1 Encodage

On part d'un message m que l'on veut encoder en un mot de code c, avec g le polynôme générateur du code.
La méthode d'encodage non systématique pour les BCH est de faire $c = m * g$, **MAIS** ici pour simplifier le décodage de c, on va utiliser l'encodage sous forme systématique, qui consiste en 2 étapes :

1. $m_c = ([0....0..m] \mod g) = (m * x^{n-k} \mod g)$, c'est le modulo de m décalé de $n-k$ zeros,m_c est de taille $n-k$
2. $c = [m_c m]$, on concatene m_c et m

Pour vérifier que l'opération fonctionne, on peut faire :
$(c \mod g) = ([m_c m] \mod g) = ([m_c 0...0] + [0..0m] \mod g) = [m_c] + [m_c] = 0$

On a $[m_c 0...0] \mod g = [m_c]$ car m_c est un polynome de degré plus petit que g. L'opération de modulo se fait avec des registres à décalage.

2 Décodage

Pour le décodage, on peut implémenter différentes méthodes, mais la méthode par syndromes semble plus facile.
Lors du décodage on a $c' = c + e$ avec e une erreur causée par le canal. On fait $(c' \mod g) = (c + e \mod g) = 0 + (e \mod g)$
On liste toutes les erreurs e_i qui peuvent être corrigées par le code, et on met dans un tableau leur modulo. Par exemple pour le code correcteur qui corrige une erreur, on crée une matrice S_1.

$$S_1 = \begin{bmatrix} e1 \mod g \\ e2 \mod g \\ .... \\ .... \\ e31 \mod g \end{bmatrix}$$

Pour cet exemple $e_i = [0...010...0]$ avec le 1 à la ième position. Pour le décodage, on compare $(c' \mod g)$ avec chacune des lignes de S_1 et on en déduit l'erreur e_i. Pour le deuxième code correcteur, la matrice sera beaucoup plus grande.
Une fois l'erreur corrigée, on peut aisément récupérer le message m car $c = [m_c m]$, d'où l'utilité de la forme systématique.