TIPE

padovan dorian

May 2025

idée clé : Unicité des polynômes d'interpolation de Lagrange

1) Construction du polynôme : soient n couples de réels : $(1, y_1), (2, y_2), ...(n, y_n)$ on pose :

$P(x) = \sum_{i=0}^{n} y_i \cdot \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x-j}{i-j}$ on a alors : $P(x_i) = y_i$

2)Valeurs de redondance : évalutation de P en les valeurs :$(n+1, ..., n+k)$

3)Envoi de $n+k$ paquets numerotés :

·Code linéaire $C(n,k)$: $\phi : (\mathbb{F})^k \longrightarrow (\mathbb{F})^n$

·Matrice génératrice $G \in M_{k,n}(\mathbb{F})$

·$A \in Gl_n(\mathbb{F})$: $G' = AG$ génère $C(n,k)$

·Si G est de la forme : $\begin{bmatrix} L & R \end{bmatrix}$

·Matrice normalisée : $G' = \begin{bmatrix} I_k & T \end{bmatrix}$ avec $T = L^{-1}R$

code de parité $C(5,4)$: $\phi(1000) = 10001$

$x^T = [x_0, x_1, x_2, x_3]$

$\phi(x)^T = [x_0, x_1, x_2, x_3, x_0 + x_1 + x_2 + x_3 mod 2]$

$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Soit $G' = \begin{bmatrix} I_k & T \end{bmatrix}$, la matrice génératrice normalisé de $C(n,k)$

Proposition 1

Soit H la matrice de contrôle (r,n) $H = \begin{bmatrix} T^T & -I_r \end{bmatrix}$. Alors $x^T = [x_1, ..., x_n] \in C(n,k)$ si et seulement si $Hx = 0$

Par exemple pour le code de parité C(5,4) : $H = [1,1,1,1]$

Preuve. Soit $x \in \mathbb{F}^n$, existe $z \in \mathbb{F}^k$ tel que $x = zG$ la matrice normalisé. D'où :

$$xH^T = z[I_k \mid T] \begin{bmatrix} T^T \\ -I_k \end{bmatrix}$$

Par conséquent,

$$xH^T = z(T^T - T^T) = 0.$$

Réciproquement, si $xH^T = 0$ alors :

$$[x_1, x_2, ..., x_n]H^T = 0,$$

Cela induit que pour $j = 1, ..., r$ que :

$$[x_1, x_2, ..., x_n][T_{1,j}, ..T_{k,j}]^T = 0,$$

Cela donne :

$$[x_{k+1}, ...x_{k+r}] = [x_1, ...x_k]T$$

Finalement, on a :

$$[x_1, ..., x_n] = [x_1, ..., x_k][Ik|T] = xG$$

ce qui montre que $x \in C$.

Soit $G = A \cdot G'$, avec $A \in \mathcal{M}_k(\mathbb{F})$ une matrice inversible et G' une matrice génératrice de C.

Alors :

$$\mathrm{Im}(G') = \{xG' \mid x \in \mathbb{F}^k\} = C,$$

et donc :

$$\mathrm{Im}(G) = \{xG \mid x \in \mathbb{F}^k\} = \{xAG' \mid x \in \mathbb{F}^k\} = \{yG' \mid y = xA \in \mathbb{F}^k\} = \mathrm{Im}(G').$$

Ainsi :

$$\mathrm{Im}(G) = C.$$