. Implémenter une fonction 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 $False$