

CODES CYCLIQUES

I) Définition:

Un code cyclique est un code polynomial qui contient toutes les permutations circulaires de ses mots de code.

Ex: si $1100 \in C$, Alors $(1100, 0110, 0011, 1001) \in C^4$

II) Propriétés:

→ Avec P mot de code de longueur n : $\forall A \in \mathbb{M}_{n-1}[x], PA \in C$

→ Matrice génératrice de la forme $G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-2} & (0) \\ & g_0 & g_1 & \dots & g_{n-2} \\ & & (0) & \ddots & \ddots \\ & & & g_0 & g_1 & \dots & g_{n-2} \end{pmatrix}$

→ g est un facteur de $x^n - 1$:

il existe H polynôme tq $\begin{cases} \deg H = k \\ H(x)g(x) = x^n - 1 \end{cases}$. H est polynôme de contrôle.

donc: $(P \in C) \Leftrightarrow (P(x)H(x) \equiv 0 [x^n - 1])$

III) Codage et décodage:

codage par la matrice génératrice ou par la méthode des polynômes.
décodage en tant que code polynomial.

$$X(x) = Q(x)G(x) + \underbrace{A(x)}_{\text{polynôme syndrome}}.$$