TS226
-
Codes correcteur d'erreur

Romain Tajan

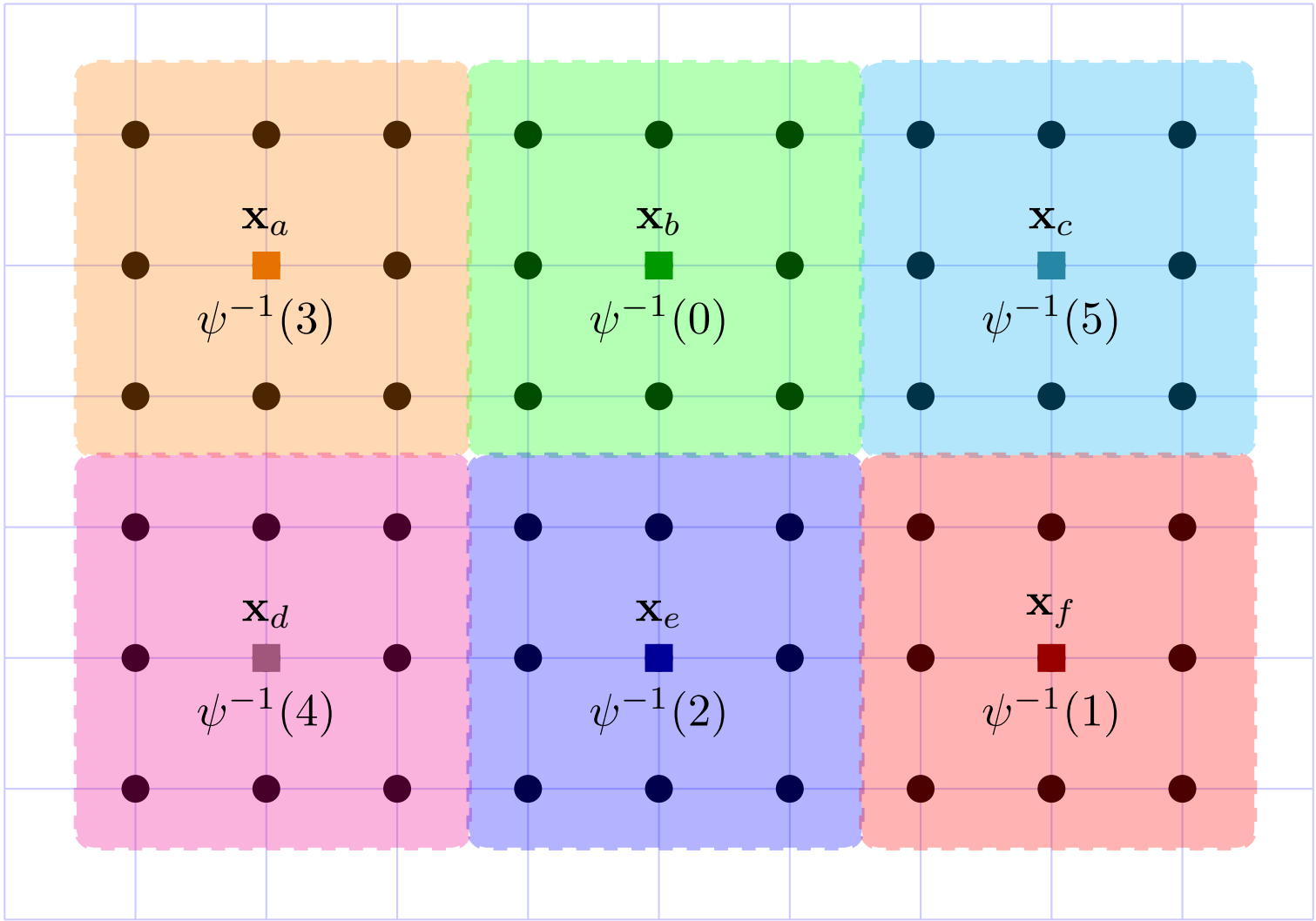
2 octobre 2019

Plan

Dernier QCM

Mettre la question 1

Plan


$\mathbf{x}_a$
$\psi^{-1}(3)$
$\mathbf{x}_b$
$\psi^{-1}(0)$
$\mathbf{x}_c$
$\psi^{-1}(5)$
$\mathbf{x}_d$
$\psi^{-1}(4)$
$\mathbf{x}_e$
$\psi^{-1}(2)$
$\mathbf{x}_f$
$\psi^{-1}(1)$

Décodage du Maximum a Posteriori

Définition

- Soit $\mathcal{C}$ un code (M, n) donné.

- Le **décodeur** du **Maximum A Posteriori** (**MAP**) est la fonction de $\mathbf{y}$ définie par :

$$\Psi_{MAP}(\mathbf{y}) = \underset{w \in \mathcal{M}}{\operatorname{argmax}}\, \mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})$$

Le décodeur MAP minimise P_e

Plan

Capacité

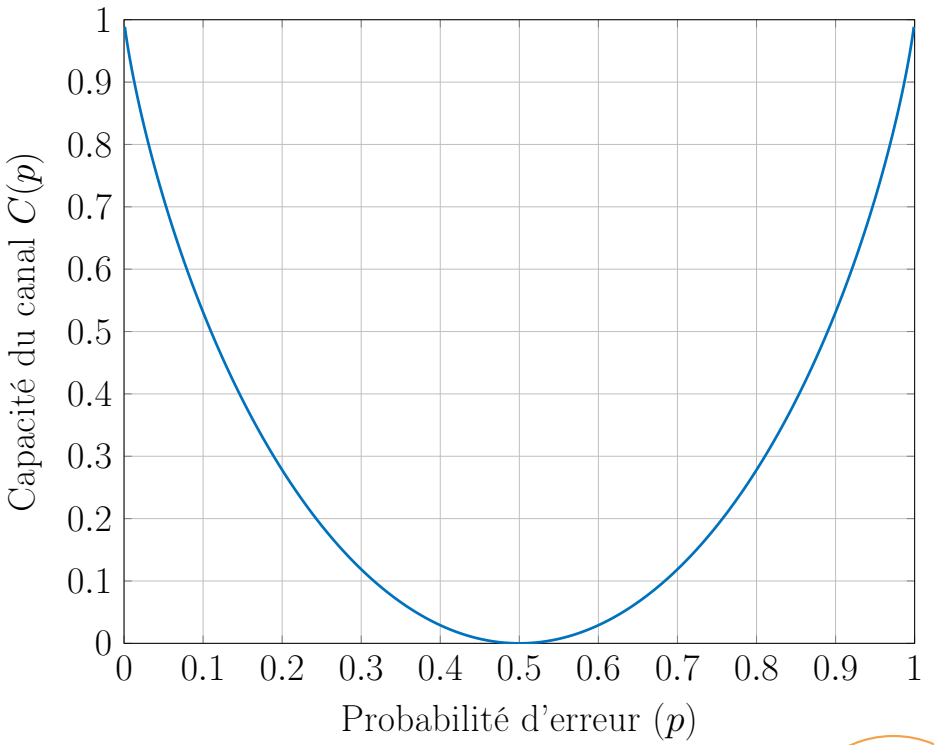
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

$$C = \sup_{p(x)} \mathbb{I}(X, Y)$$

La **capacité** du canal BSC

$$C(p) = 1 + p\log_2(p) + (1-p)\log_2(1-p)$$

est atteinte ssi $X \sim \mathcal{B}(0.5)$



Théorème du codage canal de Shannon

Soit $(\mathcal{X}, \mathcal{Y}, p(y|x))$ un **canal discret sans mémoire** de capacité $C \geq 0$ et soit $R < C$

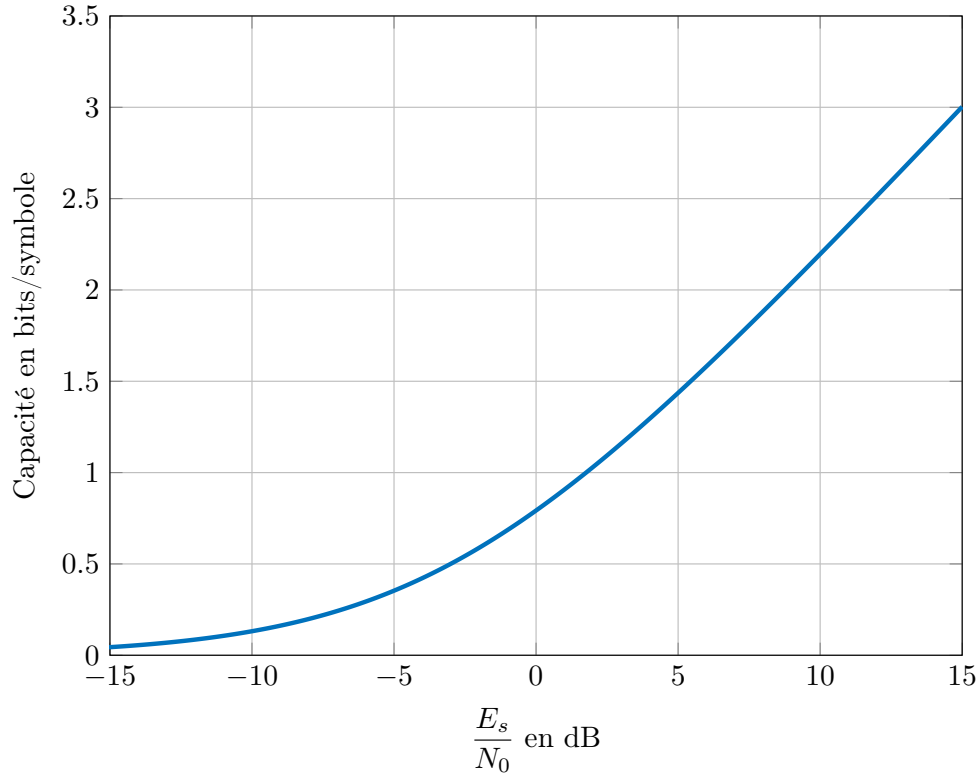
1. Il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ où $\mathcal{C}_n$ est de longueur n, de rendement R_n et de probabilité d'erreur maximale $\lambda^{(n)}$ telle que

$$\lambda^{(n)} \to 0, \text{ et } R_n \to R$$

2. Réciproquent, s'il existe une suite de codes $(\mathcal{C}_n)_{n\geq 1}$ telle que $\lambda^{(n)} \to 0$ alors

$$\limsup_n R_n \leq C$$

1. Quelque soit $\epsilon > 0$, il existe **toujours** un code $\mathcal{C}_n$ de longueur n et de rendement $R_n < C$ tel que $\lambda^{(n)} \leq \epsilon$.
2. La remarque précédente ne dit cependant rien sur la longueur n de ce code, qui **peut être éventuellement très grande**.
3. L'item (2) du théorème montre que C est une borne supérieure des rendements de codes **fiables**
4. La preuve de (1) (Cover & Thomas **Information theory**) repose sur une génération aléatoire des codes $\mathcal{C}_n$



La **capacité d'un canal Gaussien sans mémoire** avec contrainte d'énergie E_s est

$$C = \sup_{p(x):\mathbb{V}(X)\leq E_s} \mathbb{I}(X,Y) = \frac{1}{2}\log_2\left(1+2\frac{E_s}{N_0}\right)$$

- Le supremum est ici pris sur les densités de probabilités $p(x)$ telles que $\mathbb{V}(X) \leq \sigma^2$.
- Le supremum est atteint par $p(x) = \mathcal{N}(0, E_s)$

Plan

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**
2. Dans cette section on notera $\mathbb{F}_2$ le **corps** $(\{0, 1\}, \oplus, \cdot)$ où :
   - Pour $x, y \in \mathbb{F}_2$, $x \oplus y = (x + y) \mod 2$ ($\equiv$ OU exclusif)
   - Pour $x, y \in \mathbb{F}_2$, $x \cdot y$ est le produit "classique" entre x et y ($\equiv$ ET)
3. $\mathbb{F}_2$ est un corps fini à deux éléments ($\mathbb{Z}/2\mathbb{Z}$)
4. Par la suite on notera $\oplus \rightsquigarrow +$
5. $(\mathbb{F}_2^n, +, \cdot)$ est un **espace vectoriel** où
   - Pour $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, $\quad \mathbf{x} + \mathbf{y} = [x_0 + y_0, x_1 + y_1 \ldots, x_{n-1} + y_{n-1}]$
   - Pour $x \in \mathbb{F}_2$ et $\mathbf{y} \in \mathbb{F}_2^n$, $\quad x \cdot \mathbf{y} = [x \cdot y_0, x \cdot y_1, \ldots, x \cdot y_{n-1}]$

Code linéaire en bloc

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$.
$\mathcal{C}$ est dit **linéaire** si et seulement si, il existe k vecteurs $\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1} \in \mathbb{F}_2^n$ tels que, pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i$$

avec $u_i \in \mathbb{F}_2$

Remarques

1. L'ensemble $\mathcal{B}_\mathcal{C} = \{\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}\}$ est appelé **base** de $\mathcal{C}$.
2. $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k (si $\mathcal{B}_\mathcal{C}$ est une base libre)

Matrice Génératrice

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, il existe une matrice G de taille $k \times n$ telle que pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \mathbf{u}G$$

Par définition on a

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \vdots \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

1. G est appelé **matrice génératrice** du code $\mathcal{C}$

Matrice Génératrice

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, il existe une matrice G de taille $k \times n$ telle que pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \mathbf{u}G$$

Par définition on a

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \vdots \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

1. G est appelé **matrice génératrice** du code $\mathcal{C}$
2. Pour ce cours G est de **rang plein**

Matrice Génératrice

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, il existe une matrice G de taille $k \times n$ telle que pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \mathbf{u}G$$

Par définition on a

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \vdots \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

1. G est appelé **matrice génératrice** du code $\mathcal{C}$
2. Pour ce cours G est de **rang plein**
3. Pour un code $\mathcal{C}$, il existe plusieurs matrices génératrices

Matrice Génératrice

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, il existe une matrice G de taille $k \times n$ telle que pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \mathbf{u}G$$

Par définition on a

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \vdots \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

1. G est appelé **matrice génératrice** du code $\mathcal{C}$
2. Pour ce cours G est de **rang plein**
3. Pour un code $\mathcal{C}$, il existe plusieurs matrices génératrices
4. Permuter / combiner les lignes de G ne change pas $\mathcal{C}$

Matrice Génératrice

Code linéaire

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, il existe une matrice G de taille $k \times n$ telle que pour tout $\mathbf{c} \in \mathcal{C}$,

$$\mathbf{c} = \mathbf{u}G$$

Par définition on a

$$G = \begin{pmatrix} \mathbf{g_0} \\ \mathbf{g_1} \\ \vdots \\ \mathbf{g_{k-1}} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix}$$

1. G est appelé **matrice génératrice** du code $\mathcal{C}$
2. Pour ce cours G est de **rang plein**
3. Pour un code $\mathcal{C}$, il existe plusieurs matrices génératrices
4. Permuter / combiner les lignes de G ne change pas $\mathcal{C}$
5. Permuter les colonnes de G change l'espace $\mathcal{C}$ mais ne change pas les performances du code

Code dual | Matrice de parité

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, on appelle **code dual** :

$$\mathcal{C}_d = \{\mathbf{v} \in \mathbb{F}_2^n : \forall \mathbf{c} \in \mathcal{C} \ < \mathbf{v}, \mathbf{c} >= 0\} \ (= \mathcal{C}^{\perp})$$

où $< \mathbf{v}, \mathbf{c} >= \sum_{i=0}^{n-1} v_i c_i$

1. La dimension du sous-espace vectoriel $\mathcal{C}_d$ est $n - k$

Code dual | Matrice de parité

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, on appelle **code dual** :

$$\mathcal{C}_d = \{\mathbf{v} \in \mathbb{F}_2^n : \forall \mathbf{c} \in \mathcal{C} \ < \mathbf{v}, \mathbf{c} >= 0\} \ (= \mathcal{C}^{\perp})$$

où $< \mathbf{v}, \mathbf{c} >= \sum_{i=0}^{n-1} v_i c_i$

1. La dimension du sous-espace vectoriel $\mathcal{C}_d$ est $n - k$
2. Soit $\mathcal{B}_{\mathcal{C}_d} = \{\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k-1}\}$ une base de $\mathcal{C}_d$, alors $\mathcal{C}_d$ a pour matrice génératrice

$$H = \begin{pmatrix} \mathbf{h_0} \\ \mathbf{h_1} \\ \vdots \\ \mathbf{h_{n-k-1}} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

Code dual | Matrice de parité

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, on appelle **code dual** :

$$\mathcal{C}_d = \left\{\mathbf{v} \in \mathbb{F}_2^n : \forall \mathbf{c} \in \mathcal{C} \ < \mathbf{v}, \mathbf{c} >= 0\right\} (= \mathcal{C}^{\perp})$$

où $< \mathbf{v}, \mathbf{c} >= \sum_{i=0}^{n-1} v_i c_i$

1. La dimension du sous-espace vectoriel $\mathcal{C}_d$ est $n - k$
2. Soit $\mathcal{B}_{\mathcal{C}_d} = \{\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k-1}\}$ une base de $\mathcal{C}_d$, alors $\mathcal{C}_d$ a pour matrice génératrice

$$H = \begin{pmatrix} \mathbf{h_0} \\ \mathbf{h_1} \\ \vdots \\ \mathbf{h_{n-k-1}} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

3. Le code $\mathcal{C}$ peut être défini comme $\mathcal{C} = \left\{\mathbf{c} \in \mathbb{F}_2^n : \mathbf{c}H^T = \mathbf{0}\right\} (= (\mathcal{C}^{\perp})^{\perp})$

Code dual | Matrice de parité

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ linéaire, on appelle **code dual** :

$$\mathcal{C}_d = \left\{\mathbf{v} \in \mathbb{F}_2^n : \forall \mathbf{c} \in \mathcal{C} \ < \mathbf{v}, \mathbf{c} >= 0\right\} (= \mathcal{C}^{\perp})$$

où $< \mathbf{v}, \mathbf{c} >= \sum_{i=0}^{n-1} v_i c_i$

1. La dimension du sous-espace vectoriel $\mathcal{C}_d$ est $n - k$
2. Soit $\mathcal{B}_{\mathcal{C}_d} = \{\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{n-k-1}\}$ une base de $\mathcal{C}_d$, alors $\mathcal{C}_d$ a pour matrice génératrice

$$H = \begin{pmatrix} \mathbf{h_0} \\ \mathbf{h_1} \\ \vdots \\ \mathbf{h_{n-k-1}} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix}$$

3. Le code $\mathcal{C}$ peut être défini comme $\mathcal{C} = \left\{\mathbf{c} \in \mathbb{F}_2^n : \mathbf{c}H^T = \mathbf{0}\right\} (= (\mathcal{C}^{\perp})^{\perp})$
4. H est appelée matrice de parité du code $\mathcal{C}$ et vérifie $GH^T = 0_{k \times n-k}$

Mettre la question 2

Mettre la question 3

Mettre la question 4

Encodeur binaire systématique

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ pour un canal à entrées binaires. Un encodeur $\varphi(\cdot)$ est dit **systématique** ssi

$$\forall \mathbf{u} \in \mathbb{F}_2^k, \varphi(\mathbf{u}) = [\mathbf{p}\ \mathbf{u}] \text{ avec } \mathbf{p} \in \mathbb{F}_2^{n-k}$$

Encodeur binaire systématique

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ pour un canal à entrées binaires. Un encodeur $\varphi(\cdot)$ est dit **systématique** ssi

$$\forall \mathbf{u} \in \mathbb{F}_2^k, \varphi(\mathbf{u}) = [\mathbf{p}\ \mathbf{u}] \text{ avec } \mathbf{p} \in \mathbb{F}_2^{n-k}$$

Si $\mathcal{C}$ est linéaire alors il existe une matrice génératrice sous la forme

$$G = \begin{pmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,0} & \cdots & p_{k,n-k-1} & 0 & 0 & \cdots & 1 \end{pmatrix} = [P \quad I_k]$$

Encodeur binaire systématique

Soit $\mathcal{C}$ un code $(M = 2^k, n)$ pour un canal à entrées binaires. Un encodeur $\varphi(\cdot)$ est dit **systématique** ssi

$$\forall \mathbf{u} \in \mathbb{F}_2^k, \varphi(\mathbf{u}) = [\mathbf{p}\ \mathbf{u}] \text{ avec } \mathbf{p} \in \mathbb{F}_2^{n-k}$$

Si $\mathcal{C}$ est linéaire alors il existe une matrice génératrice sous la forme

$$G = \begin{pmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,0} & \cdots & p_{k,n-k-1} & 0 & 0 & \cdots & 1 \end{pmatrix} = [P \quad I_k]$$

La matrice de parité associée à la matrice G précédente

$$H = \begin{pmatrix} 1 & 0 & \cdots & 0 & p_{0,0} & \cdots & p_{k,0} \\ 0 & 1 & \cdots & 0 & p_{0,1} & \cdots & p_{k,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{0,n-k-1} & \cdots & p_{k,n-k-1} \end{pmatrix} = [I_{n-k} \quad P^T]$$

Remarques sur les encodeurs systématiques

$$G = \begin{pmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,0} & \cdots & p_{k,n-k-1} & 0 & 0 & \cdots & 1 \end{pmatrix} = [P \quad I_k]$$

1. Un encodeur systématique comporte le message **en clair**

Remarques sur les encodeurs systématiques

$$G = \begin{pmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,0} & \cdots & p_{k,n-k-1} & 0 & 0 & \cdots & 1 \end{pmatrix} = [P \quad I_k]$$

1. Un encodeur systématique comporte le message **en clair**
2. Les encodeurs systématiques sont souvent moins complexes que leurs équivalents non-systématiques

Remarques sur les encodeurs systématiques

$$G = \begin{pmatrix} p_{0,0} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k,0} & \cdots & p_{k,n-k-1} & 0 & 0 & \cdots & 1 \end{pmatrix} = [P \quad I_k]$$

1. Un encodeur systématique comporte le message **en clair**
2. Les encodeurs systématiques sont souvent moins complexes que leurs équivalents non-systématiques
3. Une matrice d'encodage systématique peut être trouvée pour tout code linéaire en bloc de matrice génératrice **pleine** (à des permutations de colonnes près)
   $\rightsquigarrow$ **Pivot de Gauss**

Détection d'erreurs

Correction d'erreurs

Mettre la question 5