TS345
-
Codage pour la 5G

Romain Tajan

9 octobre 2019

TS345 en bref...

Organisation du module

- 6 créneaux (1h20) de cours
- 3 créneaux de TP (2h40)

Découpage des cours

- 1 créneau de **rappels sur les codes correcteurs** | **sur la capacité de Shnanon**
- 3 créneaux sur les **Codes LDPC**
- 2 créneaux sur les **Codes Polaires**

Plan

Plan

Un peu d'histoire...

1948 **Shannon** - capacité d'un canal (non constructive)

1955 **Elias** - Code convolutifs (GSM)

1960 **Reed et Solomon** - Codes RS (CD $\rightarrow$ BluRay, QR, DVB-S, RAID6)

Gallager - Codes LDPC

1966 **Forney** - Codes concatennés (Pioneer (1968-1972), Voyager (1977))

1967 **Viterbi** - Décodage optimal des codes convolutifs

1993 **Berrou, Glavieux et Thitimajshima** - Turbocodes (3G/4G, deep-space)

1996 **MacKay** - Ré-invente les LDPC (DVB-S2, WiFi, 5G)

2008 **Arikan** - Codes Polaires (5G)

Plan

Le canal...

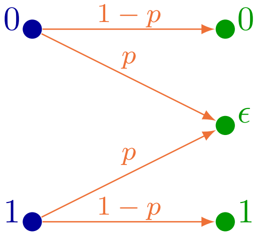
Un **canal** est défini par un triplet : $(\mathcal{X}, \mathcal{Y}, p(y|x))$ où

- $\mathcal{X}$ est l'**alphabet d'entrée**
- $\mathcal{Y}$ est l'**alphabet de sortie**
- $p(y|x)$ est la **probabilité de transition**

Soit $n \in \mathbb{N}$ et soit le canal $(\mathcal{X}^n, \mathcal{Y}^n, p(\mathbf{y}|\mathbf{x}))$, ce canal est dit "**sans mémoire**" si sa probabilité de transition vérifie

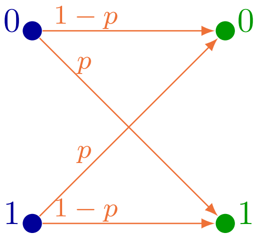
$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i)$$

Le canal à effacement binaire



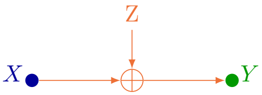
- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, \epsilon, 1\}$
- $p(\epsilon|0) = p(\epsilon|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile pour les couches hautes, pour le stockage

Le canal binaire symétrique



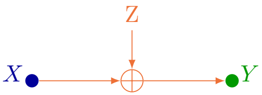
- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, 1\}$
- $p(1|0) = p(0|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile après décision

Le canal additif gaussien



- $\mathcal{X} = \mathbb{R}$
- $\mathcal{Y} = \mathbb{R}$
- $p(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(y-x)^2}$

Le canal additif gaussien à entrées binaires



- $\mathcal{X} = \{-1, 1\}$
- $\mathcal{Y} = \mathbb{R}$
- $p(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(y-x)^2}$

Code (M, n)

$\boxed{\text{Un code } (M, n) \text{ pour le canal } (\mathcal{X}^n, \mathcal{Y}^n, p(\mathbf{y}|\mathbf{x}))}$ est composé de 3 éléments

- Un ensemble de M **messages**. On notera cet ensemble $\mathcal{M} = \{0, 1, \ldots, M-1\}$
- Une fonction d'**encodage** (ou encodeur) notée ϕ :

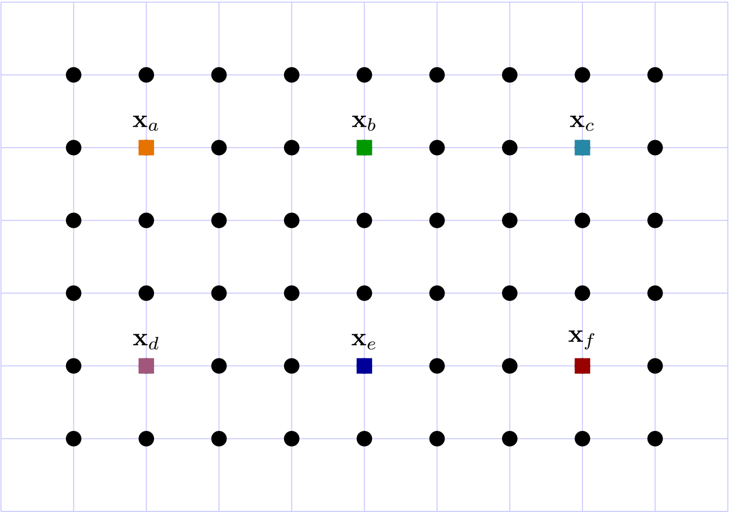
$$\begin{aligned} \phi : \mathcal{M} &\rightarrow \mathcal{X}^n \\ W &\mapsto \mathbf{X} = \phi(W) \end{aligned}$$

$$\boxed{\phi(\cdot) \text{ doit être } \textbf{injective}}$$

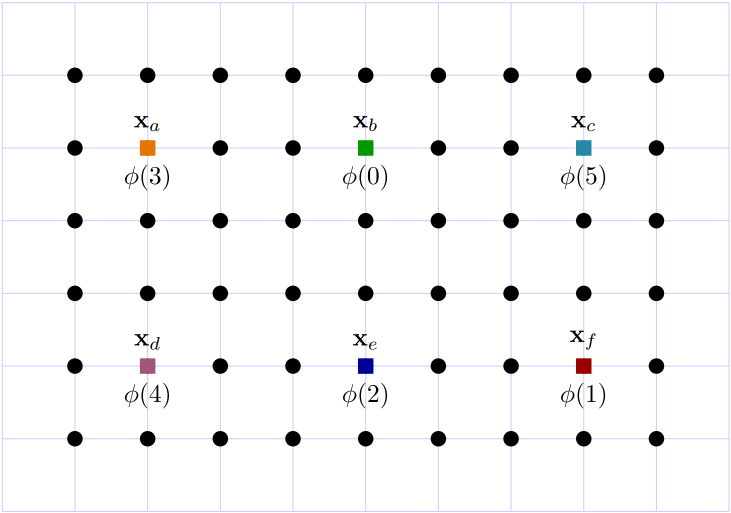
- Une fonction de **décodage** (ou décodeur) notée ψ :

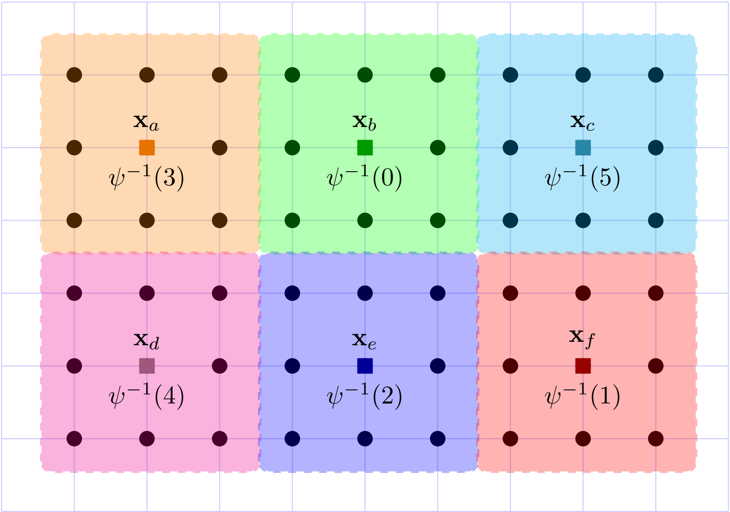
$$\begin{aligned} \psi : \mathcal{Y}^n &\rightarrow \mathcal{M} \\ \mathbf{Y} &\mapsto \hat{W} = \psi(\mathbf{Y}) \end{aligned}$$

$$\boxed{\psi(\cdot) \text{ doit être } \textbf{surjective}}$$



$\mathbf{x}_a$
$\mathbf{x}_b$
$\mathbf{x}_c$
$\mathbf{x}_d$
$\mathbf{x}_e$
$\mathbf{x}_f$


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


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

Probabilité d'erreur

Si le mot de code $W = w$ est envoyé, une erreur se produit ssi $\hat{W} \neq w$.

La probabilité associée à cet événement est notée

$$\begin{aligned}\lambda_w &= \mathbb{P}\left(\hat{W} \neq w | W = w\right) \\ &= \mathbb{P}\left(\psi(\mathbf{Y}) \neq w | W = w\right)\end{aligned}$$

Définitions

- **Probabilité d'erreur maximale** : $P_m^{(n)} = \max_w \lambda_w$
- **Probabilité d'erreur moyenne** : $P_e^{(n)} = \mathbb{P}\left(\hat{W} \neq W\right) = \frac{1}{M}\sum_{w=0}^{M-1} \lambda_w$

Décodage du Maximum a Posteriori (MAP)

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

Décodage du Maximum a Posteriori (MAP-bit)

Définition

- Soit $\mathcal{C}$ un code **binaire** (k, n) donné.
- Le **décodeur** du **Maximum A Posteriori bit** (**MAP-bit**) est la fonction de **y** définie par :

$$\Psi^{(j)}_{MAP-bit}(\mathbf{y}) = \underset{u \in \{0,1\}}{\operatorname{argmax}} \mathbb{P}(U_j = u | \mathbf{Y} = \mathbf{y})$$

- En pratique on calcule les **Logarithmes de rapports de vraisemblances** (LLR) :

$$L(U_i) = \log \frac{\mathbb{P}(U_i = 0|\mathbf{y})}{\mathbb{P}(U_k = 1|\mathbf{y})}$$

- **Le décodeur MAP minimise P_b (la probabilité d'erreur binaire)**
- **Le signe des LLRs : décisions MAP-bit**
- **Le module des LLRs : fiabilité des décisions**

Enjeux du codage

Compromis entre

- La **taille** du code (n)
- Le **rendement de code** (le débit)
- La **probabilité d'erreur** (maximale ou moyenne)
- La **complexité** de l'encodage
- La **complexité** du décodage

Efficacité spectrale $\Longleftrightarrow$ Codage $\Longleftrightarrow$ Efficacité énergétique

Plan

Information mutuelle

$$\begin{aligned}\mathbb{I}(X,Y) &= \mathbb{H}(X) - \mathbb{H}(X|Y) \\ &= \mathbb{H}(Y) - \mathbb{H}(Y|X)\end{aligned}$$

Elle représente la quantité moyenne d'incertitude soustraite de X une fois Y connue

Capacité

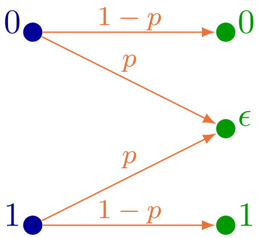
La **capacité d'un canal discret sans mémoire** de sortie $Y \in \mathcal{Y}$ et d'entrée $X \in \mathcal{X}$ et de probabilité de transition $p(y|x)$ est définie par

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

Remarque

1. Le canal ($p(y|x)$) étant **fixé**, $\mathbb{I}(X,Y)$ ne "dépend" que de $p(x)$.
2. La capacité est atteinte pour au moins une distribution ($\mathbb{I}(X,Y)$ est une fonction continue concave de $p(x)$)

Capacité du canal BEC



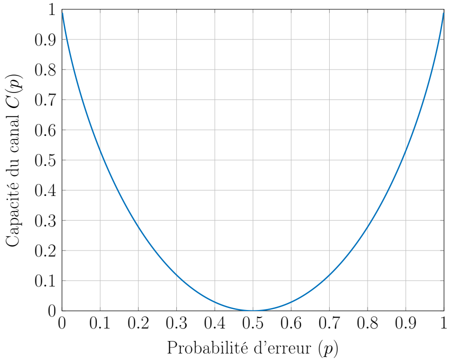
1. Montrer que la capacité du canal BEC vaut $C(p) = 1 - p$
2. Trouver la distribution $p(x)$ d'atteindre cette capacité
3. Pour quelle(s) valeur(s) de p cette capacité est-elle nulle ?

Capacité du canal BSC

La **capacité** en bits par symbole d'entrée du canal BSC vaut

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

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



Remarques

1. Si $p = 0.5$, $C(0.5) = 0$

   i.e. *la connaissance de Y ne permet pas de diminuer l'incertitude sur X.*

2. Si $p = 0$ ou $p = 1$ capacité maximale

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

$$\limsup_n R_n \leq C$$

Plan

Avant de commencer...

Remarques

1. Dans cette section $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ et le canal considéré est le **canal binaire symétrique**

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)

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)

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 ($\mathbb{Z}/2\mathbb{Z}$)

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 $\oplus \rightsquigarrow +$

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 un **code bianire linéaire** si et seulement si les mots de codes $\mathbf{c} \in \mathbb{F}_2^n$ sont obtenus à partir des messages $\mathbf{u} \in \mathbb{F}_2^k$ par la relation

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

où G est une matrice de taille $k \times n$ appelée **matrice génératrice** de $\mathcal{C}$

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

Remarques

1. $\mathcal{C}$ est un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension $rang(G) = k$
2. Il existe plusieurs matrices génératrices pour un même code.
3. le rendement du code est $R = \frac{rang(G)}{n} = \frac{k}{n}$

Code dual | Matrice de parité

Matrice de parité

Le code $\mathcal{C}$ peut aussi être défini par sa **matrice de parité** H de taille $n-k \times n$:

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

Soit $\mathbf{v} \in \mathbb{F}_2^n$, $\mathbf{v} \in \mathcal{C}$ ($\mathbf{v}$ est un mot de code) si et seulement si

$$\mathbf{v}H^T = 0$$

1. H est appelée **matrice de parité** du code $\mathcal{C}$ et vérifie $GH^T = 0_{k \times n-k}$
2. H n'est pas unique

Encodeur 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

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

La matrice de parité associée à la matrice G précédente

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

Remarques sur les encodeurs systématiques

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

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

Remarques sur les encodeurs systématiques

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

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

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

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**

Exemple de Pivot de Gauss

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

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{array}{l} \leftarrow \textbf{Pivot} \\ \\ \\ \\ \end{array}$$

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{array}{l} \leftarrow \textbf{Pivot} \\ L_2 \leftarrow L_2 + L_1 \\ \\ \\ \end{array}$$

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \leftarrow \textbf{Pivot}$$

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{array}{l} \\ \leftarrow \textbf{Pivot} \\ L_3 \leftarrow L_3 + L_2 \\ \\ \end{array}$$

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow \textbf{Pivot} \\ \\ \end{matrix}$$

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow \textbf{Pivot} \\ L_4 \leftarrow L_4 + L_3 \end{array}$$

Exemple de Pivot de Gauss

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

1. But : permuter | sommer des lignes pour faire apparaître la matrice I à droite

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

1. But : permuter | sommer des lignes pour faire apparaître la matrice I à droite
2. Cette procédure ne donne pas tout le temps une matrice de la forme $G = [P, I]$

Exemple de Pivot de Gauss

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

1. But : permuter | sommer des lignes pour faire apparaître la matrice I à droite
2. Cette procédure ne donne pas tout le temps une matrice de la forme $G = [P, I]$
3. Si G est de rang plein on peut toujours se ramener à $[P, I]$ **à une permutation de colonne près**

Exemple de Pivot de Gauss

$$G = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

1. But : permuter | sommer des lignes pour faire apparaître la matrice I à droite
2. Cette procédure ne donne pas tout le temps une matrice de la forme $G = [P, I]$
3. Si G est de rang plein on peut toujours se ramener à $[P, I]$ **à une permutation de colonne près**
4. Soit $G' = [P, I_k] = G\Pi$ où Π est une matrice de permutation des colonnes, soit $H' = [I_{n-k} P^T]$ alors

$$G'(H')^T = 0_{k \times n-k} = GH^T \text{ avec } H = H'\Pi$$