TS226
-
Codes correcteurs d'erreurs

Romain Tajan

28 septembre 2020

TS226 en bref…

Organisation du module

- 10 créneaux (1h20) de cours (amphi)
- 3 créneaux de TD (1h20) en 1/2 groupes
- 4 créneaux de TP (2h40) en 1/2 groupes
- $\sim$15 heures de travail personnel

Découpage des cours

- 1 créneau d'**introduction aux codes correcteurs**
- 2 créneaux de **théorie de l'information (Capacité d'un canal)**
- 3 créneaux sur les **codes linéaires en bloc**
- 3 créneau sur les **codes concatennés et turbocodes**

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))

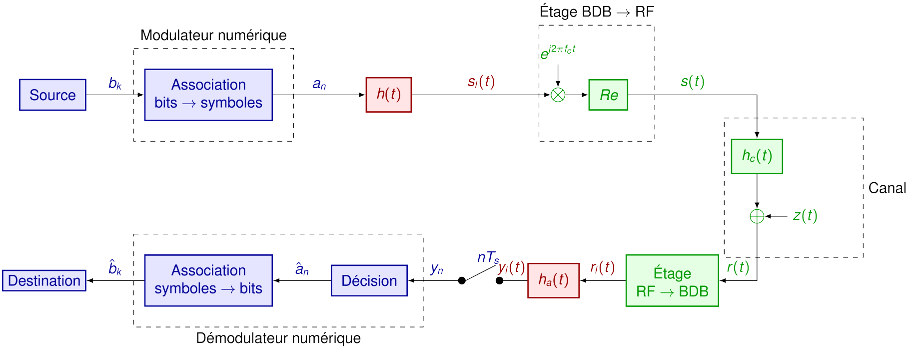
1967 **Viterbi** - Décodage optimal des codes convolutifs

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

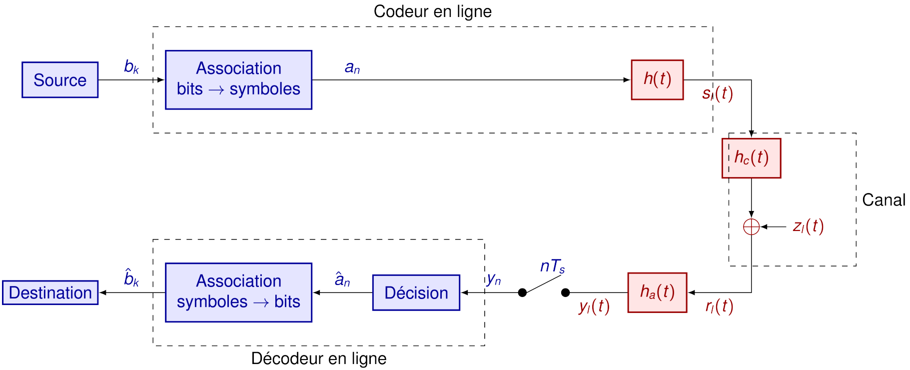
1996 **MacKay** - Ré-invente les LDPC (DVB-S2, WiFi, 5G)

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

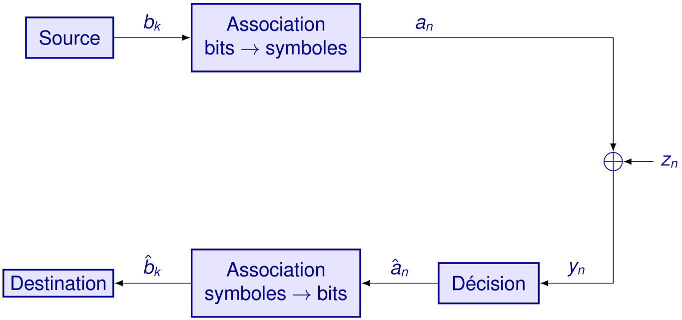
Rappels sur les communications numériques



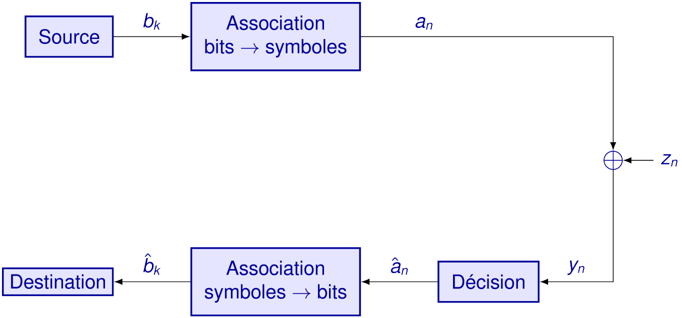
Rappels sur les communications numériques

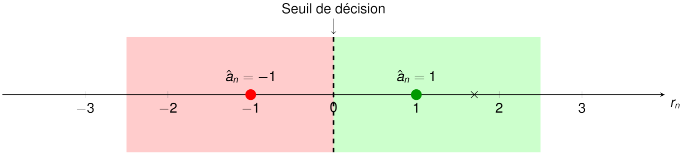


Rappels sur les communications numériques

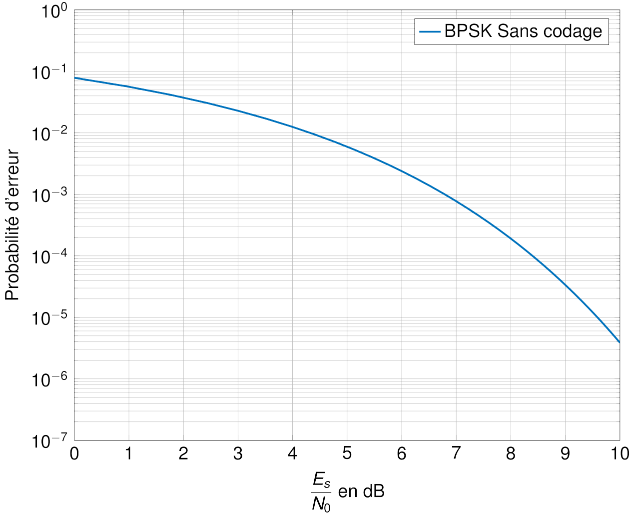


Rappels sur les communications numériques



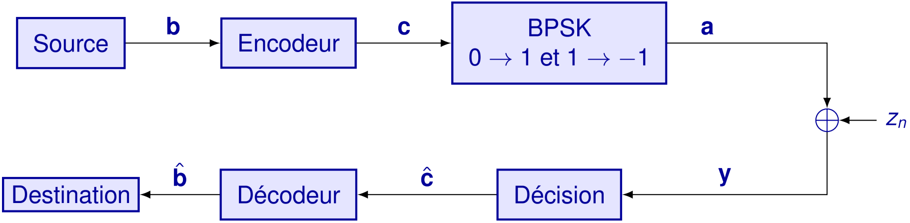


Rappels sur les communications numériques



$$P_b = Q\left(\sqrt{2\frac{E_s}{N_0}}\right)$$

Premier exemple de code : codage par répétition



Encodeur

$\mathbf{b} = [b_0, b_1, \dots b_{K-1}]$

$\mathbf{c} =$

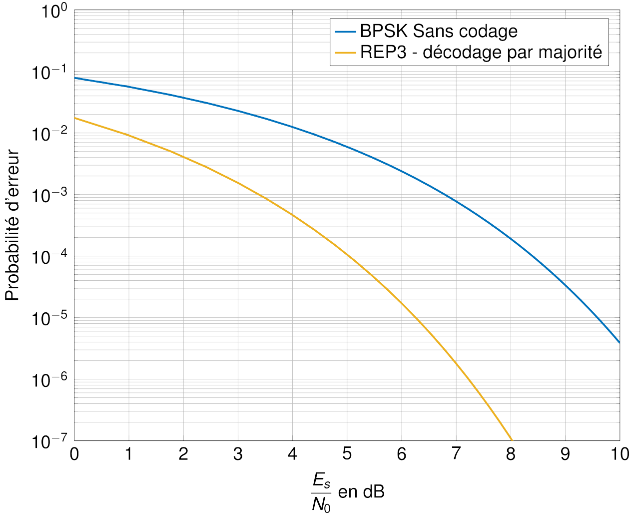
$$[\underbrace{b_0, b_0, b_0}_{\mathbf{c}_0}, \underbrace{b_1, b_1, b_1}_{\mathbf{c}_1}, \dots \underbrace{b_{K-1}, b_{K-1}, b_{K-1}}_{\mathbf{c}_{K-1}}]$$

Décodeur

$\hat{b}_k = 0$ ssi $\hat{\mathbf{c}}_k$ contient une majorité de 0

$\hat{b}_k = 1$ ssi $\hat{\mathbf{c}}_k$ contient une majorité de 1

Codage par répétition : probabilité d'erreur

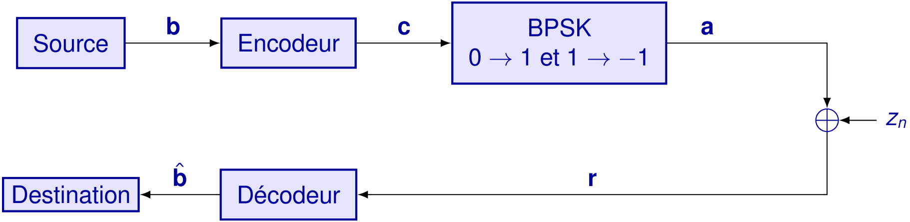


$$p_b = Q\left(\sqrt{2\frac{E_s}{N_0}}\right)$$

$$P_b = p_b^3 + 3(1-p_b)p_b^2$$

(Décodage par majorité)

Premier exemple de code : codage par répétition (2)



Encodeur

$\mathbf{b} = [b_0, b_1, \ldots b_{K-1}]$

$\mathbf{c} =$

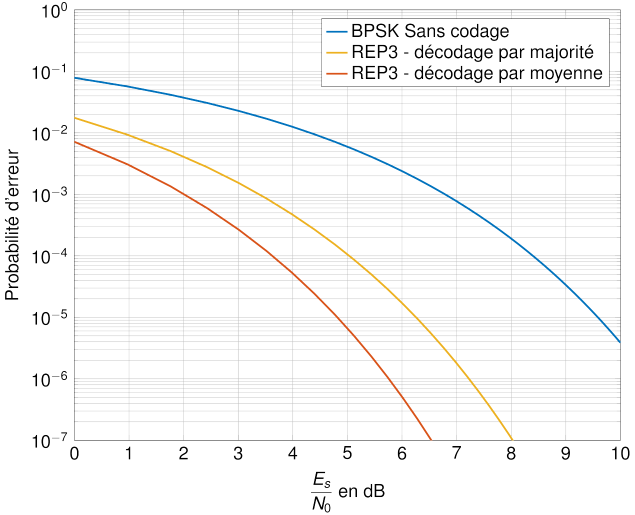
$[\underbrace{b_0, b_0, b_0}_{\mathbf{c}_0}, \underbrace{b_1, b_1, b_1}_{\mathbf{c}_1}, \ldots \underbrace{b_{K-1}, b_{K-1}, b_{K-1}}_{\mathbf{c}_{K-1}}]$

Décodeur

$\hat{b}_k = 0 \text{ ssi } \frac{1}{3} \sum \mathbf{r}_k > 0$

$\hat{b}_k = 1 \text{ ssi } \frac{1}{3} \sum \mathbf{r}_k \leq 0$

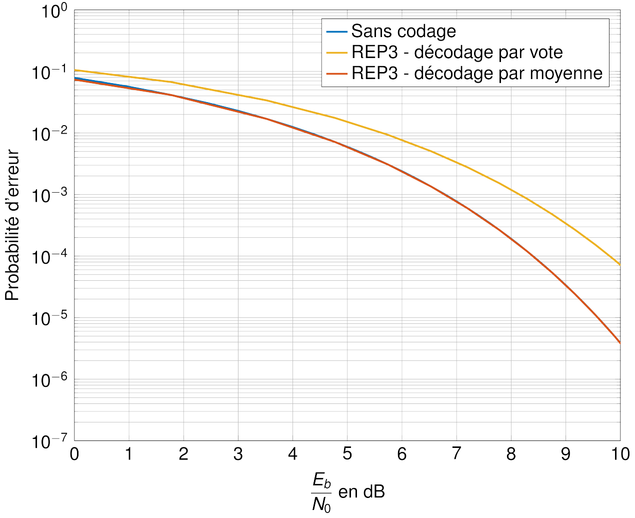
Codage par répétition : probabilité d'erreur (2)



$$P_b = Q\left(\sqrt{6\frac{E_s}{N_0}}\right)$$

(Décodage par moyenne)

Codage par répétition : probabilité d'erreur (3)



Enjeux des codes correcteurs d'erreur

Définition "naïve"

Un code correcteur d'erreur ajoute de la redondance dans le but de corriger des erreurs.

Il existe un compromis à réaliser entre :

- La taille du code (nombre de répétitions)
- Le nombre d'erreur qu'il peut corriger | détecter
- La complexité du décodage

Existe-t-il des codes plus efficaces que le code à répétition ?

Plan

Redéfinissons le canal...

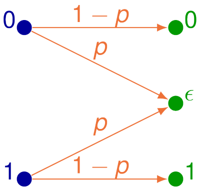
Un **canal** est défini par un triplet : $(\mathcal{X}, \mathcal{Y}, p(y|x))$ où

- $\mathcal{X}$ 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

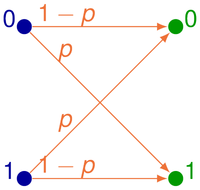
$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i)$$

Le canal à effacement binaire



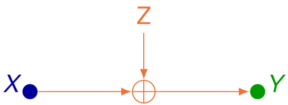
- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, \epsilon, 1\}$
- $p(\epsilon|0) = p(\epsilon|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile pour les couches hautes, pour le stockage

Le canal binaire symétrique



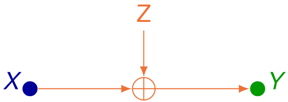
- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, 1\}$
- $p(1|0) = p(0|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile après décision

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)

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

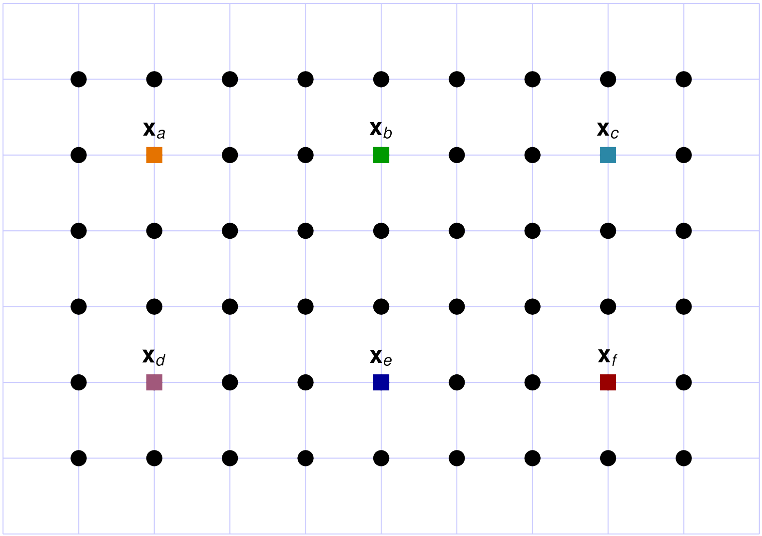
- Un ensemble de M **messages**. On notera cet ensemble $\mathcal{M} = \{0, 1, \ldots, M-1\}$
- Une fonction d'**encodage** (ou encodeur) notée ϕ **injective** :

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

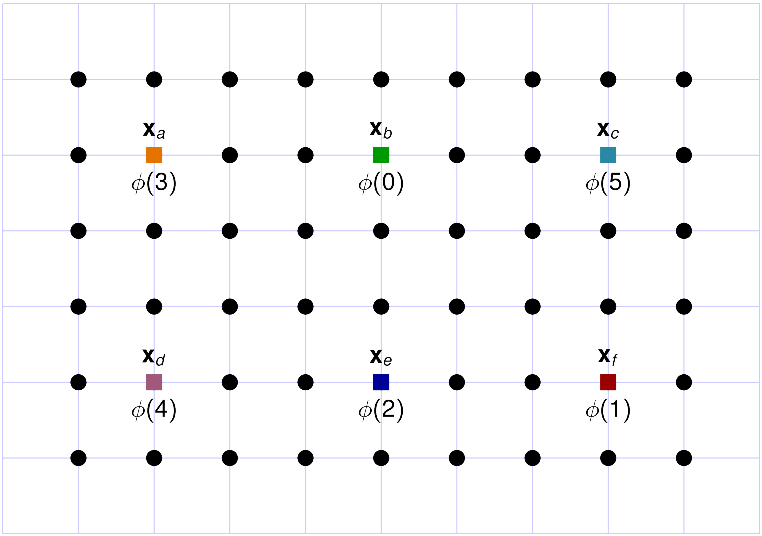
- Une fonction de **décodage** (ou décodeur) notée ψ **surjective** :

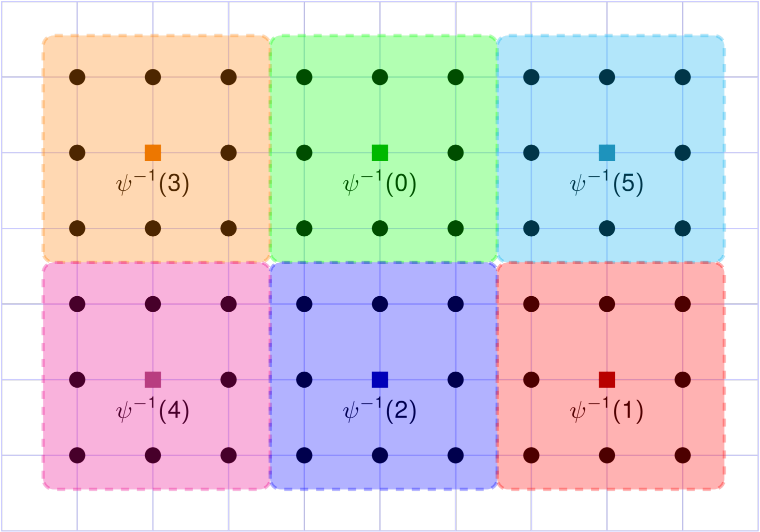
$$\begin{aligned} \psi : \mathcal{Y}^n &\rightarrow \mathcal{M} \\ \mathbf{Y} &\mapsto \hat{W} = \psi(\mathbf{Y}) \end{aligned}$$

Le ratio $R = \frac{\log_2(M)}{n}$ est appelé **rendement** du code (M, n)



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


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


$\psi^{-1}(3)$
$\psi^{-1}(0)$
$\psi^{-1}(5)$
$\psi^{-1}(4)$
$\psi^{-1}(2)$
$\psi^{-1}(1)$

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

$$\lambda_w = \mathbb{P}\left[\psi(\mathbf{Y}) \neq w | \mathbf{X} = \phi(w)\right]$$

Définitions

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

Notes :

$$\begin{aligned}
\mathbb{P}(\hat{W} \neq W) &= \sum_{w=0}^{M-1} \mathbb{P}(\hat{W} \neq w, W = w) \\
&= \sum_{w=0}^{M-1} \mathbb{P}(\hat{W} \neq w | W = w)\mathbb{P}(W = w) \\
&= \frac{1}{M} \sum_{w=0}^{M-1} \lambda_w
\end{aligned}$$

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 :

$$\Psi_{MAP}(\mathbf{y}) = \arg\max_{w \in \mathcal{M}} \mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})$$

Le décodeur MAP minimise P_e

Démonstration de l'optimalité du décodage par Maximum a Posteriori

Soit Ψ un décodeur pour un code (M, n) nommé $\mathcal{C}$. La probabilité d'erreur sous le décodage Ψ est donnée par

$$\begin{aligned}
\mathbb{P}(\Psi(\mathbf{Y}) \neq W) &= 1 - \mathbb{P}(\Psi(\mathbf{Y}) = W) \\
&= 1 - \sum_{\mathbf{y}\in\mathcal{Y}^n} \sum_{w=0}^{M-1} \mathbb{P}(\Psi(\mathbf{y}) = w | W = w, \mathbf{Y} = \mathbf{y})\mathbb{P}(W = w, \mathbf{Y} = \mathbf{y}) \text{ [Formule des proba. totales]} \\
&= 1 - \sum_{\mathbf{y}\in\mathcal{Y}^n} \sum_{w=0}^{M-1} \mathbb{P}(\Psi(\mathbf{y}) = w | W = w, \mathbf{Y} = \mathbf{y})\mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})\mathbb{P}(\mathbf{Y} = \mathbf{y}) \text{ [}\mathbb{P}(A, B) = \mathbb{P}(A|B)\mathbb{P}(B)\text{]}
\end{aligned}$$

Or, par définition de Ψ_{MAP}, nous avons que $\forall w \in \mathcal{M}, \mathbb{P}(W = w|\mathbf{Y} = \mathbf{y}) \leq \mathbb{P}(W = \Psi_{MAP}(\mathbf{y})|\mathbf{Y} = \mathbf{y})$ d'où il vient

$$\begin{aligned}
\mathbb{P}(\Psi(\mathbf{Y}) \neq W) &\geq 1 - \sum_{\mathbf{y}\in\mathcal{Y}^n} \sum_{w=0}^{M-1} \underbrace{\mathbb{P}(\Psi(\mathbf{y}) = w | \mathbf{Y} = \mathbf{y}, W = w)}_{=\delta(w-\Psi(\mathbf{y}))} \underbrace{\mathbb{P}(W = \Psi_{MAP}(\mathbf{y}) | \mathbf{Y} = \mathbf{y})\mathbb{P}(\mathbf{Y} = \mathbf{y})}_{\text{Indépendent de } w} \\
&= 1 - \sum_{\mathbf{y}\in\mathcal{Y}^n} \mathbb{P}(W = \Psi_{MAP}(\mathbf{y}) | \mathbf{Y} = \mathbf{y})\mathbb{P}(\mathbf{Y} = \mathbf{y}) \\
&= 1 - \mathbb{P}(W = \Psi_{MAP}(\mathbf{Y})) \\
&= \mathbb{P}(W \neq \Psi_{MAP}(\mathbf{Y}))
\end{aligned}$$

Décodage du Maximum de vraisemblance

Définition

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

- Le **décodeur** du **Maximum de vraisemblance** (**MV** ou **ML** (Maximum Likelihood)) est la fonction de $\mathbf{y}$ définie par : $\Psi_{ML}(\mathbf{y}) = \arg\max_{w \in \mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y} | W = w)$

- **Sur le canal BSC, décodage ML** $\Leftrightarrow \Psi_{ML}(\mathbf{y}) = \arg\min_{w \in \mathcal{M}} d_H(\phi(w), \mathbf{y})$

  $d_H(\mathbf{x}, \mathbf{y})$ est la distance de Hamming entre $\mathbf{x}$ et $\mathbf{y}$, i.e. le nombre de différences entre les deux vecteurs

Décodage du Maximum de vraisemblance

Définition

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

• Le **décodeur** du **Maximum de vraisemblance** (**MV** ou **ML** (Maximum Likelihood)) est la fonction de **y** définie par : $\Psi_{ML}(\mathbf{y}) = \arg\max_{w \in \mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y} | W = w)$

- **Sur le canal BSC, décodage ML** $\Leftrightarrow \Psi_{ML}(\mathbf{y}) = \arg\min_{w \in \mathcal{M}} d_H(\phi(w), \mathbf{y})$

  $d_H(\mathbf{x}, \mathbf{y})$ est la distance de Hamming entre **x** et **y**, i.e. le nombre de différences entre les deux vecteurs

- **Sur le canal AWGN, décodage ML** $\Leftrightarrow \Psi_{ML}(\mathbf{y}) = \arg\min_{w \in \mathcal{M}} d_E(\phi(w), \mathbf{y})$

  $d_E(\mathbf{x}, \mathbf{y})$ est la distance Euclidienne entre **x** et **y**.

Décodage du Maximum de vraisemblance

Définition

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

• Le **décodeur** du **Maximum de vraisemblance** (**MV** ou **ML** (Maximum Likelihood)) est la fonction de **y** définie par : $\Psi_{ML}(\mathbf{y}) = \arg\max_{w \in \mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y} | W = w)$

- **Sur le canal BSC, décodage ML** $\Leftrightarrow \Psi_{ML}(\mathbf{y}) = \arg\min_{w \in \mathcal{M}} d_H(\phi(w), \mathbf{y})$

  $d_H(\mathbf{x}, \mathbf{y})$ est la distance de Hamming entre **x** et **y**, i.e. le nombre de différences entre les deux vecteurs

- **Sur le canal AWGN, décodage ML** $\Leftrightarrow \Psi_{ML}(\mathbf{y}) = \arg\min_{w \in \mathcal{M}} d_E(\phi(w), \mathbf{y})$

  $d_E(\mathbf{x}, \mathbf{y})$ est la distance Euclidienne entre **x** et **y**.

- **Si W est une variable aléatoire uniforme sur $\mathcal{M}$, alors le décodeur ML est équivalent au décodeur MAP.**

Démonstration du décodage ML sur canal BSC

On cherche à exprimer Ψ_{ML} pour un code (M, n) nommé $\mathcal{C}$ sur canal BSC.

$$\begin{aligned}
\Psi_{ML}(\mathbf{y}) &= \arg\max_{w\in\mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y}|W = w) \\
&= \arg\max_{w\in\mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y}|\mathbf{X} = \mathbf{x}(w)))\ \text{[Où on note } \mathbf{x}(w) = \Phi(w)] \\
&= \arg\max_{w\in\mathcal{M}} \prod_{j=1}^{n} \mathbb{P}(Y_i = y_i|X_i = x_i(w))
\end{aligned}$$

Or, ar définition du canal BSC on a $\mathbb{P}(Y_i = y_i|X_i = x_i(w)) = \begin{cases} p, & \text{si } y_i \neq x_i(w) \\ 1-p, & \text{si } y_i = x_i(w) \end{cases}$ d'où il vient

$$\begin{aligned}
\Psi_{ML}(\mathbf{y}) &= \arg\max_{w\in\mathcal{M}} \prod_{j=1}^{n} \mathbb{P}(Y_i = y_i|X_i = x_i(w)) \\
&= \arg\max_{w\in\mathcal{M}} p^{d_H(\mathbf{y},\mathbf{x}(w))}(1-p)^{n-d_H(\mathbf{y},\mathbf{x}(w))}\ [d_H(\mathbf{y},\mathbf{x}(w)) \text{ est le nombre de différences entre } \mathbf{x} \text{ et } \mathbf{y}] \\
&= \arg\max_{w\in\mathcal{M}} d_H(\mathbf{y},\mathbf{x}(w)) \log(\frac{p}{1-p}) + n\log(1-p)\ [\log() \text{ est une fonction croissante}] \\
&= \arg\max_{w\in\mathcal{M}} d_H(\mathbf{y},\mathbf{x}(w)) \log(\frac{p}{1-p})\ [n\log(1-p) \text{ ne dépend pas de } w]
\end{aligned}$$

Si de plus $p \in [0, 0.5]$ on a $\log(\frac{p}{1-p}) \leq 0$ et finalement : $\Psi_{ML}(\mathbf{y}) = \arg\min_{w\in\mathcal{M}} d_H(\mathbf{y},\mathbf{x}(w))$

Démonstration du décodage ML sur canal AWGN

On cherche à exprimer Ψ_{ML} pour un code (M, n) nommé $\mathcal{C}$ sur canal BSC.

$$\begin{aligned}\Psi_{ML}(\mathbf{y}) &= \underset{w\in\mathcal{M}}{\arg\max}\, \mathbb{P}(\mathbf{Y} = \mathbf{y} | W = w)\\ &= \underset{w\in\mathcal{M}}{\arg\max}\, \mathbb{P}(\mathbf{Y} = \mathbf{y} | \mathbf{X} = \mathbf{x}(w)) \text{ [Où on note } \mathbf{x}(w) = \Phi(w)]\\ &= \underset{w\in\mathcal{M}}{\arg\max} \prod_{j=1}^{n} \mathbb{P}(Y_i = y_i | X_i = x_i(w))\end{aligned}$$

Or, ar définition du canal AWGN on a $\mathbb{P}(Y_i = y_i | X_i = x_i(w)) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2\sigma^2}(y_i - x_i(w))^2}$. De plus la constante $\frac{1}{\sqrt{2\pi\sigma^2}}$ étant positive, il vient

$$\begin{aligned}\Psi_{ML}(\mathbf{y}) &= \underset{w\in\mathcal{M}}{\arg\max}\, e^{-\frac{1}{2\sigma^2}\sum_{i=1}^{n}(y_i - x_i(w))^2}\\ &= \underset{w\in\mathcal{M}}{\arg\min} \sum_{i=1}^{n} (y_i - x_i(w))^2\\ &= \underset{w\in\mathcal{M}}{\arg\min}\, d_E(\mathbf{y} - \mathbf{x}(w))\end{aligned}$$

Démonstration de d'équivalence entre ML et MAP

On cherche à montrer que le décodeur Ψ_{ML} est équivalent à Ψ_{MAP} si $\mathbb{P}(W = w) = \frac{1}{M}$.

$$\begin{aligned}
\Psi_{ML}(\mathbf{y}) &= \arg\max_{w \in \mathcal{M}} \mathbb{P}(\mathbf{Y} = \mathbf{y} | W = w) \\
&= \arg\max_{w \in \mathcal{M}} \frac{\mathbb{P}(\mathbf{Y} = \mathbf{y}, W = w)}{\mathbb{P}(W = w)} \\
&= \arg\max_{w \in \mathcal{M}} \frac{\mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})\mathbb{P}(\mathbf{Y} = \mathbf{y})}{\mathbb{P}(W = w)} \\
&= \arg\max_{w \in \mathcal{M}} \mathbb{P}(W = w | \mathbf{Y} = \mathbf{y})\mathbb{P}(\mathbf{Y} = \mathbf{y})M \\
&= \arg\max_{w \in \mathcal{M}} \mathbb{P}(W = w | \mathbf{Y} = \mathbf{y}) \text{ [car } \mathbb{P}(\mathbf{Y} = \mathbf{y})M \geq 0] \\
&= \Psi_{MAP}(\mathbf{y})
\end{aligned}$$

Retour sur les enjeux

Le codage est une affaire de 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